KARLSRUHER INSTITUT FÜR TECHNOLOGIE (KIT)
SCHRIFTEN DES ZENTRUMS FÜR ANGEWANDTE RECHTSWISSENSCHAFT

18

THOMAS OTTER

Externalities and Enterprise Software

Helping and Hindering Legal Compliance

KIT Scientific
Publishing

Thomas Otter

Externalities and Enterprise Software

Helping and Hindering Legal Compliance

Schriften des Zentrums für angewandte Rechtswissenschaft

BAND 18

ZAR | Zentrum für angewandte Rechtswissenschaft
Karlsruher Institut für Technologie (KIT)

HERAUSGEBER DER SCHRIFTENREIHE

Prof. Dr. Thomas Dreier M.C.J.

Externalities and Enterprise Software

Helping and Hindering Legal Compliance

by
Thomas Otter

KIT Scientific Publishing

Karlsruher Institut für Technologie
Zentrum für Angewandte Rechtswissenschaft

Externalities and Enterprise Software:
Helping and Hindering Legal Compliance

Zur Erlangung des akademischen Grades eines Doktors der Wirtschaftswissenschaften (Dr. rer. pol.) bei der KIT-Fakultät für Wirtschaftswissenschaften des Karlsruher Instituts für Technologie (KIT)

von LL.M. Thomas Otter

Tag der mündlichen Prüfung: 13. März 2019
Referent: Prof. Dr Thomas Dreier
Korreferent: Prof. Dr. Andreas Oberweis

Impressum

Scientific
Publishing

Karlsruher Institut für Technologie (KIT)
KIT Scientific Publishing
Straße am Forum 2
D-76131 Karlsruhe

KIT Scientific Publishing is a registered trademark
of Karlsruhe Institute of Technology.
Reprint using the book cover is not allowed.

www.ksp.kit.edu

Print on Demand 2019 – Gedruckt auf FSC-zertifiziertem Papier

ISSN 1860-8744
ISBN 978-3-7315-0937-0
DOI 10.5445/KSP/1000094954

To my father, without whose persistent chiding,
this would never have been completed.

Abstract

Enterprise software plays a key role in helping organizations comply with a variety of laws and regulations, yet software itself creates negative externalities that can undermine rights and laws. Software developers are an important regulatory force, yet many know little about IT law, and how law and software interact. This work examines enterprise software developer understanding and perception of legal concepts, and explores four examples of the software code and law relationship: payroll, the Sarbanes-Oxley Act (SOX), web accessibility and data protection law.

This work is multi-disciplinary, relying on law, computer science and commerce research. Lessig's 'code as law' serves as a framework to explain how the regulatory modalities of law, market, social norms and software code interact to shape how the software industry develops for compliance. It uses two empirical studies, the first being a survey of software developer knowledge and perceptions, highlighting how little software developers know about the law that relates to software. The second is a lab test with blind and visually impaired testers of the accessibility of corporate career sites.

The majority of websites are inaccessible to many people with disabilities. This work traces the history of web accessibility, performs a lab test to assess corporate career site accessibility, analyses the causes of failure, and suggests mechanisms to reduce the negative externality of accessibility failure. Payroll illustrates a synergistic relationship between vendor and government; modern income taxes and social insurance collection would be impossible without the collaboration of the software industry. Within 2 years of the passage of SOX, the enterprise software industry created a new multi-billion US$ market for controls and risk software called GRC. This highlights how the software industry can respond with alacrity to a new compliance requirement, and how laws can have unintended consequences.

The General Data Protection Regulation (GDPR) is the largest change in privacy law this century. The perspectives developed with payroll, SOX and accessibility are used to explore and assess GDPR in the enterprise software context.

The conclusion provides suggestions on how regulators, software vendors and educators might work more effectively to reduce the negative externalities that enterprise software directly or indirectly creates.

Acknowledgements

Well over a decade ago, Klaus Tschira suggested that I talk to Professor Thomas Dreier at the ZAR at KIT. I am grateful to Klaus for many things, but I am especially thankful for that. Klaus is sorely missed. Professor Dreier's patient encouragement enabled me to push through to submission. Thank you.

Dr Oliver Raabe has been a most dedicated and willing mentor and guide. His knowledge, encouragement and generosity seem limitless. Without his support, much of this work would have remained mere ideas. Dr Thorsten Schwarz at the KIT SZS went out of his way to help me with the lab test for the blind and visually impaired students, and provided support and advice as I learnt about the challenges that software can inflict on people with disabilities. Max, Florian, Joshua and Philipp, thank you for your deep and focused engagement with testing. Thank you also to Professor Andreas Oberweis for being the secondary supervisor. Thanks to Daniel Vonderau for his help with legal citations and research, and others at KIT for their support. It is a most welcoming and special place

I am very grateful to the nearly 600 people who took time to diligently respond to the survey, and to those who publicised it, especially James Governor. Thanks to Irina Sedenko and Dr Ron Fisher for their help with the statistical analysis. They helped me make sense of the survey data. Professor Armin Trost, your encouragement and advice helped me develop more discipline and rigour. Thanks also to the people I interviewed along the way: Matthew, Liz, Michael, Anne, Neil, Chirag, Janet, Nichole, Jerome, Nigel, Rebecca, James, Jonas and Dr Fuchs.

To my wife, Charlotte, and our children, thank you for all you do. I am sure I have not been that easy to live with during the final push. Charlotte's proofreading was invaluable, but any remaining random punctuation is entirely my fault.

I would also like to thank my employer, SAP SE, for allowing me the time off work to finally put to bed what I had been doing in a desultory fashion part time for a very long time.

And finally, thanks Dad. Your gentle but constant chiding was a brilliant bit of parenting.

Table of Contents

List of Tables

List of Figures

List of Abbreviations and Acronyms

ADA	Americans With Disabilities Act of 1990, as amended
AGG	Allgemeines Gleichbehandlungsgesetz
ANSI	American National Standards Institute
ANSI A117.1	Specifications for Making Buildings and Facilities Accessible to, and Usable by, the Physically Handicapped (1961)
APA	American Payroll Association
AS2	Audit Standard 2
AS5	Audit Standard 5
AT	Assistive Technologies
BDA	Bundesteilhabegesetz
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGG	Behindertengleichstellungsgesetz
BITV	Barrierefreie-Informationstechnik-Verordnung
BMAS	Bundesministerium für Arbeit und Soziales
BMG	Bundesministerium für Gesundheit
BS	British Standard
BS10012	Personal Information Standard (data protection)
BS8878	Web accessibility guideline

BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI	British Standards Group
CAGR	Compound Annual Growth Rate
CEA	Council of Economic Advisers
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization.
CIPP	Chartered Institute of Payroll Professionals
CNIL	Commission nationale de l'informatique et des libertés
COBIT	Control Objectives for Information and Related Technologies
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRPD	See UNCRPD
DAISY	Digital Accessible Information System
DARPA	Defense Advanced Research Projects Agency
DDA	Disability Discrimination Act 1995
DEÜV	Verordnung über die Erfassung und Übermittlung von Daten für die Träger der Sozialversicherung
DIN	Deutsches Institut für Normung
DIN18040	Norm Barrierefrei Bauen
DOJ	Department of Justice
DPIA	Data Protection Impact Assessment
DPO	Data Protection Office

DWP	Department of Works and Pensions
EBU	European Blind Union
EEA	European Accessibility Act
EN 301 459	Accessibility requirements suitable for public procurement of ICT products and services in Europe
ERM	Enterprise Risk Management
ETSI	The European Telecommunications Standards Institute
ETSI EG 202	Guidelines for generic user interface elements for mobile terminals and services
EUDPD	The Data Protection Directive 95/46/EC
eXTRa	einheitliches XML-basiertes Transportverfahren
FIPS	Federal Information Processing Standards
FLSA	Fair Labor Standards Act
GAAP	Generally Accepted Accounting Principles
GDPR	General Data Protection Regulation
GG	Grundgesetz
GRC	Governance Risk and Compliance
HCM	Human Capital Management
HIPPA	Health Insurance Portability and Accountability Act
HMRC	Her Majesty’s Revenue and Customs
IAPP	International Association of Privacy Professionals
ICIF	Internal Controls Integrated Framework
ICO	Information Commissioner’s Office

ICT	Information and computer technology
IDE	Integrated Development Environment
IFRS	International Financial Reporting Standards
IoT	Internet of Things
ISO	International Standards Organization
ISACA	Information Systems Audit and Control Association
ISAE-3402 / SSAE 16	Assurance Reports on Controls at a Service Organization
ISMS	Information Security Management System
ISO-14289 PDF/UA-1	Document management applications. Electronic document file format enhancement for accessibility
ISO25010/1	Systems and software Quality Requirements and Evaluation (SQuaRE) System and software quality models
ISO27001	Information technology – Security techniques – Information security management systems
ISO27014	Provides guidance on concepts and principles for the governance of information security, by which organizations can evaluate, direct, monitor and communicate the information security related activities within the organization
ISO38500	Provides guiding principles for members of governing bodies of organizations on the effective, efficient and acceptable use of information technology (IT) within their organizations
ISO9001	Specifies requirements for a quality management system
ISTQB	International Software Testing Qualification Board

ITIL	Information Technology Infrastructure Library
ITSG	Informationstechnische Servicestelle der gesetzlichen Krankenversicherung GmbH
NAO	National Audit Office
PAYE	Pay as you earn
PbD	Privacy by Design
PCAOB	Public Company Accounting Oversight Board
PET	Privacy Enhancing Technology
PIA	Privacy Impact Assessment
PWD	People with Disabilities
RFID	Radio Frequency Identification Device
RNIB	Royal National Institute of Blind People
RTI	Real Time Integration
SAS 70	Statement on Auditing Standards No. 70
SEC	Securities and Exchange Commission
Section 404	Section 404 of the Sarbanes-Oxley Act of 2002
Section 508	Section 508 of the Rehabilitation Act of 1973
SEI	Software Engineering Institute
SGB IV	Sozialgesetzbuch (SGB) Viertes Buch (IV) – Gemeinsame Vorschriften für die Sozialversicherung
SGB IX	Sozialgesetzbuch Neuntes Buch – Rehabilitation und Teilhabe von Menschen mit Behinderungen
SOC	Service Organization Controls Report
SoD	Separation of Duties

SOX	Sarbanes-Oxley Act
SZS	Studienzentrum für Sehgeschädigte
TOGAF	The Open Group Architecture Framework (TOGAF)
UML	Unified Modelling Language
UNCRPD	United Nations Convention on the Rights of Persons with Disabilities
UNDHR	United Nations Universal Declaration of Human Rights
UNECE	United Nations Economic Commission for Europe
VPAT	Voluntary Product Accessibility Template
W3C	World Wide Web consortium
WCAG	Web Content Accessibility Guidelines
WP29	Working Party 29
ZAR	Zentrum für Angewandte Rechtswissenschaft

1 Research introduction

This dissertation sits awkwardly at the intersection of information technology, law and business. This multi-disciplinary approach runs the risk of glibly skimming the surface of specialized research, without adding anything of substance.

While software has helped positively transform our lives and society in so many ways, it also creates and perpetuates negative externalities. This work aims to explore those externalities through the lens of enterprise software.

1.1 Research observation

The enterprise software industry has built solutions that aid legal compliance, yet it also creates externalities that undermine significant laws and rights. Software developers are an important regulatory force, yet many do not know much about law. This research will examine enterprise software developer understanding and perception of legal concepts, and explore four examples of where software code and law interact: payroll, Sarbanes Oxley[1] (SOX), web accessibility and data protection law, specifically the GDPR.[2]

[1] Sarbanes Oxley (SOX), a major reform in US financial reporting and audit practice. The Sarbanes – Oxley Act of 2002 (Pub.L. 107–204, 116 Stat. 745, enacted July 30, 2002). See chapter 10 for details.

[2] GDPR General Data Protection Regulation – General Data Protection Regulation (GDPR) (EU) 2016/679

1.2 Research justification and significance

A quote from a well-known computer scientist, a phrase from a leading legal theorist and a Latin maxim served as the inspiration for this research.

Joseph Weizenbaum:

> *"The computer programmer is a creator of universes for which he alone is the lawgiver. No playwright, no stage director, no emperor, however powerful, has ever exercised such absolute authority to arrange a stage or field of battle and to command such unswervingly dutiful actors or troops."*

Lawrence Lessig:

> *"Code is Law" and "The code embeds certain values* or *makes certain values impossible"*

Brocard: (attributed to Cicero and others)

> *"Ignorantia legis non exusat"*[3]

Adding to the understanding of how software code can help or hinder compliance will require a mix of theoretical and empirical analysis:

1. Software developers create code that interacts with, supports or undermines law and rights, but there has been little examination into what software developers are taught or know about law and legal concepts.
2. Modern income tax and social insurances are collected by software. In the most fundamental sense, payroll software is responsible for the collection of trillions of dollars of tax revenue and impacts almost all people in formal employment. This research will illustrate how

[3] Ignorance of the law is no excuse.

software development has supported and fostered tax collection regulation and compliance. Payroll technology has received relatively little attention from legal or information technology academia.

3. SOX has been the largest revision of US financial regulations since the 1930s. It impacted accounting and business controls around the world, and it helped spawn a new software market, called Governance, Risk and Control (GRC). This research will show how the enterprise software industry was able to exploit the law to drive favourable business outcomes for itself, while providing solutions to aid compliance. There is extensive research on SOX, but relatively little about the software vendor role.
4. More than 10% of the world's population has some form of disability. Accessibility is well established as a human right in UN, EU and many national laws, yet most web applications are not accessible. This research will show that law-makers have largely failed to create a legal framework that encourages accessible web software development and why software developers continue to develop inaccessible software.
5. The General Data Protection Directive is the most significant legal development of this century for the software industry and privacy by design is central to GDPR's success or failure. This research will highlight strengths and concerns with the GDPR, then use experiences from accessibility, SOX and payroll as well as early evidence from GDPR compliance efforts to analyse GDPR's likelihood of success, and tentatively suggest areas for improvement.

1.3 Research questions

What do software developers understand about the law that relates to software?

How does the software industry fail to deliver accessible solutions?

How has the development of payroll software supported and influenced tax and social insurance regulations?

What drove the investment into software to support Sarbanes-Oxley compliance?

Is privacy by design, as defined in the GDPR, likely to succeed?

What should software companies, software developers, educators and regulators do to reduce software's negative externalities?

1.4 Research techniques

While some of this work depends on an analysis of prior literature, market data, statutes, court case reports, functional and technical standards documentation, two primary source empirical studies provide the main foundation for the findings.

1. A structured 25 question survey of almost 600 software developers from over 20 countries.
2. A four day laboratory evaluation and observation of blind and visually impaired users applying for jobs on 10 career sites to robustly assess the accessibility of the sites.

These are bolstered by several other more modest empirical initiatives: Semi / unstructured, documented interviews with several relevant experts and users, such as payroll legal product managers, software designers, accessibility advocates, blind and visually impaired software users as well as automated accessibility tool assessment of the 10 career sites, and meta-data analysis of an industry software analyst database.

1.5 Chapter structure and outline

Chapter two: Defining and exploring key concepts

It is useful to define and explore the key concepts that this work broadly relies on. These are externalities, ‘code is law’, standards and regulation, and enterprise software. The modality framework from code is law (law, social norms, market and architecture) is then used extensively throughout the work.

Chapter three: Software developer knowledge and perception survey design

This describes the survey research method and structure. It briefly notes the reasons for the survey, its assumptions and limitations. It then explains the structure and content of the survey. The primary goal of the survey is to explore developer attitudes, understanding and awareness of legal topics, and how they relate to software.

Chapter four: Software developer knowledge and perception survey results and analysis

This provides the survey results and the analysis thereof. It also examines weaknesses in the survey design. The findings from the survey are then used throughout the rest of the work.

Chapter five: Defining and exploring disability and web accessibility

Disability rights, law and study is a rich field of research, but not widely followed in broader information technology law or computer science research. This section will provide an overview of disability rights and accessibility law, focusing predominantly on web accessibility. The overview covers the law, its implementation in the US, UK, Germany and the EU, and at UN level. This chapter sets the scope for chapter six.

Chapter six: Empirical assessment of web accessibility in an enterprise software context

This chapter begins by providing a summary of web accessibility assessments done to date. It then explores modern recruitment practices and technologies. The main part of the chapter is the lab assessment of the accessibility and usability by blind / visually impaired users of the corporate career sites of 10 German companies / public sector organizations. It also examines the results of automated tests. The chapter provides evidence of the impact of the negative externality of poor accessibility and usability.

Chapter seven: Examining the causes of accessibility failure

The reasons for accessibility failure are complex and multi-disciplinary, and this chapter seeks to highlight and categorise those failures, across the dimensions of the 'Lessig' modalities of law, social norm, market and architecture / code. It explores issues such as the fragmented legal landscape, developer attitudes, educational gaps, the state of standardization and market dynamics.

Chapter eight: Fixing accessibility failure

Having analyzed both a specific example of accessibility failure and the broader context earlier, this chapter aims to make suggestions on how to improve accessibility. It suggests that the software industry has much to learn from the building architecture profession and, while more effective government intervention will help, ultimately it is the responsibility of the software industry to avoid building software that undermines the human rights of others.

Chapter nine: Payroll: The original code is law

The previous chapters on accessibility highlighted how the software industry's approach to accessibility has undermined the rights of people with disabilities. It is a strong example of a negative externality. Payroll software provides a study in the opposite position. This chapter will explore the history of payroll software and the market, noting briefly the birth of business computing, and illustrate how the tight working relationship between the software vendors and governments has shaped modern income tax and social insurance processes. It will examine how technology shifts empowered new forms of collection in the UK and Germany. The chapter concludes by briefly noting how the experiences of payroll could be more thoughtfully applied elsewhere in the industry.

Chapter ten: Sarbanes-Oxley. The accidental instigator of a new software market

The passage of SOX, and the regulatory framework it created spawned the rapid development of a new market for software, called Governance Risk and Compliance (GRC). This chapter traces the passage of SOX and its regulatory framework and standards. It then examines how the enterprise software industry reacted to turn this law into a massive market for its software. Again, it will rely on the 'Lessig' modality framework.

Chapter eleven: GDPR in the enterprise software context

GDPR has reset the legal and technical focus on data protection, in both academia and in business. This chapter briefly notes the history of data protection law; it then compares GDPR with its predecessor. It notes some of the critiques of the GDPR. The Lessig modality framework provides a useful lens to provide suggestions for how the aims of the GDPR, in particular Privacy By Design, can be more effectively achieved. SOX, Payroll and Accessibility all provide mechanisms and lessons learned that can be applied to data protection.

Chapter twelve: Returning to Weizenbaum, Cicero and Lessig

This chapter will briefly reflect on the research questions and observations, and then make a plea for the software industry to consign the 'move fast and break things' maxim to the bin of history.

2 Definitions and context

2.1 Chapter purpose: Placing code is law, externalities and enterprise software in context

It is useful to define and place in context key concepts: ‘Code is law’, externalities, and enterprise software and standards. These are important throughout this work and, given its multi-disciplinary nature, what may seem obvious to a legal scholar may be new to a computer scientist, political scientist or economist, and the reverse.

2.2 Code is law: Expanding on Lessig’s modalities

Code is law, and the research it spawned, is central to this work. This section will discuss Lessig’s aphorism[1] and explore some of the research that it inspired, and make some modest suggestions for improvement.

When the question of internet governance first emerged in the 1990s, there were two common schools of thought.

- The internet doesn’t pose new challenges to the existing legal frameworks, and that regulation would not need to change much at all. See for instance, Esterbrook.[2]

[1] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999).

[2] Frank H Easterbrook, ‘Cyberspace and the Law of the Horse’ (1996) 207 University of Chicago Legal Forum; Jack Goldsmith, ‘Regulation of the Internet: Three Persistent Fallacies’ (1997) 73 Chicago-Kent Law Review.

- The aspiration that the internet would replace traditional laws, creating entirely new forms of governance, most famously Barlow's declaration of the independence of cyberspace.[3] And that it "radically subverts a system of rule-making based on borders between physical spaces, at least with respect to the claim that cyberspace should naturally be governed by territorially defined rules."[4]

The practical reality lay between the two, and over the course of the 1990s and 2000s legal scholars began to take the idea that software code serves a regulatory function seriously.[5] Intellectual property, especially copyright, was at the centre of much of the early discussion, but privacy also received some attention, as legal theorists grappled with the question of who and how will the internet be governed?

Lessig's code is law provides a useful framework to understand how behaviour in society is regulated. He initially notes four regulating modalities.[6]

Laws regulate by the threat of ex post sanction. Law is a command, backed up by the threat of sanctions. Law is (in theory anyway), a well-defined constraint within the jurisdiction of the law giver or sovereign. The constraint, objectively, is the threat of punishment.

[3] John Perry Barlow, 'A Declaration of the Independence of Cyberspace, 1996' [1996] URL: http://homes. eff. org/~ barlow/Declaration-Final. html.

[4] David G Post, 'Against "Against Cyberanarchy" - a Reply to Jack Goldsmith' (2002) 17 Berkeley Technology Law Journal 1365; David Reynold Johnson and David G Post, 'Law And Borders -The Rise of Law in Cyberspace". '.

[5] Lessig, *Code and Other Laws of Cyberspace*; Lawrence Lessig, 'The Limits in Open Code: Regulatory Standards and the Future of the Net' 759; Joel R Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76; Timothy S Wu, 'Cyberspace Sovereignty? - The Internet and the International System' (1998) 10 Harvard Journal of Law & Technology 647; G. Greenleaf, 'An Endnote on Regulating Cyberspace: Architecture vs Law?' (1998) 21; Jonathan Zittrain, 'Internet Points of Control' (2003) 44 Boston College Law Review 653.

[6] Lessig, *Code and Other Laws of Cyberspace* 89.

Social norms constrain differently; these are those constraints that members of a community place on each other. Like law, the sanction comes after the breach. Depending on the norm, it may be a more powerful regulator than law (norm theory has a rich history in sociology, going back to Durkheim and Weber). Much of our lives is governed by norms, and often following them is not a conscious effort. Until relatively recently, legal theorists and economists largely underplayed the importance of social norms.[7]

The market constrains or manages the exchange of goods and services via the mechanism of price. The market constraint is synchronous in that the obligation to pay and the right to receive happen at the same time. The market in turn is constrained by norms and laws.

Physical architecture: An impassable mountain range or body of water serves as a dividing border. The design of roads regulates traffic flow. A cathedral creates a sense of awe. Physical architecture as a constraint is obvious when discussing built accessibility. The architectural constraint differs from both norms and laws in that you cannot disobey it and then risk punishment, as the architecture prohibits or constrains your behaviour ex ante. Some architectural constraints are relative, for instance the strength of a lock on a door; others absolute, for instance gravity.

Lessig makes the critical point that architectural constraints work whether the subject knows they are working or not. Laws and norms work only if the subject knows something about them, either deliberately or via internalization.

This model of regulation is not novel. For instance, Reidenberg developed the useful metaphor of Lex informatica.[8] In Germany, the relationship

[7] Robert C Ellickson, 'Law and Economics Discover Social Norms' (1998) 27 Journal of Legal Studies 537.

[8] Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology'.

between technology and regulation has received considerable attention, see for instance[9] the work of Lutterbeck[10] and others.[11] The contribution of Lessig and his colleagues was to popularize applying the architecture constraint concept to software code. Lessig equates the software code regulatory role to that of architecture. The code makes some behaviours possible and other behaviours impossible. The code embeds certain values or makes certain values impossible.[12] Code regulates. The 4 modalities of regulation are not independent; they all influence each other and sometimes overlap.

Lessig's theory is not without its critics, for instance Mayer-Schönberger argues the "interplay between technology and society is both vastly more complex and bidirectional than Lessig's model, with societal processes (much beyond the simplistic metaphor of the invisible hand of commerce) influencing technology as technology influences society."[13] Post levelled similar criticism.[14] Also technology is rarely without unintended consequences and Hosein et al give the example of the problem of reification of code, more commonly called technological determinism.[15]Wu examines

[9] This work does not give the German school of data protection theory enough attention.

[10] Bernd Lutterbeck, 'IT and Society: One Theory to Rule Them All?' (2006) 4 Poiesis & Praxis: International Journal of Technology Assessment and Ethics of Science 1.

[11] Johann Bizer, 'Sieben Goldene Regeln Des Datenschutzes' (2007) 31 Datenschutz und Datensicherheit – DuD 350; Oliver Raabe and others, '14 Thesen Zum Datenschutz Im Smart Grid' (2011) 35 Datenschutz und Datensicherheit – DuD 519; Ulrich Dammann and Spiros Simitis, *Bundesdatenschutzgesetz* (Nomos 2014); Gerrit Hornung, 'Regulating Privacy Enhancing Technologies: Seizing the Opportunity of the Future European Data Protection Framework' (2013) 26 Innovation 181; Helmut Bäumler and others, 'Marktwirtschaftlicher Datenschutz' (2002).

[12] Tim Wu, 'When Code Isn't Law' (2003) 89 Virginia Law Review 679, 129.

[13] Viktor Mayer-Schonberger, 'Demystifying Lessig' (2008) 2008 Wisconsin Law Review.

[14] David G Post, 'What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace' (2000) 52 Stanford Law Review 1439.

[15] Ian Hosein, Prodromos Tsiavos and Edgar A Whitley, 'Regulating Architecture and Architectures of Regulation: Contributions from Information Systems.', *Regulating architecture and architectures of regulation: Contributions from information systems. International review of law, computers & technology.* (Taylor & Francis Group 2002).

the drivers behind compliance more precisely. He makes the point that compliance can be understood to depend less on punishment than on the cost of mechanisms of change or avoidance, and he notes the power of code to change that equation. Wu also notes the similarity between the coder and the tax lawyer.[16] This metaphor will be revisited in the sections on payroll and SOX.

Grimmelmann argues that Lessig's architecture metaphor is strained.[17] In his critique of Lessig's code as architecture postulation, he outlines 3 attributes of software code.

- Automated: Once the code is written, it can operate on its own
- Immediate: Software constrains conduct prospectively. (It doesn't allow you to do something, rather than punishing you after the act)
- Plastic: Programmers have a power to build almost whatever they want. Grimmelmann quotes Brooks' castles in the air. [18]

He then describes the consequences of using software as a regulator.

- Software acts according to rules rather than standards:[19]This is an important differentiator, and one that is often lost when law makers seek to apply standards to software. In law, standards typically involve a case-by-case assessment. Rules provide an outcome, using a defined set of inputs. The algorithm is the judge. Grimmelmann makes the important point that the software implements what the programmer thinks is right. He calls this "ruleishness." While grammatically awkward, it makes the point well.
- Software need not be transparent: Good law is generally predictable and accountable. For instance, a judge needs to be able to explain why

[16] Wu, 'When Code Isn't Law'.

[17] James Grimmelmann, 'Regulation by Software' 1719.

[18] The Weizenbaum quote cited in the introduction here is perhaps even more appropriate.

[19] Software developers and legal theorists use the term standard to mean different things. See standards section below.

they took a position, and is accountable for that position. Software is asymmetric in that unless one can actually read and test the code, the mechanisms by which the software set the constraints and rules are not apparent. Software can also become so complicated that it becomes impossible for anyone to actually explain it. He calls this opacity.

- Software rules can't be ignored: In society, the decision to obey or ignore a law is a matter of choice versus consequences. Indeed, sometimes it is good social policy to ignore the law, either because the law is imperfect or because it isn't needed. People agree to loan money without contracts when there is a high level of trust. The law should not intrude unless it is needed, but, when law is coded, it imposes itself even if it is not wanted or needed in the relationship.[20] Code does not cope with ambiguity very well. Outside of code, feedback drives change. If a judge gets it wrong, it can be addressed at appeal. In a market, if price is too high, it will drop. Social norms adapt. Once written, code doesn't listen. He calls this ubiquity.

- Software is vulnerable to sudden failure: Software can be hacked. Software can break. Software generally doesn't heal itself either. He calls this fragile.

Despite the criticism, Lessig's metaphor of code as architecture remains useful and, like all metaphors, it has it limits. Grimmelmann and others have added a more nuanced understanding of code's regulatory powers and limits.

2.2.1 Adding to code is law

This understanding of code, while richer, is not complete and requires further clarification.

[20] The struggle to get copyright functioning effectively in software is evidence of this.

- Code is stubborn. Grimmelman's categorization of software as plastic is only half correct. Software is more like clay or concrete. Creating it and modifying it are very different things. For instance, in the context of payroll, the bespoke payroll of a railway required information about whether the employee's work shift was uphill or downhill. This was a rule that was developed when the trains ran on steam, as uphill was paid more because the stoker needed to shovel more coal. The rule was phased out when the union agreement eventually changed, but because the code was so complex, it was never changed, even 30 years later.[21]
- Code watches and remembers. Lessig and others rightly note that code acts to stop actions at the point of action. But code also has a powerful ex-post function. Code creates evidence. Even if the code is not engineered to force compliance, audit logs and data trails can create evidence that fundamentally shifts the balance of other laws. Witness the tension between privacy and surveillance.
- Code is business. While some software is built for research purposes, most software is built with the end goal that someone will pay for it.[22] Software companies generally build what they believe the market is asking for. There are no prizes in capitalism for building software that complies with a law that the market isn't interested in complying with.
- Code costs. The idea that developers have few design constraints is overly romantic. Commercial pressures, technical constraints, and developer or designer ignorance lead to decisions or omissions that compromise code's regulatory effectiveness.

Brown and Marsden note the differing forms of regulation: government regulation, industry self-regulation and co-regulation, and they develop a more sophisticated framework for understanding regulation, beyond the simple binary government 'sledge hammer' v industry self-regulation

[21] Author's own experience as a software consultant to several railways.

[22] Even open source code is paid for, even if indirectly, via support-based companies such as RedHat.

perspective. They explore the example of IoT /RFID data protection in Europe as an example of this co-regulatory approach.[23]

The research into the relationship between software and law has grown into a significant discipline, and since code is law was published, legal scholars have become more sophisticated in their understanding of code, and information technologists have become better acquainted with legal theory and economics. However, there is still much to do.

2.3 What is enterprise software?

The term enterprise software is widely used by practitioners, industry, in business research and to a lesser extent in computer science. Other related terms such as Enterprise Resource Planning, Enterprise Risk Management and Enterprise Architecture are all examined extensively in literature, in both business and computer science. There is no consistent definition of what enterprise software is in academic literature. Campbell-Kelly, the computer historian, uses the term corporate software products and notes "there is no one best way to understand the growth and development of the corporate software industry."[24] Kude et al note enterprise application software (EAS) providers develop and offer solutions that range from components and modules that support particular business functions to cross-functional or inter-organizational enterprise systems that are integrated through comprehensive middleware.[25] For the sake of this work, enterprise software is software that is built for or sold to corporations or the public sector. Typically, software is described as either enterprise or consumer.

[23] Ian Brown and Christopher T Marsden, *Regulating Code* (2013) 63.

[24] Martin Campbell-Kelly, *From Airline Reservations to Sonic the Hedgehog : A History of the Software Industry* (MIT Press 2003) 168.

[25] Thomas Kude, Jens Dibbern and Armin Heinzl, 'Why Do Complementors Participate? An Analysis of Partnership Networks in the Enterprise Software Industry' (2012) 59 IEEE Transactions on Engineering Management 250.

There are various firms analyzing the size of the enterprise software market, with Gartner suggesting that the 2017 spend on enterprise software was 354 billion US$.[26] Statisica note similar numbers, with 2017 spending at 335 billion US$.[27]

Human Resource Management software (HRMS) or Human Capital Management (HCM) software was a 14 billion US$ market in 2017,[28] sometimes seen as a subset of the ERP market. HCM is made up of learning management, employee performance management, compensation, career and succession planning, workforce planning, recruitment, time and attendance, core HRMS, benefits and payroll. This work examines payroll systems and recruitment systems in closer detail. Within financial systems, this work will focus on Governance Risk and Compliance systems (GRC). IDC estimated the market for GRC software to be 11.8 billion US$.[29]

2.4 Externalities and market failure theory, briefly

Market failure theory has occupied leading economic minds since Adam Smith, and the extent of market failure and the mechanisms to remedy that market failure have been topics of fierce debate for many years, with no obvious end in sight.

[26] See *https://www.gartner.com/newsroom/id/3811363*

[27] *https://www.statista.com/statistics/203428/total-enterprise-software-revenue-forecast/*

[28] Human Capital Management Applications from IDC WW HCM & Payroll Applications Forecast, 2017-2021 (June 2017) #US42766017

[29] See *https://www.businesswire.com/news/home/20170726005133/en/Strong-Demand-Expected-Drive-Worldwide-Governance-Risk*

See for instance, the Pigou v Coase debate. [30] This work does not seek to add to that debate.

Market failure, in economic parlance, is the inefficient allocation of goods and services. An externality is a form of market failure.

Dahlman, an economist, notes that, "We say that when an externality is present there is a divergence between private and social cost."[31] Alternatively, externalities are instances where an individual or firm's actions have consequences for others for which there is no compensation.[32]

Externalities can be positive or negative. Pollution is often cited as an example of a negative externality, and law and regulations have been deployed to help address the negative externality.[33] Car usage also has negative externalities, for instance, air pollution, noise, road damage, injury to others.[34]A classic example of a positive externality is immunization

[30] Harold Demsetz, 'The Core Disagreement between Pigou, the Profession, and Coase in the Analyses of the Externality Question' (1996) 12 European Journal of Political Economy 565; RH Coase, 'The Problem of Social Cost' (1960) 3 The Journal of Law and Economics 1; Arthur Cecil Pigou, *Wealth and Welfare* (Macmillan 1912); Steven G Medema and Warren J Samuels, 'Ronald Coase and Coasean Economics: Some Questions, Conjectures and Implications' [1997] The economy as a process of valuation 72.

[31] Dahlman, 'The Problem of Externality' (1979) 22 The Journal of Law and Economics 141 162, 141.

[32] Jean Camp and Catherine Wolfram, 'Pricing Security', *Economics of Information Security* (2004).

[33] JV Henderson, 'Externalities in a Spatial Context' (1977) 7 Journal of Public Economics 89.

[34] Georgina Santos and others, 'Part I: Externalities and Economic Policies in Road Transport (2010) 28 Research in Transportation Economics 2; Aaron S Edlin and Pinar Karaca-Mandic, 'The Accident Externality from Driving' (2006) 114 Journal of Political Economy 931; Ian WH Parry, Margaret Walls and Winston Harrington, 'Automobile Externalities and Policies' 373.

and vaccination in that marginal externality of a vaccination can be greater than one case of illness prevented among the non-vaccinated.[35]

There are several forms of externality that are relevant to the software industry: Information asymmetries, lack of competition, principle agent problems, moral hazard and network externalities.[36]

A brief explanation:

Information asymmetry: Where either the buyer or seller knows more than the other does. Akerlof's paper, The Market for Lemons, which uses the used car allegory, explored this thoroughly and is very widely cited.[37]

Principal agent problems: This is when an agent acting on behalf of a principal acts in their own interests, rather than in the interests of the principal (for instance when a bank trades for its own benefit, causing losses or less profit for its clients).

Moral hazard: When the presence of insurance (or another risk mitigation) makes one actor act more riskily than they would have done without it. For instance, wearing a cycling helmet may make someone ride more recklessly than they would if not wearing one.

Network externalities: This is at one level a positive externality. When more users adopt a technology, it benefits all other users. This is defined more precisely as "products for which the utility that a user derives from consumption of the good increases with the number of other agents

[35] Bryan L Boulier, Tejwant S Datta and Robert S Goldfarb, 'Vaccination Externalities' (2007) 7 The B.E. Journal of Economic Analysis & Policy.

[36] Roksana Moore, 'Standardisation: A Tool for Addressing Market Failure within the Software Industry' (2013) 29 Computer Law and Security Review 413.

[37] George A Akerlof, 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism' (1970) 84 The Quarterly Journal of Economics 488.

consuming the good."[38] This theory has been used to analyse the growth of the telephone, railways, software operating systems,[39] social media, SMS[40] and music services[41] amongst others. Network externalities also benefit those that produce complementary products. However, when network externalities are too powerful, they create another set of negative externalities. They crowd out competition and generate lock in, and they create a rush to win market share, at the risk of quality or other attributes.

Virtue signalling: This is a mechanism to help overcome information asymmetries, first suggested by Spence,[42] who noted that in cases of information asymmetries, parties use signals to convey information. He uses the example of qualifications in job interviews. Others have used virtue signalling to explain corporate branding, why banks build imposing offices, sponsor stadiums,[43] or invest in governance policies.[44] The term has developed a pejorative meaning in the press.[45] When this work uses the term, it is using the academic definition.

[38] Michael L Katz and Carl Shapiro, 'Technology Adoption in the Presence of Network Externalities' (1986) 94 Journal of Political Economy 822.

[39] Erik Brynjolfsson and Chris F Kemerer, 'Network Externalities in Microcomputer Software: An Econometric Analysis of the Spreadsheet Market' (1996) 42 Management Science 1627.

[40] Gil Son Kim, Se Bum Park and Jungsuk Oh, 'An Examination of Factors Influencing Consumer Adoption of Short Message Service (SMS)' (2008) 25 Psychology and Marketing 769.

[41] Atip Asvanund and others, 'An Empirical Analysis of Network Externalities in Peer-to-Peer Music-Sharing Networks' (2004) 15 Information Systems Research 155.

[42] Michael Spence, 'Signaling in Retrospect and the Informational Structure of Markets' (2002) 92 American Economic Review 434.

[43] Moore 418.

[44] Karen A Campbell, 'Can Effective Risk Management Signal Virtue-Based Leadership?' (2015) 129 Journal of Business Ethics 115.

[45] See *https://www.theguardian.com/commentisfree/2016/jan/20/virtue-signalling-putdown-passed-sell-by-date*

2.4.1 Externalities in the context of software code

Spam as an example

Spam illustrates the externality concept well. The similarities between pollution as a negative externality and email spam have been explored in detail.[46] Spam is a robust example of a negative externality in that the amount of spam sent far exceeds that which society desires[47] and that the cost of receiving the spam far outweighs the cost benefit of sending it. It has been noted that, in 2010, the Rustock Botnet was responsible for sending a third of the spam that year, and it was estimated that this made the botnet owner roughly 3.5 million US$. The estimate of the cost of fighting spam in 2010 was put at over 1 billion US$.[48] Other estimates put the number higher.[49] Spam creates further negative externalities beyond the mere inbox overload in that spam can serve as a payload for security intrusions leading to identity theft and other costs. Spam was a factor in the survey distribution strategy.

Security weaknesses and safety failures as negative externalities

It is well known that software and the web are insecure, the total cost of that insecurity for society is hard to measure,[50] but the US Council of Economic Advisors estimated that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016. Studies abound listing examples where security issues have led to deaths, injury, financial

[46] Amelia Rickard, Jeffrey Wagner and Jonathan Schull, 'Observations on the Technology and Economics of Digital Emissions' (2017) 48 Technology in Society 28.

[47] Oleg V Pavlov, Nigel Melville and Robert K Plice, 'Mitigating the Tragedy of the Digital Commons: The Problem of Unsolicited Commercial E-Mail' (2005) 16 Communications of the Association for Information Systems.

[48] Ross Anderson, 'Security Economics', *Proceedings of the 28th Annual Computer Security Applications Conference on - ACSAC '12* (ACM Press 2012).

[49] Justin M Rao and David H Reiley, 'The Economics of Spam' (2012) 26 Journal of Economic Perspectives 87.

[50] Ross Anderson and others, 'Measuring the Cost of Cybercrime Motivation A Framework for Analyzing the Costs of Cybercrime Fitting the Estimates into the Framework'.

loss, embarrassment and so on.[51] On any given day, there is a warning of yet another security issue.[52] Software vendors are rarely held liable for the costs of these breaches.

Merely noting that most code vulnerabilities could be avoided through better coding, while accurate, misses the main causes and incentives. Since the early 2000s, researchers have been applying concepts from economics and other disciplines to better understand incentives that will drive or hinder better security. Anderson's work is seminal.[53] He noted information insecurity is at least as much due to perverse incentives, and many of the "problems can be explained more clearly and convincingly using the language of microeconomics: network externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the tragedy of the commons." For instance, moral hazard models have been applied to explain vendor behaviour in vulnerability disclosure.[54]

The CEA report noted:

> *Cybersecurity is a common good; lax cybersecurity imposes negative externalities on other economic entities and on private citizens. Failure to account for these negative externalities results in underinvestment in cybersecurity by the private sector relative to the socially optimal level of investment.*

Security is a significant negative externality and market failure. The costs of security failures are not carried by the makers of software, but by the users and sometimes broader society. This is well known, but the pressing

[51] Schneier; Bruce, 'Information Security and Externalities' (2006) 2 ENISA Quarterly review; David Rice, 'Geekonomics: The Real Cost of Insecure Software' 362.

[52] For instance, at the time of writing this paragraph, the UK intelligence Agency warned of vulnerability issues with smart metres. *http://www.information-age.com/smart-metres-vulnerable-cyber-attacks-123470837/*

[53] Ross Anderson, 'Why Information Security Is Hard - An Economic Perspective'.

[54] Karthik Kannan, 'An Economic Analysis of Market for Software Vulnerabilities' (2004).

question is how to fix it. While this work will not focus on security specifically, it is important to stress that privacy cannot be adequately protected without adequate security.

2.4.2 Externalities in the context of this work

The table below places the externality concepts into context:

Table 2.1: Externalities in context

Externality form	**Examples relevant for this work**
Negative externality	Inaccessible recruitment websites. Loss of privacy, biased algorithmic decision making. Liability dumping. Lack of interoperability for assistive technology tools. (i.e. Kindle v Daisy).
Positive network externality	ERP ecosystem third party tools development, standards adoption. Improved browser accessibility tools.
Network externality chasing	Race to ship. API incompatability.
Moral hazard	Security vulnerability disclosure, data processor behaviour. Over-reliance on check box accessibility (VPAT) or privacy compliance (i.e. Safe Harbor) checks.
Information asymmetry	Product quality awareness, data usage by controller, privacy policy compliance, true product accessibility.
Principal-agent problem	Dark pattern UX development. Audit v consulting revenue.
Positive externality	Payroll vendors providing employment market data. Closed captioning improves video enjoyment for all users.
Virtue signalling	Product certifications, Corporate Social Responsibility (CSR) initiatives.

2.5 Standard and standards

This work is riddled with the mention of standards, for instance WCAG 1.0 /2.0, ISO27001, COSO, COBIT, eXTRA, AS2, AS5, SOC70 to name a few. This work does not propose to provide a detailed assessment of standards history and theory, but it would be appropriate to explore standards, if briefly. The term standard (ironically) has different meanings for different audiences and contexts. There is no standard definition of what a standard is.

2.5.1 Standards from an engineering perspective

Schumpeter noted that standards play an important role in driving industrial growth.[55] It has been calculated that for Germany in the period from 2002 to 2006, the total economic benefit of standardization averaged about 16.77 billion Euros per year.[56] There are over 35,000 DIN standards in Germany. Standards drive growth because they encourage the diffusion of knowledge.[57] Growth doesn't only depend on new ideas, it requires the consistent, rapid dissemination of existing ideas. They codify and commoditize invention. Standards help avoid reinventing things that don't need reinventing. Standardization encourages specialization, and enables economies of scale. Technical standards contribute at least as much as patents do to economic growth. Herewith a definition of an industry standard:

[55] K Krechmer and E Baskin, 'The Fundamental Nature of Standards: Technical Perspective' (2000) 38 Ieee Communications Magazine 70.

[56] Knut Blind, Andre Jungmittag and Axel Mangelsdorf, 'The Economic Benefits of Standardization' (2014).

[57] Eric J Iversen and Richard Tee, 'Standards Dynamics and Industrial Organization in the Mobile Telecom Sector' (2006) 8 info 33; Blind, Jungmittag and Mangelsdorf.

> *A standard can be defined generally as a construct that results from reasoned, collective choice and enables agreement on solutions of recurrent problems. More functionally, an industry standard is a set of specifications to which all elements of products, processes, formats, or procedures under its jurisdiction must conform. The process of standardization is the pursuit of this conformity, with the objective of increasing the efficiency of economic activity.*[58]

Standards, while helping to drive the diffusion of innovation, also have a significant impact on market participation and entry. Standards can have a massive impact on competition, and the tension between standards collaboration and anti-competitive behaviour is addressed robustly in other research [59], and it is not of specific relevance for this work. Standards range from specific product standards, for instance the size of a door in building standards, to the very broad, for instance ISO 9001, which covers quality. See Manders et al who examine the relationship between ISO9001 and innovation.[60] Industry standards can specify outcomes, for instance a product standard for steel purity. Other industry standards are concerned with process. Industry standards can drive interoperability, see for instance Iversen,[61] who examines the dynamics of standards in the mobile communications industry. Werle et al note the challenges relating to the legitimacy of standards, especially in the context of standards developing organizations, and regulative standards.[62] This is especially relevant to the accessibility chapter. Industrial standards play an important role in product safety, and the EU in particular has been a strong

[58] Gregory Tassey, 'Standardization in Technology-Based Markets' (2000) 29 Research Policy 587.

[59] Kei Ishii, 'Code Governance' (Berlin 2005).

[60] Basak Manders, Henk J De Vries and Knut Blind, 'ISO 9001 and Product Innovation: A Literature Review and Research Framework' (2016) 48–49 Technovation 41.

[61] Iversen and Tee.

[62] R Werle and EJ Iversen, 'Promoting Legitimacy in Technical Standardization'.

proponent of standards driven safety, for instance in food safety.[63] The question of product safety is becoming more prominent in software.[64]

The automotive industry provides a useful parallel. For the first 60 years or so, the automotive industry successfully avoided significant safety regulations. The early regulations before the 1960s focused on driver training and road surface safety, and it took the actions of activists, most famously Ralph Nader, to establish a focus on manufacturers improving automotive safety. Regulatory intervention is now common in the automotive industry.[65] In Europe, cars are regulated by general product liability legislation, as well as specific transport safety regulations. The technical standards come via the UNECE (United Nations Economic Commission for Europe), and are applied to car manufacturers. Standards are often global in that US and Japanese manufacturers comply too. In the last 40 years, automotive innovation has continued, while deaths, injuries and emissions have been significantly reduced.

Almost every industry has some form of liability regulation, even those that sell services. Almost all products and services today are embedding software code into their products and services so the pressure on regulators to make software vendors absorb more of their externality will grow. Today, almost all industries have a complex mix of regulation, co-regulation, self-regulation and insurance. While this work will not examine software liability in any detail, it supposes that software manufacturers will eventually have some form of product liability.

[63] Lotte Holm and Bente Halkier, ‘EU Food Safety Policy’ [2009] European Societies.

[64] Ross Anderson, Richard Clayton and Tyler Moore, ‘Security Economics and European Policy’, *WEIS 2008 - Seventh Workshop on Economics of Information Security* (2008).

[65] The recent incidents with emissions avoidance highlight two interesting points. Firstly, that firms may continue to attempt to circumvent regulations, even while they market compliance with those same regulations. Secondly, applying the Lessig architecture metaphor helps explain the deceit. Code lacks transparency, and it is a model case of information asymmetry.

When compared to other branches of engineering, the software industry's adoption and creation of standards has been predominantly opportunistic. For instance, the mechanisms to measure software product quality lack the precision of those in mechanical or electrical engineering. This is in part because of the difficulty in developing such standards, but to date it has not been in the industry's interest to have precise standards, as this would make stronger product liability obligations easier for regulators to enforce more aggressively. As Moore notes, there is a continued lack of clarity for software liability in both tort and contract, partly because there are no effective tests recognized to assess software manufacturers against the legal standards of satisfactory quality or duty of care.[66]

While the software industry uses the term engineering liberally, it has not yet developed the methodological disciplines that characterize other forms of engineering. Shaw noted this was the case in 1990[67], and it is still so today, despite the progress in software development methods. Boehm's work in describing and predicting the evolution of software engineering is insightful.[68] The methods by which software is built remain in flux, for instance in the rapid evolution of agile techniques and methods.[69] This work will argue that some of the negative externalities that software creates are receiving increasing attention from regulators and this will drive an increased focus on standards, for instance with GPDR. The survey will examine software developer awareness of standards.

[66] Moore 428.

[67] Mary Shaw, 'Prospects for an Engineering Discipline of Software' (1990) 7 IEEE Software 15.

[68] Barry Boehm, 'A View of 20th and 21st Century Software Engineering', *Proceedings of the 28th international conference on Software engineering – ICSE '06* (ACM Press 2006).

[69] Sue Black and others, 'Formal versus Agile: Survival of the Fittest' (2009) 42 Computer 37.

2.5.2 Legal standards

When legal theorists talk of standards, typically they mean something different. Legal theorists differentiate between rules and standards.[70] For example, Kaplow notes a rule may prohibit driving at more than 55mph on the expressway. A standard may say don't drive at excessive speeds. The law often uses the term standard in a broad sense, for instance a standard of care, satisfactory quality, a reasonable man. Grimmelmann follows this distinction between rule and standard when discussing the limits of Lessig's code / architecture metaphors (see above). For a legal theorist, this is highly appropriate, but confusing for a software developer or mechanical engineer. What legal theorists are likely to call a rule might be considered a standard by a software developer or engineer. What a legal theorist might call a standard would probably be described as a vague requirement by a programmer.

2.5.3 Accounting and audit standards

Accountants and auditors also make extensive use of standards. Accounting standards developed in part to cope with a problem that Adam Smith identified:

> *The directors of such [joint-stock] companies, however, being the managers rather of other people's money than of their own, it cannot well be expected that they should watch over it with the same anxious vigilance with which the partners in a private copartnery frequently watch over their own ... Negligence and profusion, therefore, must always prevail, more or less, in the management of the affairs of such a company.*[71]

[70] Tassey 558.

[71] Adam Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations* (1776) 311.

Modern economists would describe this is as a principal-agent problem.

Accounting and audit standards aim to increase trust, assess risk, cut costs, encourage innovation, lower the cost of capital and, with international standards, increase international transparency. There are disadvantages to standards too in that they create barriers to entry for smaller audit firms, create new costs, can lead to regulatory capture. Changes in auditing standards play an important role in the chapter on Sarbanes-Oxley.

Of particular interest in this work is where audit and technology standards intersect. An example of this would be ISAE 3402 / SSAE 16. This standard is applied when an organization uses a service provider, to process transactions, host data. The organization needs to test the effectiveness of the service provider's controls. Instead of every company doing unique checks on their supplier's controls, this audit standard is used. Audit requirements, especially after SOX, have helped drive the adoption of IT standards, such as IS027001.

2.5.4 Where law, industry and audit standards meet

Many laws rely on terms such as State of the Art, *Stand der Technik*, *Stand von Wissenschaft und Technik*[72]. In order to elaborate on what the state of the art is, the courts and regulators often rely on industry standards. For instance, German building law and regulation uses the DIN standards to determine appropriate building standards. The ISO27000 series of standards are relied upon by both regulators and the courts to assess adherence to security standards, for instance with Data Protection in Europe, SOX and the Health Insurance Portability and Accountability Act (HIPPA) in the US.[73] Other standards are demanded by public

[72] Alfons Schulze-Hagen, 'Die Bindungswirkung Technischer Normen Und Der Anscheinsbeweis Im Baurechtsprozess' (2005) 65 Festschrift für Prof. Ulrich Werner zum 65. Geburtstag. 355.

[73] Moore.

procurement regulations and laws, for instance, the Federal Information Processing Standards in the US (for encryption), or Section 508 of the Rehabilitation Act for accessibility. Standards can also be used in contracts, to stipulate performance or conformity.[74]

In cases where the standards are well defined, and have a high level of legitimacy, this works effectively. Problems arise, however, when the standards that the courts or regulators adopt don’t reflect the state of the art, or lack input or output legitimacy.

2.5.5 Standards in the context of this work

Standards play an important role in modern society and, when well designed and applied, they serve to encourage innovation and also reduce negative externalities. Lawyers, architects, software developers and auditors all use the term standard, but they are not always referring to the same thing. The effective development, application and enforcement of standards to the software will be a major determinant of how effectively negative externalities such as inaccessibility or privacy loss are minimized. Standards can also have unintended consequences and costs. Table 2.2 illustrates and classifies some of the standards mentioned in this work.

[74] ibid 423.

Table 2.2: Examples of standards, guidelines, etc.

Form	Example
De facto standard	Windows, PDF, navigation methods.
Legal standard	Reasonable care, *Stand der Technik*, informed consent, coercion, fairness, state of the art.
Audit and accounting standards	AS2, IFRS, GAAP, ISAE 3402.
Product standard	WCAG 2.0, CSS, HTML 4, BITV, EN 301 549, DIN18040, Section 508 standards.
Process standard	ISO 270001, ISO 9000, COBIT, ISO 25010:2011, BS 10012:2009.
Industry specific standard	IEC 62304 (medical) DO-178C (aircraft).
Frameworks and governance models	COSO, COBIT, SEI maturity model, NIST Cyber-security framework, ISO 27014, ISO 38500, ITIL, TOGAF.
Guidelines	WP 29 Guidelines on Consent, ICO legitimate interest guidance, ETSI EG 202 115.
Code of Practice	ICO COP conducting PIA.

2.6 Summary: Definitions and context

This chapter provided a brief overview of code is law, enterprise software, externalities and standards. These concepts provide the foundation to explore how enterprise software aids and hinders compliance.

3 Empirical Survey Design

3.1 Chapter purpose: Empirical survey design

This chapter describes the survey design, providing some background into the survey design and the purpose behind the questions.

3.2 The purpose and design of the software developer survey

The starting point for this research was the anecdotal observation that most software developers have a very limited understanding and awareness of the legal issues that relate to software. This is articulated more formally in the research question: What do software developers understand about the law that relates to software?

In order to explore this question, a survey was designed and administered. The decision to design and deploy using a standard on-line tool and leverage social media as a distribution channel is explained and justified below.

The internet is an attractive mode of data collection to survey researchers due to cost savings and timeliness in comparison with other modes.[1] Web-based survey usage has grown dramatically in practitioner led surveys, and by 2004 it was estimated that at least one third of market research is conducted through on-line surveys.[2] Since then, the web has

[1] JA Dever, A Rafferty and R Valliant, 'Internet Surveys: Can Statistical Adjustments Eliminate Coverage Bias?', *Survey Research Methods* (2008).

[2] Stephane Ganassali, 'The Influence of the Design of Web Survey Questionnaires on the Quality of Responses' (2008) 2 Survey Research Methods 21.

become the dominant method of survey distribution. See also Couper[3] for a thorough examination of on-line survey growth and design.

Ganassali considers that web surveys are especially well adapted to internal surveys (staff evaluation or social satisfaction), to access panels and more generally to a well identified target population, particularly in a Business-to-Business context[4]. The target population of the survey is relatively well defined and falls into the business-to-business context. Andrews notes that electronic surveys have distinctive technological, demographic and response characteristics that affect their design, use and implementation. Survey design, participant privacy and confidentiality, sampling and subject solicitation, distribution methods and response rates, and survey piloting are critical methodological components that must be addressed.[5]

3.2.1 Advantages of an online survey

There are a number of advantages in using an online survey, mentioned briefly in Table 3.1.

[3] MP Couper, MW Traugott and MJ Lamais, 'Web Survey Design and Administration' (2001) 65 Public Opinion Quarterly 230.

[4] Ganassali.

[5] Dorine Andrews, Blair Nonnecke and Jennifer Preece, 'Electronic Survey Methodology: A Case Study in Reaching Hard-to-Involve Internet Users' (2003) 16 INTERNATIONAL JOURNAL OF HUMAN–COMPUTER INTERACTION, 185.

Table 3.1: Advantages of online surveys

Advantage	**Explanation**
Reach	The online survey takes advantage of the internet to provide access to groups and individuals who would be difficult, if not impossible, to reach through other channels.
Time	Online surveys allow researchers to reach thousands of people in a relatively short period of time.
Cost	Other than the cost of the subscription to the survey tool, the survey has had no direct financial costs.
Response collation and user check	Web-based survey tools automatically collate responses in a database and rules can be set to stop multiple entries by a user.
Metadata collection	Modern tools collect useful metadata, such as the IP address, time to complete, entry source. This makes for a richer result set. For instance, an IP address can be used to verify locational data collected in the survey.
Ongoing monitoring	The online tools enable researchers to monitor the survey as it is running. This enables them to pick up issues with the questionnaire with early participants. If the problems are significant, they can stop the survey and re-run it. This option would not be available with a postal survey.
Pilot testing and peer review	It is good practice to test and pilot the survey before launching it, and modern survey tools make this a relatively simple process. The survey can be piloted with a broader and more dispersed sample than would be the case with paper surveys. The tools also enable versioning.
Data sharing	Modern survey tools allow sharing of results and data sets to enable further research and validation.

3.2.2 Disadvantages

Wright also notes several disadvantages of online survey research.

A common concern is that online surveys have a demographic bias in that by definition participants need to be online. Samples can be biased, as those without access are excluded. In the case of this survey, the target population is software developers. It is safe to assume that the vast majority of developers do have Internet access and are proficient with online forms. So, this concern can be discounted.

Other disadvantages include:

- Researchers know relatively little about the characteristics of the respondents in an online survey.
- Finding valid email lists is difficult.
- The dispersed nature of an online survey means that the researcher can never be quite sure who clicks on it.
- When subjects are recruited by targeting newsgroups or search engines, it is nearly impossible to determine the distribution of the sample population.
- These survey procedures should be used only when sampling and self-selection biases can be tolerated[6].
- As a result of the inability to identify all on-line users, web-based surveys do not provide generalizable results, due to self-selection, non-random and non-probabilistic sampling.[7]
- Self selection bias is also a challenge. In any given community, there are individuals who are more likely to complete the survey.
- There are also problems with using incentives to encourage participation.[8]

[6] Titus Schleyer and Jane Forrest, 'Methods for the Design and Administration of Web-Based Surveys' (2000) 7 The Journal of the American Medical Informatics Association 416.

[7] Ganassali.

[8] Kevin B Wright, 'Researching Internet-Based Populations: Advantages and Disadvantages of Online Survey Research, Online Questionnaire Authoring Software Packages, and Web Survey Services.' (2005) 10 Journal of Computer-Mediated Communication 0.

3.3 Survey design and survey execution

3.3.1 Choice of tool

SurveyMonkey was chosen as the survey tool, based on successful personal experience and feedback from colleagues, who had used the tool on a significant scale for larger and more complex surveys. The tool is well established in the market. For the survey, a professional version was licensed so as to have improved control of the HTML layout, better analytics and unlimited survey participants. Web-based survey tools have existed since the early 1990s and they are now in widespread use.

A formal tool selection process, as suggested by Andrews et al[9] was deemed unnecessary. Nevertheless, the tool meets the requirements they lay out below.

Survey design quality criteria:

- Supports multiple platforms and browsers/e-mail clients
- Controls for browser settings
- Detects multiple submissions automatically
- Presents questions in a logical or adaptive manner: for example, provides control of when and how questions are displayed
- Allows responses to be saved before completion
- Collects open-ended and quantified-option responses
- Provides automatic feedback upon completion
- Uses paper questionnaire design principles
- Provides automatic transfer of responses to a database
- Prevents survey alteration
- Provides response control and economical displays

[9] Andrews, Nonnecke and Preece.

- Provides for links to definitions, menus, button and check box options, animation, sound, graphics options and so forth
- Does not require familiarity with survey presentation software
- Displays appear quickly to participant
- Tracks response source of response failure

Andrews et al do not mention accessibility as a design requirement. The literature review of online survey research found very little mention of accessibility in on-line survey design. Harper does make a brief mention of accessibility, but this is the exception.[10]. Additionally, if selecting a survey tool today, the author suggests that adequate mobile device support would be an essential requirement.

3.3.2 Survey pilot and testing

A testing and pilot approach as per Andrews et al was followed.

- Colleague test
- Cognitive test
- Live test
- Clean up

This was done over a period of several weeks. The pilot exercise was useful as it identified some questions that were confusing and it picked up several formatting errors. The survey was also tested on several second language English speakers, namely German, French and Spanish native speakers. They were able to point out some places where explanations were awkward to follow. The survey was also tested across the major browsers. No technical issues were found with the tool. The test did not capture all design failings and these are discussed in the review of the questions below, see for instance Question 24, discussed in the analysis chapter.

[10] Simon Harper and Yeliz Yesilada, *Web Accessibility: A Foundation for Research* (Springer UK 2008).

3.3.3 The spam filter challenge

Through prior experience with the tool, the author was aware that mass emailing was ineffective to some corporate email addresses. Many corporate spam filters are very aggressive, and one of the disadvantages of using an off-the-shelf tool is that many others use it too. So spam filters sometimes treat academic surveys as spam. The software survey tool company is aware of this issue, but does not suggest a solution.[11]

The challenges of spam filters in research are noted by Fan[12] and Fricker et al .[13] Mass mailings from the survey tool were not used for this survey. No one reported issues of the survey tool site being blacklisted by corporate systems administrators, but this can be a risk when the respondents attempt to access the survey at work.

3.3.4 Defining the target population

This research did not formally define a survey frame other than enterprise software developers. The target population is described in the introductory description of the survey.[14]

[11] If you choose to use our mail server for survey distribution, there is the chance that your recipients' networks may automatically send the message to a SPAM or junk folder. Their networks may have email filters that look for specific words in the message. Since SPAM filters can be configured to be as restrictive as possible and unless you know the specific filter configuration for each recipient, there is little you or SurveyMonkey can do to prevent a message from being filtered out as probable SPAM. http://help.surveymonkey.com/app/answers/detail/a_id/226

[12] Weimiao Fan and Zheng Yan, ‘Factors Affecting Response Rates of the Web Survey: A Systematic Review’ (2010) 26 Computers in Human Behavior 132.

[13] Ronald D Fricker and Matthias Schonlau, ‘Advantages and Disadvantages of Internet Research Surveys: Evidence from the Literature’ (2002) 14 Field Methods 347.

[14] See Appendix A

3.3.5 Limitation awareness

The survey was never assumed to be probabilistic in that the results and findings can be extended beyond the respondents with any precise statistical confidence. The survey is largely descriptive in nature and while the statistical analysis exposes some potentially useful correlations, for instance between employer size and accessibility focus, the goal is not to prove causality. There are some additional issues of bias because of the author's work profile at Gartner and SAP. At the time of the survey, the author worked for Gartner. This may have influenced some of the responses on how participants rate their organization.[15]

3.3.6 Applying a web 2.0 approach to survey distribution

At the time of designing and delivering the survey (2009), academic research largely focused on using email to distribute access to an electronic web form.[16] In order to publicize the survey to the target audience, an alternative to the mailing list approach was used. Extensive use of blogging, Twitter and, to a lesser extent, LinkedIn and Facebook was used to notify the target audience of the survey, its purpose, and invite them to participate.

Blogging has become an effective mechanism of communication,[17] and many software developers are active social media users, and see social media as a useful tool for their work.[18] The author started a blog, mainly

[15] Gartner evaluates software company products and performance. See *www.gartner.com*

[16] Couper, Traugott and Lamais.

[17] Chin Lung Hsu and Judy Chuan Chuan Lin, 'Acceptance of Blog Usage: The Roles of Technology Acceptance, Social Influence and Knowledge Sharing Motivation' (2008) 45 Information and Management 65.

[18] Sue Black, Rachel Harrison and Mark Baldwin, 'A Survey of Social Media Use in Software Systems Development', *Proceedings of the 1st Workshop on Web 2.0 for Software Engineering - Web2SE '10* (ACM Press 2010).

about information technology, and at the time of the survey it had roughly 300 readers a day, most of whom worked in the software industry. This was used to launch the survey.[19] The survey was also seeded with a number of other influential bloggers who cover topics of interest to the target group. They publicized the survey.[20]

While the survey didn't go viral in the sense of it receiving thousands of responses, it gathered over 500 completed responses with a strong fit to the target profile of the enterprise focused software developer.

For future surveys, a more structured use of Twitter with #tags and "tweet this" widgets, etc. would be recommended. At the time of survey development, the literature search did not find any academic research pointing to best practice for using social software for survey distribution. The survey tool providers are now making it easier to leverage these new channels, and Twitter and other social media platforms have garnered significant research attention.

3.3.7 Use of free-format text

The survey design made extensive use of free-format text, but largely made those questions voluntary. A significant portion of the survey respondents filled in the free-format texts. This indicates a relatively high

[19] See *http://theotherthomasotter.wordpress.com/2009/01/03/launching-a-survey/*

[20] *http://blogs.gartner.com/debbie_wilson/2009/01/07/software-development-and-the-law-an-opportunity-to-contribute-to-research/*
http://discuss.joelonsoftware.com/default.asp?biz.5.726142.3
http://www.redmonk.com/cote/2009/01/12/developers-and-the-law/
http://nigeljames.wordpress.com/2009/01/07/software-and-the-law/
http://electromate.blogspot.com/2009/01/seeking-views-of-software-developers.html
http://www.redmonk.com/jgovernor/2009/01/09/developers-and-privacy-questions-code-quality-and-business-process/
http://thingamy.typepad.com/sigs_blog/2009/02/software-developers-and-vendors-a-request.html
http://opendotdotdot.blogspot.com/2009/01/take-this-survey-its-law.html

level of engagement. Although the free-format text is more time consuming to analyze than multiple choice answers, the survey population is of a manageable size, and every comment was read. Modern text analysis tools can help with large-scale sentiment analysis, but these were not deployed with this survey. The free-format comments can reinforce or challenge the structured question responses and provide a deeper view of the software developer perspective, which is the goal of the survey. The comments also helped point out some weaknesses in the survey design, discussed below.

3.4 A detailed description of the survey questions and their purpose

This section will list the survey questions, describe and provide insight into the purpose of the questions, and mention some of the methodological weaknesses in the survey.

3.5 Survey introduction

The text introduction to the survey is important in order to:

- Explain to the participants the purpose of the research
- Define the target audience
- Enable those reading the introduction to decide on participation or not
- Establish that this is not related to the author’s employment research

The introductory text can be seen in Appendix E.

3.6 Biographical / organizational data

Given that the survey was not being distributed to a known audience, it was essential to gather biographical data so that it would be possible to understand the background of the persons answering the survey. In hindsight, the analysis options would have been stronger had there been fewer multiple selection fields (for instance Questions 6 and 7). While the multiple selection fields provided strong descriptive granularity, it made those data items unsuitable for more advanced statistical analysis.

Table 3.2: Biographical survey information questions

Question number	**Topic**	**Question**
1	Education	Describe the formal tertiary education you have received where a significant part of that education focused on software development / information technology.
2	Education	In which country did you study?
3	Education	Major
4	Professional certifications	Do you hold any professional certifications, such as Microsoft certified professional, Oracle certified professional, SAP, Java, Cisco?
5	Professional membership	Are you a member of any software development related formal professional body? Such as the IEEE, ACM, GI (Gesellschaft für Informatik) or BCS (British Computer Society)?
6	Work experience	Describe your role in software development. You can click on more than one answer. • Programming • Business analysis • Architecture • Testing/Quality designing • Technical specification writing • Documenting • Project management • Technical administration

		• User interface expert/usability • Managing /Executive • Product configuration (e.g. ERP consulting) • Solution management • Product management • Product marketing • Other (please specify)
7	Employer type	What sort of organization do you work for? You can select more than one answer. • A software company • A consulting company (systems integrator for instance) • An applications hosting company (such as a BPO provider) • An IT department • Research institution (university research lab for instance) • Self employed
8	Development organization size	Roughly how many people work in “software” in your organization – i.e. how big is your “development” organization?
9	Organization type	How would you describe the software your organization builds or implements? • Enterprise software (software that companies use) • Consumer software • Other
10	Software experience	How long have you been working in a software related role?
11	Work location	In which country do you currently work?

3.7 General legal knowledge section

Table 3.3: General legal knowledge survey questions

Question number	Topic	Question
12	Legal knowledge	Either during your work, or as part of your education, have you received any formal training in the following areas? Contract law Software liability Software licensing models Privacy and data protection Industry standards (ISO standards for instance) Copyright Patent Trademark Accessibility (For instance for partially sighted users.)
13	Legal knowledge	Please rate your level of knowledge of the following: (5-point scale) Contract law Software liability Software licensing models Privacy and data protection Industry standards (ISO standards for instance) Copyright Patent Trademark Accessibility (For instance for partially sighted users.)

The purpose of this section is to gather information regarding education respondents have received on legal topics, and a self-assessment of their knowledge level. The goal was to cover a broad range of topics relevant for software developers. The topics were kept consistent throughout the survey. The textbook *Professional Issues in Software Engineering*[21] provided an inspiration for this element of the survey.

[21] Frank Bott and others, *Professional Issues in Software Engineering* (3rd edn, Taylor & Francis Group 2001).

Table 3.4: Legal concepts relevance

Legal concept	**Relevance**
Contract law	Contract law underpins almost all commercial relationships. Software development contracts have specific nuances, for instance, who owns the copyright? Code may also be placed in escrow as part of the contract. While in large software companies, contract issues are typically remote to developers; for those in start ups or who operate as contractors, understanding contractual obligations is critical.
Software liability	This relates closely to contract. Software liability is very complex, and is sometimes a matter for dispute. Limited liability clauses have been a matter of significant confusion in the courts, especially in the context of large software projects, see St Albans v ICL.[22] Questions such as who is liable for data security breaches are critical, especially in the context of cloud computing. Liability is a well-established concept in other professions, such as architecture, mechanical engineering, law and medicine, but its position with software is far from resolved. In the US, the US Uniform Commercial Code has struggled to define whether software is a good or a service.
Software licensing models	Again, this relates to contract. There is a variety of software licensing models: on-premise, perpetual licence, open-source, etc.
Privacy and data protection	This field is particularly relevant for the data protection section in the research. The terms privacy and data protection were both used, as while they are not completely analogous in law, privacy is the more commonly used term in the US. Data protection is more common in Europe. At the time of the survey creation, the EU Data Protection Directive was the most significant legal instrument.
Industry standards	Industry standards play a vital role in software and other forms of engineering: for instance, ISO27001 or the WCAG accessibility standards, or specific industry standards, such as DEF-STAN 00-55, which relates to software safety in defence applications, and EUORCAE in aeronautics. In other disciplines, such as architecture and mechanical engineering, students and practitioners are taught about standards, and are required to keep up to date. Standards play an important role in product quality.

[22] St Albans City and District Council v ICL [1996] EWCA Civ 1296 (26 July 1996) available at *http://www.bailii.org/ew/cases/EWCA/Civ/1996/1296.html*.

Copyright	Computer programs and compilations of computer programs are protected as literary works. Key questions for software developers include when is decompilation for the purposes of interoperability allowed. An incorrect interpretation of copyright can have major implications for software companies. In enterprise software, disputes over third party maintenance have been fraught, see the Oracle v SAP Tomorrow Now[23] case. Another example of an enterprise software related copyright case is SAS Institute v World Programming LTD.[24] The long running Oracle v Google case relating to APIs is also relevant, and relates closely to the questions on third party web service consumption.
Patent	Over the past 30 years, it has become common to seek patents for software. Software developers should ideally be aware of what to patent and what not to patent.
Trademark	While not as complex as either patent or copyright, a trademark is an important component of intellectual property. Naming a product incorrectly can lead to significant problems and costs. A trademark is also important in the context of domain name disputes. Typical questions would be when would trademark registration be appropriate? Issues of passing off can be a problem when the branding of an implementation partner implies that the service comes directly from the vendor.
Accessibility	Software accessibility means that people with disabilities can use software. More specifically, software accessibility means that people with disabilities can perceive, understand, navigate and interact with the software. Various laws around the world encourage and enforce this accessibility.

[23] See *https://dockets.justia.com/docket/california/candce/3:2007cv01658/190451/* and *https://www.reuters.com/article/us-oracle-sap-se-settlement/oracle-sap-settle-long-running-tomorrownow-lawsuit-idUSKCN0IX2RJ20141113*

[24] See C-406/10 SAS Institute v World Programming Ltd. (WPL). *http://curia.europa.eu/juris/document/document.jsf?docid=122362&doclang=EN*

3.8 Data protection and organization perceptions

The data protection section aims to:

- See if those answering the survey work directly with personal and/or sensitive data
- Gather their perception of how they see their employer approaching privacy
- Provide a more detailed check of Data Protection law knowledge

Expecting employees to evaluate their employers without bias in a survey that is not totally anonymous is problematic so the reliability and validity of Questions 16 and 17 is doubtful as an absolute measure and will be treated with some circumspection.

While the education section had asked about privacy knowledge in a general sense, focusing on the Data Protection Directive in Question 18 tests that knowledge more directly. For instance, someone who states that they have good privacy knowledge but no awareness of the Directive would likely be overstating their knowledge. Also, someone developing systems that manage personal data who has not received training on the Directive, yet states that their organization sees privacy as a competitive advantage, is likely to be overstating their organization's commitment. This question is fundamental to understanding what software developers know about privacy law. The Directive is fundamental to understanding data privacy so a lack of awareness would help answer the research question, at least in the context of privacy and data protection.

Table 3.5: Data Protection knowledge and organization perceptions

Question number	Topic	Question
14	People data	Do you build, design or maintain applications that process data about people (data items such as name, address, email, phone number and so on)?
15	Sensitive data	Do you build, design or maintain applications that process sensitive data? For instance political memberships, religion, sexual orientation or data relating to children.
16	How does your organization approach privacy?	Which statement best describes your perception of how privacy and privacy law affect product development process in the organization? We see building privacy into our products as a competitive advantage and we pro-actively focus on privacy. We have a sound knowledge of privacy law, and we have policies and methodologies in place that ensure that our development practices are privacy aware. Privacy is sometimes considered in product design, but it is an ad hoc process. Privacy is largely ignored in our product design and processes. Privacy is actively avoided in our product design. We collect as much data as we can, even though some of it might be illegal.
17	Benchmark	How do you perceive your organization's development practices with regards to privacy compared with other organizations in your industry? More focus on privacy About the same Less focus Don't have an opinion
18	EU DP knowledge	The EU Data Protection Directive. It forms the basis for data privacy law in all countries that are members of the European Union, and has had a significant influence on privacy law in many other countries. It is sometimes known as the "EU Privacy law", although not officially. National implementations of the Directive include the UK Data Protection Act and the German Bundesdatenschutzgesetz. (If you need

		more background information, see here. It will open in a separate window.) How did you learn about the Directive or the national level legislation? I have had training in it at work or as part of my education I've read about it in the press or on the web I've no idea what you are talking about

3.9 Web service risk perception

Software is not made up of a single component, and software developers must rely on code delivered by others to build solutions today. Even large vendors do not control the complete development stack and software increasingly depends on services from third parties. This section of the questionnaire aims to assess developer awareness and perceptions of the risks of consuming those services. At the time of writing, SOA was a widely used term to describe software architecture that uses services.

The section begins with an introductory definition.

> *Service-Orientated Architectures are a way of developing distributed systems where the components of these systems are stand alone services. These services may execute on geographically distributed computers. A service is a loosely coupled, reusable software component that encapsulates discrete functionality, which may be distributed and programmatically accessed.*
>
> *A web service is a service that is accessed using standard Internet and XML-based protocols. (Sommerville, Software Engineering, 2006)*

Over the last few years, consuming web services built by others has grown dramatically. Obvious examples include mashups, such as with Google maps, but SOA is becoming widely used across many types of software.

I would like you to think of a scenario where your organization is building a business process, partly made out of components delivered by third parties via a service architecture. These services exchange data and run transactions (book a hotel, calculate a route, calculate tax, for instance).

Now I would like you to consider the risk of consuming these third party services.

Table 3.6: Third Party Service consumption risk

Question number	**Topic**	**Question**
19	Service risk perception	Please assess the risk of using services built by other organizations in solutions that you deliver. Please rate the risk of using services in the following matrix: Contract Liability Licensing Privacy & Data Protection Industry standards Copyright Patent Trademark Accessibility Across the matrix of: Critical risk Risk Minor risk Irrelevant Don’t know
20	Service risk organization	Do you believe that your organization adequately assesses the risks of consuming third party web services?

3.10 Accessibility

Accessibility: This section begins by defining accessibility. Feedback in the pilot survey recommended defining accessibility more clearly and extensively. The following definition was added:

> *Accessibility, in a software context, is the ability of disabled people to access the application or website. This right is governed by various laws across the world:*
>
> *US: The Americans with their Disabilites Act, Section 508 of the Rehabilitation Act*
>
> *UK: The Disability Discrimination Act*
>
> *Germany: Barrierefreie Informationstechnik Verordnung – BITV*
>
> *Accessibility is often linked to standards, such as those from W3C. The most recent ones are available here. (link).*

In hindsight, it would have been appropriate to ask other accessibility related questions, especially given the greater focus on accessibility in this dissertation than was originally intended.

Table 3.7: Accessibility knowledge and organization approach

Question number	**Topic**	**Question**
21	Accessibility organization	Select the paragraph that best agrees with how your organization approaches accessibility: We design accessibility into our products, and consider building accessibility a moral obligation. We actively take into account accessibility standards in our products, even if the law doesn't force us to. We build accessibility into the product when we aim it at a market with strong legal accessibility rules (i.e. the US public sector). We retrofit accessibility into the product when threatened with legal action. We largely ignore accessibility issues in our product design and build. I'm not close enough to the accessibility issue to answer this.

3.11 General legal issues

This section explores at what point in the software development cycle do participants believe legal risks and issues should be assessed. The phases of software development remain roughly the same, irrespective of development methodology, so this would apply to the classic waterfall, agile or a hybrid development model. For instance, is accessibility considered in up front design or only as a testing issue at the end of development?

Of particular interest is whether organizations have experts that understand the legal implications to advise software developers. The expectation is that larger organizations are more likely to provide specialist support.

Table 3.8: General legal questions

Question number	Topic	Question
22	When to assess	At what stage do you feel legal risks and issues should be assessed in the software development cycle? (You can select more than one): Conception Design Build Test Maintain Never
23	Use of experts	My organization employs/uses experts who help developers understand the legal implications of software development. Yes No Don't know

Table 3.9: General legal questions continued

Question number	Topic	Question
24a	Legal implications	Software technology is increasingly impacting how we live, and actions in code can have real-world legal implications.
24b	Understanding	I clearly understand the legal issues that impact designing, building and maintaining software.
24c	Responsibility	I see it as part of my professional responsibility to keep up to date with the legal issues that relate to software.
24c	Knowledge	I have some knowledge of the legal issues that relate to software.
24d	Knowledge	I have a vague knowledge of the legal issues that relate to software.
24e	Interest	I have no interest in legal issues. The law is irrelevant and doesn't impact my job.

Question 24 has a number of design flaws.

- It should have been split into separate questions, each with their own free text comment box. This would have improved usability. Several respondents commented to that effect.
- 24c and 24d are too similar, and created confusion.
- The use of a 5-point Likert scale also created some confusion, as in hindsight some of the questions could have been better answered with a simple yes or no selection. It also made the data analysis unnecessarily complicated, as the ordinal nature of the Likert scale requires more sophisticated statistical techniques to analyze.

These issues will be discussed further in the analysis section.

3.12 Training adequacy

Table 3.10: Training adequacy

Question number	Topic	Question
25	Training	Do you believe that you receive enough formal training, either as part of your studies or as part of your professional development at work on the legal issues that impact software? Too much Enough Not enough Not relevant

Do software developers feel adequately educated? As part of the research, a brief analysis of computer science curriculae highlighted the lack of training in legal issues and this question serves to explore that further.

3.13 Wrap up

Table 3.11: Wrap up

Question number	Topic	Question
26	Wrap up	Would you be prepared to do a more detailed interview by phone? We will select a small sample for this.
27	Wrap up	Would you like a copy of the final research paper?
28	Wrap up	Thanks again for your time and effort. If you want to make any general comments about the survey, please go ahead. I will read them!

A PDF copy of the survey is attached as Appendix E.

3.14 Analysis approach

Most of the data analysis is descriptive in nature. Some additional statistical analysis was done in order to seek out correlations, for instance by geography, education level, industry certification, and organization size. It is appropriate to note that the author had assistance with the statistical calculations.

4 Survey results analysis

4.1 Chapter purpose: Survey results analysis

The primary goal of the survey is to explore the research question: What do software developers understand about the law that relates to software? This section will provide analysis and commentary on the results of the survey. The majority of the analysis is descriptive in nature.

4.2 Demographic characteristics

4.2.1 Country of study and country of work

There was a total of 590 respondents, of whom 539 indicated the country in which they completed their studies. There were 51 different countries indicated by the respondents, of whom the largest percentage of respondents (35.1%) was from the United States, followed by respondents from the United Kingdom (14.3%), Germany (8.7%), India (6.3%), Australia (4.3%), South Africa (4.1%) and Canada (3.5%). Five hundred and thirty-five respondents indicated the country where they currently work, for a total of 48 countries. Similarly to the country where they completed their studies, the largest percentage of respondents indicated they work in the United States (38.3%), followed by respondents from the United Kingdom (14.0%), Germany (9.5%), Canada (4.1%), Australia (3.9%) and India (3.7%). The results are illustrated in Figure 4.1.

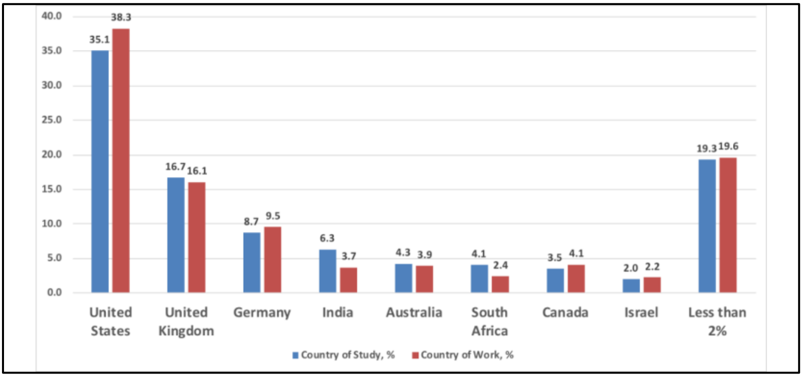


Figure 4.1: Country of work / country of study distribution

There was a total of 500 respondents who indicated both the country where they completed their studies and the country where they currently work. Of these, the majority of 411 (82.2%) work in the same country as the country where they completed their studies.

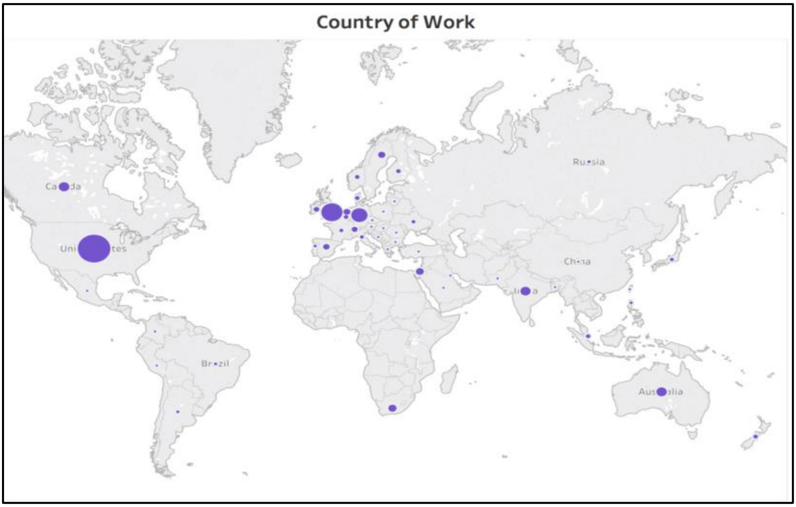


Figure 4.2: Map of country of work

4.2.2 Commentary on country distribution

The country distribution highlights two useful points:

- The sample distribution is relatively broad across countries, and the relatively high response from the US goes someway to alleviate the author's concern that there would be a significant selection bias towards people that know him. (Again, the goal is not to formally extrapolate the results beyond the survey population).
- While the differences between country of study and country of work are generally not large, some evidence of migration flows between countries can be noted. There is a strong outflow of trained people from India and South Africa, and an inflow into the US, Canada and Germany. Software developers can relatively easily move countries and begin work in the new country immediately, unlike some other professions, which may require local certification.

4.2.3 Educational background

The respondents were asked to describe the tertiary education they received, where a significant part of that education was focused on software development/Information Technology. There was a total of 704 responses, with most respondents indicating that they received a university degree (45.9%) or a post-graduate degree (24.9%). There were 83 respondents (11.8%) who did not have any tertiary education. Other responses included formal degree, a degree that was not related to Information Technology, community college certificate, workshops, books, on-the-job training, self-taught, and several certification courses such as SAP. Nine respondents chose not to answer the question. The tabulated responses are presented in Table 4.1.

Table 4.1: Formal tertiary education

Formal Tertiary Academic Education of Respondents Based on a Multiple Answer Question (N = 704)			
Tertiary Academic Education	Responses		Percentage of Cases
	N	Percent	
University degree (Bachelors)	323	45.9%	55.8%
Post-graduate degree (Masters or Doctorate)	175	24.9%	30.2%
Technical college	41	5.8%	7.1%
Specialist programming school	25	3.6%	4.3%
Other	57	8.1%	9.8%
None	83	11.8%	14.3%

489 respondents indicated their first major, with computer science as the most indicated major (26.38%), mathematics (3.89%) and physics (4.09%). Computer science (14.29%), physics (1.7%) and mathematics (5.53%) were marked as the most common second majors, while the third major had computer science (8.45%) and mathematics (11.27%) as the most common degrees. There were 217 respondents who indicated their second major and 71 respondents who indicated their third major.

With regards to any professional certifications, such as Microsoft certified professional, Oracle certified professional, SAP, Java or Cisco, there were 143 respondents (25.4%) of 563 respondents who answered affirmatively. When asked to describe the certification in more detail, 135 respondents provided more details. The most common certifications were SAP (22.96%) and MCP (9.63%).

Most respondents were not part of any software development related formal professional body such as IEEE, ACM, GI or BCS, with 111 (19.8%) of 560 respondents answering affirmatively to this question. Of the 102 respondents who chose to give more details, some respondents were part of the ACM (38.24%) and IEEE (15.68%) professional bodies.

4.2.4 Commentary on education and certification

The majority of those responding have had significant education in computer science or related subjects. Direct software certification responses illustrate the enterprise software focus of the respondents. Despite the relatively high level of academic qualification, the low levels of professional body membership illustrate the failure of professional bodies to gain traction with the respondents. Many other professions, for instance mechanical engineering, law, architecture and so forth, have a much higher level of professional membership. This is illustrative of the relative immaturity of the software industry and the lack of regulatory or self-regulatory control of the software developer role / profession.

4.2.5 Roles in software development

The respondents were asked to describe their role in software development. There was a total of 2984 responses, with most respondents indicating that they were programming (12.8%), designing (11.2%), or working on architecture (10.2%). Other responses included being involved in everything, consulting, competitive sales, internationalization and localization, research, process monitoring, support, visionary and presales. 52 respondents chose not to answer the question. The tabulated responses are presented in Table 4.2.

Table 4.2: Role in software development

Role in Software Development as Indicated by the Respondents			
Role	Responses		Percentage of Cases
	N	Percent	
Programming	381	12.8%	70.9%
Business analysis	249	8.3%	46.4%
Architecture	305	10.2%	56.8%
Testing/Quality	232	7.8%	43.2%
Designing	335	11.2%	62.4%
Technical specification writing	204	6.8%	38.0%
Documenting	212	7.1%	39.5%
Project management	263	8.8%	49.0%
Technical administration	110	3.7%	20.5%
User inference expert / usability	155	5.2%	28.9%
Managing/Executive System	155	5.2%	28.9%
Product configuration (for instance ERP consulting)	72	2.4%	13.4%
Solution management	100	3.4%	18.6%
Product management	132	4.4%	24.6%
Product marketing	79	2.6%	14.7%
Total	2984	100.0%	555.7%

4.2.6 Commentary on the roles in software development

The multiple choice nature of this question, while it is useful in describing the respondent population very precisely, has meant that this data would not be useful for slicing the responses of the later questions, which is unfortunate. However, the data shows that the vast majority of respondents are closely involved in the process of writing and developing code. It also clearly highlights that the survey has attracted the sort of respondents it was hoping to attract. Those who answered that they performed multiple roles work for smaller organizations or independently (this was validated by a line item review of some those respondents).

4.2.7 Organizational type, size and software segment

When asked what sort of organization they worked for in a multiple answer type of question, most respondents indicated a software company (42.7%), followed by a consulting company (21.6%) and self-employed (14.4%). Other responses included a communications company, a non-profit volunteer Open Source software project, a computer hardware company, unemployed, equipment manufacturing, food delivery, financial services, marketing company, IT research company, manufacturing, a newspaper, the government, university, wireless ISP and student. 48 respondents chose not to answer this question. The results are presented below.

Table 4.3: Organization type

Type of Organization where Respondents Work Based on a Multiple Answer Question			
Company	Response		Percentage of Cases
	N	Percent	
A software company	279	42.7%	54.6%
A consulting company	141	21.6%	27.6%
An application hosting company	34	5.2%	6.7%
An IT department	74	11.3%	14.5%
A research institution	31	4.7%	6.1%
Self employed	94	14.4%	18.4%
Total	653	100.0%	127.8%

Most people worked in a company with few people in the software development department - between 0 and 19 employees - (42.1%), followed by large departments of over 2500 employees (23.2%) and small departments of 20 to 99 people (17.4%). The median response was between 20 and 99 people in the software development department. There were 56 respondents who chose not to answer this question. The results are presented below.

Table 4.4: Number of employees in software development

Number of Employees in the Respondents' Organization in "software development"			
Number of Employees	Frequency	Percent	Valid Percent
0-19	225	38.1	42.1
20-99	93	15.8	17.4
100-249	29	4.9	5.4
250-499	18	3.1	3.4
500-999	24	4.1	4.5
1000-2499	21	3.6	3.9
> 2500	124	21.0	23.2

When asked to describe the software their organization builds or implements, in a multiple answer type of format, there were 623 responses. The majority of respondents indicated that they would describe the software in their company as enterprise software (71.1%), followed by consumer software (19.6%) and other (9.3%). Descriptive responses included a common database and enterprise framework, business process management, business to business, customization to vendor software, educational software, enterprise software for the public sector or on the web, ERP, financial markets, game development, GIS, healthcare information systems, hospital patient administration systems, internal facing applications, software for artists, online bingo, productivity software and point of sale (POS), research prototypes, SaaS, SAP, SMB, software for NGOs, spatial

ETL, telecom, university level learning management systems and websites and web applications.

4.2.8 Commentary on organization type

This section further confirms that the respondents are the desired target population. The respondents work on a broad range of software solutions, and there is broad distribution across differing sizes of organization. If the survey was to be run today, the differentiation between application hosting and software company would be unnecessary, as this would simply have been subsumed into one, given the shift to cloud computing.

4.2.9 Work experience

The respondents indicated that they had mostly worked between 10-20 years (38.4%) in their software related role, followed by 5-10 years (28.6%) and more than 20 years (16.9%). The median number of years worked in a software role was 10-20 years. There were 51 respondents who chose not to answer this question. The results are tabulated below.

Table 4.5: Experience in software role

Number of Years Worked in a Software Related Role			
Number of Years	Frequency	Percent	Valid Percent
0-1 year	11	1.9	2.0
1-2 years	17	2.9	3.2
2-5 years	59	10.0	10.9
5-10 years	154	26.1	28.6
10-20 years	207	35.1	38.4
> 20 years	91	15.4	16.9

4.2.10 Commentary on experience

The distribution is towards experienced software developers. As the survey is also interested in how developers perceive their organizations' approach to topics such as accessibility and privacy, that broad experience should provide knowledgeable responses. The extensive experience is also likely to mean that some of the respondents are in relatively senior roles, with broad organizational awareness.

4.3 Formal training in legal concepts

The respondents were asked in a multiple answer question if during their work, or as part of their education, they received any formal training in contract law, software liability, software licensing, privacy and data protection, industry standards, copyright, patent, trademark and accessibility. The percentage of respondents who received any formal training varied between 8% for software liability and 21.6% for privacy and data protection. Most respondents had no formal training in any of the nine legal concepts included. There were 326 (55.25%) respondents who did not answer yes to any of the questions regarding any formal training in legal concepts.

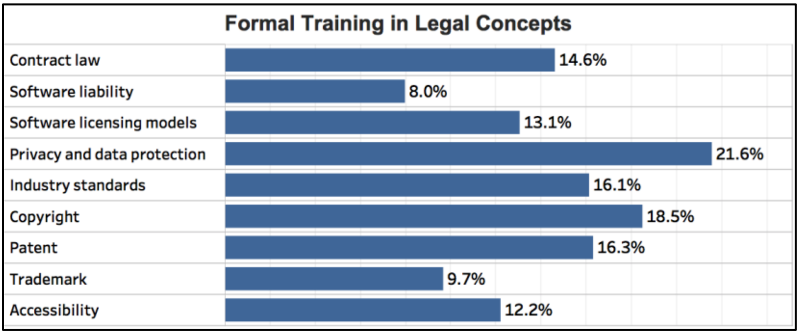


Figure 4.3: Formal training in legal concepts

4.3.1 Commentary on formal training

This response highlights the lack of formal training in these fundamental legal concepts. For instance, fewer than 1 in 10 software developers have had formal training in accessibility and just over 1 in 10 have formal training in standards. This does go some way to explaining the failure of software developers to build accessible software, for instance. Over 50% of the respondents have no training in any of the legal concepts at all. While formal training is not the only method to gain knowledge, this data point provides an answer to the research question, "What do software developers understand about the law that relates to software?" Neither the education system nor employers provide the vast majority of software developers in this survey sample with education in these fundamental legal concepts.

4.4 Legal knowledge

The mean, standard deviation and median score across the 5-point scale for the legal concepts knowledge questions are presented in Table 4.6. According to the mean and median score, the least known legal concepts are contract law and software liability, and the highest knowledge was indicated for the software licensing model and privacy and data protection legal concepts.

Table 4.6: Legal knowledge perception

Descriptive Statistics of Legal Concept Scores for the Respondents				
Legal Concept	N	Mean	Std. Dev	Median
Contract law	509	2.24	0.041	2
Software liability	508	2.15	0.039	2
Software licensing model	512	2.96	0.040	3
Privacy and data protection	513	2.96	0.038	3
Industry standards	513	2.50	0.043	3
Copyright	513	2.86	0.038	3
Patent	510	2.63	0.039	3
Trademark	505	2.45	0.040	3
Accessibility	505	2.53	0.043	3
Total Score	485	23.19	0.261	3

To test if there is a relationship between any formal training in a specific legal concept area (Question 12) and the level of knowledge in that particular area, non-parametric Mann-Whitney U tests[1] were applied for each legal concept area and the knowledge score for that particular legal concept. There were statistically significant differences between the scores of respondents with no training in contract law, software liability, software licensing models, privacy and data protection, industry standards, copyright, patent, trademark and accessibility, and those who indicated formal training (p = 0.000). The respondents who received formal training scored consistently higher than those who received no training across all legal concepts. The results are presented in Table 4.7.

[1] The author relied on the assistance of a statistics expert to develop the statistical analysis here.

Table 4.7: Knowledge scores v formal training

Knowledge Score Differences between Respondents Trained in a Legal Concept and those not Trained in the Legal Concept			
Legal Concept	Training	Mean Rank	p
Contract Law	Yes	389.98	0.000
	No	227.56	
Software liability	Yes	401.24	0.000
	No	240.93	
Software licensing model	Yes	357.51	0.000
	No	238.89	
Privacy and data protection	Yes	329.09	0.000
	No	233.77	
Industry standards	Yes	365.84	0.000
	No	232.26	
Copyright	Yes	338.77	0.000
	No	235.45	
Patent	Yes	361.66	0.000
	No	230.88	
Trademark	Yes	384.87	0.000
	No	236.55	
Accessibility	Yes	395.04	0.000
	No	229.76	

To determine the relationships between the knowledge scores reported by the respondents for the nine legal concepts, non-parametric Spearman's rho correlation tests were applied. All the correlations were positive, indicating that an increase in the knowledge score in one area is associated with an increase in the knowledge score in another area. The correlation varied from weak (0.153) between Trademark and Industry Standards, and medium (0.664) between Trademark and Patent.

Table 4.8: Correlations between legal concepts

	Contract law	Software liability	Software licensing	Privacy	Industry standards	Copyright	Patent	Trademark	Accessibility
Contract law	1.000								
Software liability	.357**	1.000							
Software licensing model	.296**	.462**	1.000						
Privacy and data protection	.263**	.394**	.348**	1.000					
Industry standards	.211**	.263**	.309**	.421**	1.000				
Copyright	.373**	.376**	.425**	.324**	.195**	1.000			
Patent	.325**	.243**	.374**	.261**	.219**	.630**	1.000		
Trade-mark	.401**	.306**	.350**	.248**	.153**	.657**	.664**	1.000	
Accessi-bility	.169**	.273**	.255**	.397**	.344**	.183**	.200**	.176**	1.000

To test if the demographic characteristics are associated with the aggregated legal knowledge score, a multiple regression was used with the aggregated legal knowledge score as the dependent variable and country of study, professional certifications, membership of formal professional bodies, organization size, experience and country of work as the independent variables. The model was statistically significant (F_6 = 4.052, p = 0.001) and it explained 4.1% of the variability in the legal knowledge score. Country of study, professional certifications, organization size and country of work were not statistically significant as predictors for the total legal knowledge score, while a membership of formal professional bodies and experience were statistically significant predictors ($p < 0.005$). When a respondent indicated that they were not a member of formal professional bodies, the total legal knowledge score decreased by 1.757 points, while an increase in experience from one level to the next resulted in an increase in the total legal knowledge score of 0.758.

4.4.1 Commentary on legal knowledge

The graphic of this response is useful to illustrate relative levels of self-assessed knowledge / understanding. Basic understanding implies that the respondent has an adequate grasp of the topic. The levels of basic understanding are relatively consistent across the 9 categories and there are very few self-defined experts. The statistical analysis showed that training, experience and professional body membership increase knowledge perception. The author expected that Germany-based respondents would rate themselves as having more knowledge on privacy and data protection, but this was not evident in the statistical analysis.

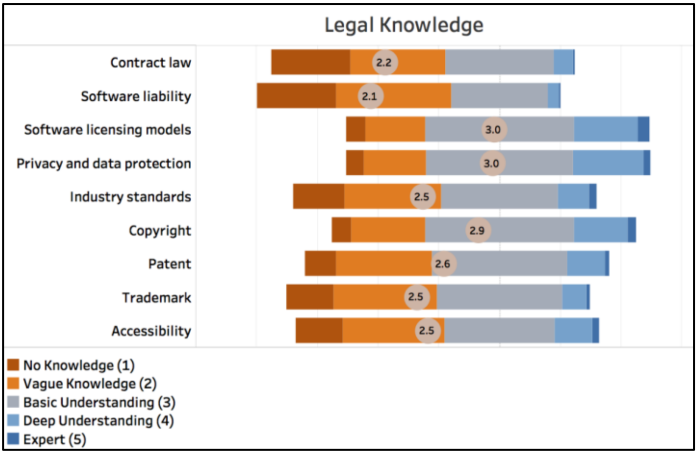


Figure 4.4: Legal knowledge self assessment

4.5 Privacy knowledge

The Data Protection Directive, or more precisely, the national implementations thereof, is concerned with the processing of personal data. Furthermore, it places stronger protection on sensitive data.

Most respondents (81.5%) answered that they build, design or maintain applications that process data about people (data items such as name, address, email, phone number), while approximately half of all respondents (51.6%) did not build, design or maintain applications that process sensitive data (political memberships, religion, sexual orientation or data relating to children). There were 93 respondents who chose not to answer the first question and 94 respondents who chose not to answer the second question. The responses are tabulated below.

Table 4.9: Build systems with personal and/or sensitive data

Frequencies and Percentages of Answers to Questions 14 and 15				
Question	Answer	Frequency	Percent	Valid Percent
Do you build, design or maintain applications that process data about people (data items such as name, address, email, phone number and so on)?	Yes	405	68.6	81.5
	No	88	14.9	17.7
	Don’t know	4	.7	.8
Do you build, design or maintain applications that process sensitive data? For instance, political memberships, religion, sexual orientation or data relating to children.	Yes	228	38.6	46.0
	No	256	43.4	51.6
	Don’t know	12	2.0	2.4

Respondents were asked about their knowledge of the ‘EU Data Protection Directive, which forms the basis for data privacy law in all countries that are members of the European Union and has a significant influence on privacy law in many countries.' Of the 491 respondents who answered this question, 253 (51.5%) read about it in the press or on the web, 47 (9.6%) had training in it at work or as part of their education and 191 (32.4%) had no idea about it. The differences in the knowledge of the EU privacy law across Germany, the United Kingdom and the United States were tested using a non-parametric Kruskal-Wallis test. The differences were statistically significant ($p = 0.000$). To determine which pairs exhibited statistically significant differences, multiple non-parametric Mann-Whitney tests were applied, with Bonferroni corrections to account for the Type I error increase in multiple simultaneous tests. There were no statistically significant differences between Germany and the United Kingdom. In contrast, there were statistically significant differences between Germany and the United States ($p = 0.000$), and the United Kingdom and the United States ($p = 0.000$), with the respondents working in the United States scoring consistently lower than those in Germany or those in the United Kingdom.

Crosstabs with Chi-square tests were applied to check if the respondents who build, design or maintain applications that process data about people were more likely to be formally trained in privacy and data protection, as well as have more knowledge of privacy and data protection. The results indicated that there were no statistically significant differences ($p > 0.005$) between people who worked with such applications versus those who did not or did not know if they worked with such applications or not. The differences in the level of knowledge in privacy and data protection were not statistically significant either ($p > 0.005$).

The same tests were applied to check if the respondents who build, design or maintain applications that process sensitive data were more likely to be formally trained in privacy and data protection, as well as have more knowledge of privacy and data protection. The results indicated that there were no statistically significant differences in training or knowledge levels between respondents who worked with such systems and those who did not or did not know.

A non-parametric Mann-Whitney test was run based on the statements chosen in relation to the respondents' perception of privacy and privacy law to test if there were any statistically significant differences between the respondents who had no idea about the EU privacy law and those who had training or read about it in the press or on the web. The results indicated that there were statistically significant differences (p = 0.000), with respondents who had no idea of EU privacy law more likely to state that privacy is largely ignored or actively avoided, while the ones who were aware of the EU privacy law more likely to have sound knowledge of privacy law or build privacy into their products.

4.5.1 Perceptions of organization approach to privacy

When respondents were asked how they perceived their organization's development practices with regards to privacy compared to other organizations, there were 488 valid responses. Of these, more than half (54.9%) indicated that they perceived them to be about the same, followed by those who found more focus on privacy in their organization (26.6%), ones who did not have an opinion (11.1%) and those who found less focus in their organization (7.4%). Respondents were also given a set of statements that described their perception of how privacy and privacy law affect product development process in their organization. About the same number of respondents felt that they had a sound knowledge of privacy law and they had policies (35.6%) or that privacy is sometimes considered in product design, but it is ad hoc (35.8%). The remaining respondents either saw building privacy into their products as a competitive advantage (17.7%), that privacy is largely ignored in their product design and process (10.2%) or that privacy is actively avoided in their product design (0.80%).

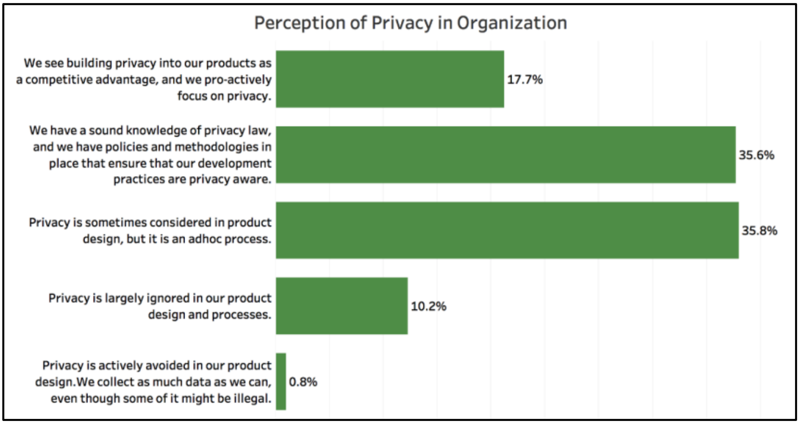


Figure 4.5: Perception of privacy in organization

To test any differences in the statements chosen based on demographic characteristics, several Kruskal-Wallis tests were conducted. There were no statistically significant differences based on the country of study, professional certification, membership of formal professional bodies or country of work ($p > 0.005$). In contrast, there were statistically significant differences based on the organizational size and the total legal knowledge score ($p = 0.000$). Respondents who stated that privacy is actively ignored in their organization were more likely to be in a smaller organization compared to those who indicated that privacy is a competitive advantage or that the organization has sound knowledge of privacy law. Similarly, respondents who stated that privacy is largely ignored or that privacy is actively ignored consistently scored lower on the total legal knowledge measure compared to those who indicated that privacy was a competitive advantage or that the organization had a sound knowledge of privacy law.

A non-parametric Mann-Whitney test was run based on the statements chosen in relation to the respondents' perception of privacy and privacy law to test if there were any statistically significant differences between the respondents who had no idea about EU privacy law and those who had training or read about it in the press or on the web. The results indicated that there were statistically significant differences (p = 0.000), with respondents who had no idea of EU privacy law more likely to state that privacy is largely ignored or actively avoided, while the ones who were aware of EU privacy law more likely to state that the organizations have sound knowledge of privacy law or build privacy into their products.

4.5.2 Commentary on data protection and building systems with personal data

Two clear points emerge from this section.

The vast majority of the respondents work with some form of personal data; many work with sensitive data. A reasonable expectation would be that people working with personal data have training in and understanding of data protection law, but this is not the case. Given the importance of the EU Data Protection Directive in data protection law, the lack of formal training and awareness is concerning. It would be difficult to accept that a software developer could have a basic understanding of data protection without being aware of the Directive. This does bring into question the validity of the self-assessment of privacy by the respondents. It could be argued that they over-estimate their knowledge.

While one would expect developers in the US to be less aware of the Directive, the scores of the European-based developers is a matter of particular concern. The relative lack of formal training should be of concern for educators, employers and the data protection authorities.

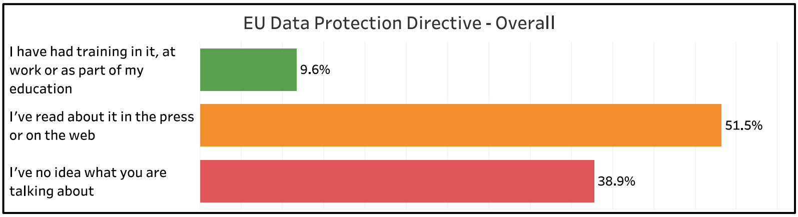


Figure 4.6: EU DPD awareness

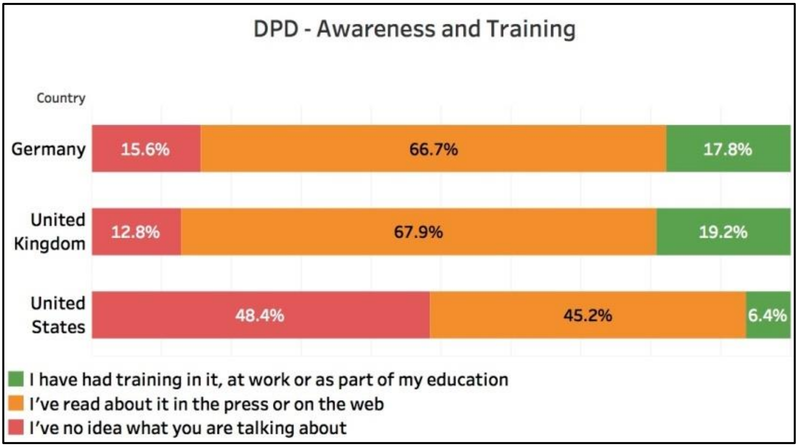


Figure 4.7: DPD awareness and training in the UK, Germany and the US

4.6 Web services risk perception

Respondents were asked to assess the risk of using services built by other organizations in solutions they deliver (Question 19). 425 respondents answered this question. Data protection and privacy was seen as the most risky, with 36% seeing this as a critical risk and 34% seeing it as a risk. Accessibility and trademark were seen as the least risky, with roughly 55% seeing this as a minor risk or irrelevant.

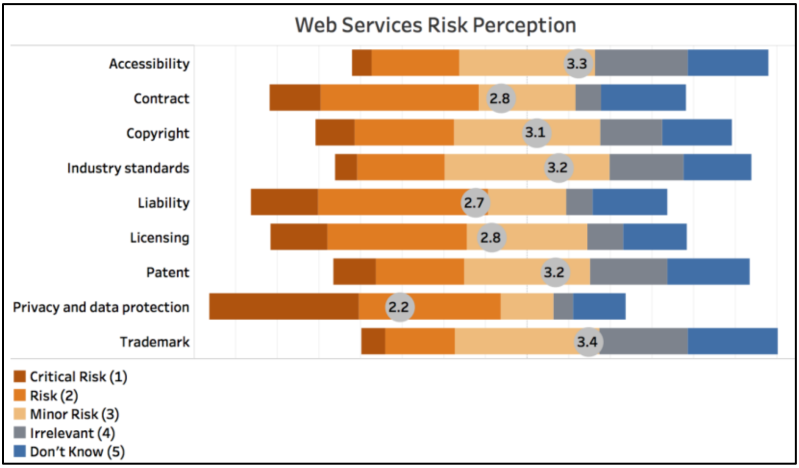


Figure 4.8: Web services risk

Question 20 asked respondents do you believe that your organization adequately assesses the risks of consuming third party web services? To assess whether there were differences between respondents who believed that their organization adequately assesses the risks of consuming third party web services and those who didn't or didn't know, a non-parametric Kruskal-Wallis test was applied in terms of the total legal knowledge score,. The differences were statistically significant (p = 0.000). Post-hoc non-parametric Mann-Whitney U tests with Bonferroni corrections were run to further investigate which pairs were different. There were statistically significant differences between those who responded affirmatively versus those who responded negatively (p = 0.009), with the ones who responded affirmatively scoring consistently higher on the legal score than those who answered negatively. There were statistically significant differences between the respondents who answered "yes" and those who answered "I don't know" (p = 0.000), with those who answered affirmatively scoring consistently higher on the legal score than those who didn't know. There were no statistically significant differences between those who answered negatively and those who answered with "I don't know" (p > 0.005). (To simplify, those who self assessed as being more knowledgeable felt their organizations had a better handle on web services risk than those who didn't).

Question 20 asked whether respondents believe their organization assesses the risks of consuming third party web services; 433 respondents provided responses. Of these, 211 (48.7%) indicated that their organization adequately addresses the risks, while 115 (26.5%) didn't know and 107 (27.7%) did not believe so.

4.6.1 Web services risk commentary

Web services rely on APIs to work and over the last 10 years or so various social network tools changed their API models on several occasions, eventually undermining the market for third party tools such as TweetDeck. APIs are at the centre of the current Google v Oracle dispute. The topic of API licensing is very complex and the debate about whether APIs themselves are subject to copyright is still not resolved. In the case of accessibility, many recruitment sites mash up maps or other additional third-party services and many of these are not accessible. Consuming a web service that does not meet security standards may well be in breach of IT audit standards such as SOC 2. Poorly engineered web services can be entry points for security breaches such as denial of service attacks. Data theft in transit is also a problem, especially if the service does not comply with security standards. At the time of writing, a third party web service that aids accessibility, BrowseAloud, was hijacked by cyptominers, forcing tens of thousands of government sites around the world to make emergency repairs.[2]

Over 20% of developers noted that all legal risks are irrelevant for web-services consumption and only 5% saw industry standards as a critical

[2] *https://nakedsecurity.sophos.com/2018/02/12/cryptomining-script-poisons-government-websites-what-to-do/*

risk. It is safe to assume that software developers underestimate the various legal risks of web-services consumption. The fact that data privacy scored higher is perhaps as a result of it being the subject of the prior question in the survey.

Less than 50% of those responding felt that their organizations adequately assessed the risk of consuming third-party web services

4.7 Accessibility

In Question 21, respondents were asked to select a paragraph that best agrees with how their organization approaches accessibility. There was a total of 429 responses, of which 135 (31.0%) indicated that they build accessibility into the product, 118 (27.1%) indicated that they largely ignore accessibility issues in their product design, 98 (22.5%) design accessibility into their products, 72 (16.6%) were not close enough to accessibility issues and 12 (2.8%) would retrofit accessibility when threatened.

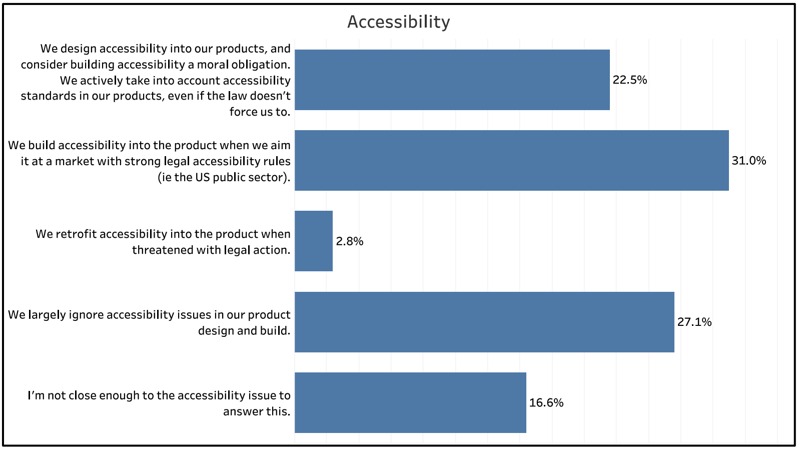


Figure 4.9: Accessibility perceptions

There were statistically significant differences in the size of the company based on the paragraph chosen (p = 0.000), with respondents from larger companies designing or building accessibility into their product, while respondents from smaller companies are more likely to ignore accessibility issues. There was a statistically significant weak positive correlation of 0.147 (p = 0.000) between the paragraph chosen and the organization employing or using experts to understand legal implications of software development. Similarly, there was a statistically significant weak positive correlation of 0.234 (p = 0.000) between the paragraph chosen and the statement chosen in regards to perceptions on privacy and privacy law.

4.7.1 Commentary on accessibility

As Chapter 6 will show, many applications are not accessible. So, it would seem that software developers over-estimate their organizations' commitment to accessibility. There is a perception from some developers that accessibility is something that some expert somewhere else in the organization deals with. So, this may go some way to explaining why those working for larger organizations see themselves as taking accessibility more seriously.

4.8 Legal risk in the development cycle

In Question 22, respondents were asked at what stage do they feel legal risks and issues should be assessed in the software development cycle. The question was a multiple answer type; it was answered by 431 respondents: 356 (60.4%) indicated that they address the legal risks and issues at the design stage, while 321 (54.5%) considered the legal risks and issues at the conception stage. The percentage of responses indicating the build, test and maintain stages were almost equally distributed (31.9%, 31.2%, 33.1%). Only 5 (0.8%) respondents indicated the legal risks and issues should never be addressed.

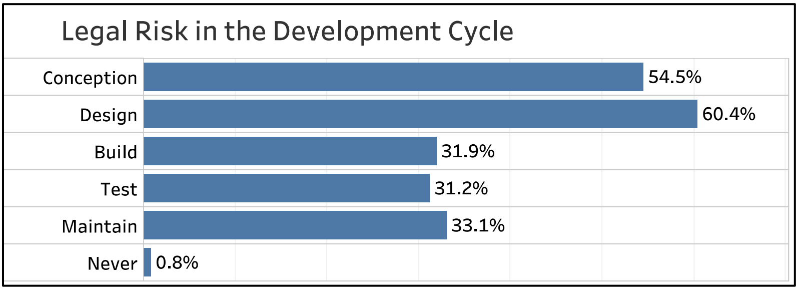


Figure 4.10: Legal risk in the development cycle

4.8.1 Use of legal experts

When respondents were asked if their organization employs/uses experts to help developers understand the legal implications of software development, of 429 valid responses 215 (46.4%) did not believe so, 142 (24.1%) believed so and 72 (12.2%) didn't know (Q 23).

Using a non-parametric Kruskal-Wallis test, it was determined that there were statistically significant differences between the respondents' organization using experts to understand the legal implications of software development and the organization size (p = 0.000). Thus, respondents from larger companies were more likely to have experts in legal implications of software development versus those from smaller companies.

4.8.2 Commentary on legal risk and issues in the development cycle

The conception phase of software development is the obvious starting place for assessing legal risk and issues, with the vast majority of respondents supporting assessment early in the development cycle. Given the importance of testing for accessibility or security compliance, the author was expecting a higher score on the testing role.

There is a tension between the responses in 19 and 22. The responses in 22 suggest a stronger interest in legal risk assessment than the responses in Question 19 on web services risk, where over 20% of the respondents felt that legal risks were irrelevant. It would have been useful to analyze this more robustly, but the use of multiple choice questions in the design of Question 22 make this awkward.

Respondents working for larger organizations have more access to experts to help. However, more respondents felt their organizations did not use legal experts to help than they did. This is dissonant with the responses to the questions on organization focus on privacy, web services risk and accessibility.

4.9 Formal training

Respondents were asked in Question 25 if they believe that they received enough formal training, either as part of their studies or as part of their professional development at work, on the legal issues that impact software. There were 424 valid responses, of which the majority of 297 (70.04%) stated that they did not receive enough training and only 2 (0.47%) stated that they had too much training. The remaining respondents either stated that they received enough training (20.75%) or that the question was not relevant (8.73%).

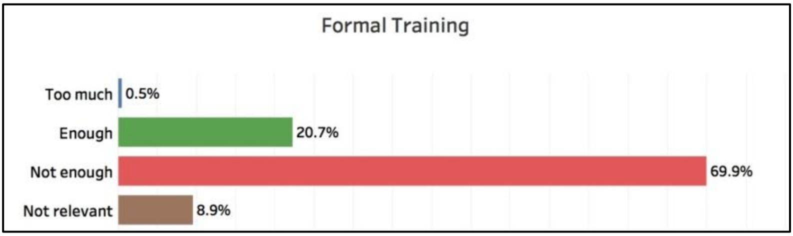


Figure 4.11: Formal training

Several Chi-Square tests were conducted to test if there were any differences in the responses provided, based on the demographic characteristics. There were no statistically significant differences based on professional certifications, membership of formal professional bodies and experience ($p > 0.005$). In contrast, there were statistically significant differences in the responses based on the organization size ($p = 0.000$). The respondents in an organization with 100-249 employees scored consistently higher than those in bigger companies (1000 and over) which means that more respondents in smaller companies felt that they did not have enough training in comparison to bigger companies. There were also statistically significant differences in responses to this question based on whether respondents indicated that they clearly understood the legal issues that impact designing, building and maintaining software ($p = 0.000$). Those who disagreed or strongly disagreed with clearly understanding the impacts were more likely to indicate that they did not receive enough training in comparison to those who agreed or strongly agreed. Similarly, there were statistically significant differences in responses to this question based on whether respondents indicated that they saw it as part of their professional responsibility to keep up to date with the legal issues that relate to software ($p = 0.000$). Thus, the respondents who agreed with keeping up to date being their professional responsibility were more likely to indicate that they received enough training in comparison to those who strongly disagreed.

The free format comments on this question are also useful.

Table 4.10: Free format training comments.

Formal training free format comments
It seems to me that most businesses would prefer to ignore the legal issues unless it either affects the bottom line or directors will be held personally responsible in law.
I have not received any training, but have attended a couple of seminars and follow a blog, read articles on subjects (when it seems relevant to our business). This I have done off my own back - previous employers did not ask me to do this or even recognise I did it.
Since you asked the questions, otherwise I would have assumed enough.

Open Source software development projects that rely on volunteers often have no money with which to seek professional specialist advice or training.
There is probably not enough training, but it depends on your definition of “formal”. I think there should be more training regardless of whether or not it is formal or informal.
Training must be ongoing, and focused on risks for a given engagement/ development One difficulty is how quickly law is changing and how inconsistant the law is across borders. There are other much deeper concerns about the rights of developers and free speech rights.
This is a premium market and as such I use the web for personal research/training to keep costs down, the downside is that my knowledge/expertise is not endorsed by the necessary ‘gongs’ as these costs outweigh the benefits due to my circumstances.
There are people who are assigned to this task, and yet I hold an interest… but it would not form part of my core work. Thus the education would offer a background on which I would not be held accountable.
I am in charge of my own professional development, so it is my own fault. Life’s too short.
It’s not so much that the quantity is wrong, more that the depth which it covers is pitiful.
for the last two years I’ve been working on a book entitled “Legal Issues for Software Engineers”
Mostly it’s lip-service from management, but I like to be up to speed, personally.
Not now I’ve done this survey!
I don’t know. It would depend on what legal considerations there are in our industry.
I feel it has been my responsibility to learn about legal issues, but have not got formal support to do so
No time to absorb legal issues. Software development of the scale that I’m involved in requires specialists in nearly every topic and sub topic in order to get it right. I do not wish to specialize in legal issues. Having written Global Payroll software where legality is critical, I only address legality as it applies directly to what Im doing and no further.
Actually once you understand the law, thats it. it is so depressing and threatening that one does not want to do coding any more.
One of my current duties involves developing ideas to the level where they can be patented. Yet I never received any training on what is patentable and why. I have had to learn on my own.
We had a course on Business Law mandatory to our degree but some subject more relevant to Software and the Law would have been very beneficial.
Not covered in school at all, nor in professional training. Learn from own private study as topics come up. Almost all available resources are obtuse and unusable.

Based on this survey interesting thoughts are occurring to me that will spur me to look for more information.
As I’m an industry analyst now, it doesn’t apply. However, the only training I ever got as a programmer were things that would profit the company, like figuring out things we should patent.
Keeping informed of legal issues impacting software is often left up to the individual to pursue especially for companies that support multi-country software.
I got my bachelor’s degree in the 1980s, when legal issues were an afterthought. My experience from hands-on working experience under business owners and managers that taught me a bit. Zero formal training as yet.
Received a lot of informal training/education.A necessary evil - not interesting, but it has to be done
The M.Sc was self-funded part-time. If I hadn’t done it, I wouldn’t have learnt about the legal issues highlighted above.
I did a 4 year honours math/CS degree at one of the best schools in Canada (Waterloo) and law as it relates to IT was an optional 4th year “bird” course (i.e. one that is easy) that few students take. I did, only because I was sick of not sleeping while doing labs. Security was not discussed anywhere in the mandatory curriculum.
People around don’t care about legal concerns because they mostly unaware of them. They, however, know that the legal department could review the technologies and object to some inclusions that might be legally infringing.
I will consider it a competitive advantage, if I understand the laws in multiple countries.
The separation of legal and technical responsibilities worries me. It also has a very negative impact on productivity.
Legal topics support should be built into the tools that R&D and Solution/Product Mgmt uses during the end-to-end software dev lifecycle. The capabilities should become easy to consume like a Spell Checker, and enforced in the tooling. I would avoid long, exhausting lectures / documentations that cannot transcend the importance of legal concerns to the real world.
In most cases legal awareness is something that filters through feedback from the legal department rather than through training. When consulting with some companies they were far more proactive in designing with legality involved due to the sensitive nature of their data (medical and financial industries).
Concerns about legal issues in software development should be part of an introduction to basic computer concepts.
Formal corporate training is almost non-existent where I work.
I place very little faith in formal training programs, preferring to self-educate.

I think designers need basic understanding and good advice from legal experts who review the product designs and share their legal expertise.
I’d like to you contact me. I work on Global teams, and I think that general application developers/DBAs like myself need help
On-the-job training
Ignorance of the law is no defence. Just as a civilian has to make him/herself aware of the law so it is in business. But wouldn’t it be great if employers were to be more proactive and offer or provide training!
It’s provided on a needs-basis. Actually we have departments such as Legal, Risk and Accessibility specialists who sign off on our work when necessary.
I receive none. Today, any developer who should learn about legal issues must find the motivation themselves. This is not good (obviously).

4.9.1 Formal training commentary

The question responses show there is a clearly articulated request for better training on legal issues. The vast majority of the respondents state that they are inadequately trained. This is further enforced by the key feedback from the free-text commentary, namely that formal training in both the university and professional context is inadequate, and there is a strong desire from respondents for education in the legal concepts. Several respondents also suggested that companies need better engagement between legal experts and software developers. One commentator raised the need for more automated tool support for legal testing.

4.10 Perception questions

As noted earlier, there are some issues with the design of this question. Nevertheless, the results are somewhat usable, at least at a descriptive level, and the free form comments are especially useful. Respondents were asked six questions in relation to legal issues and their importance for software technology.

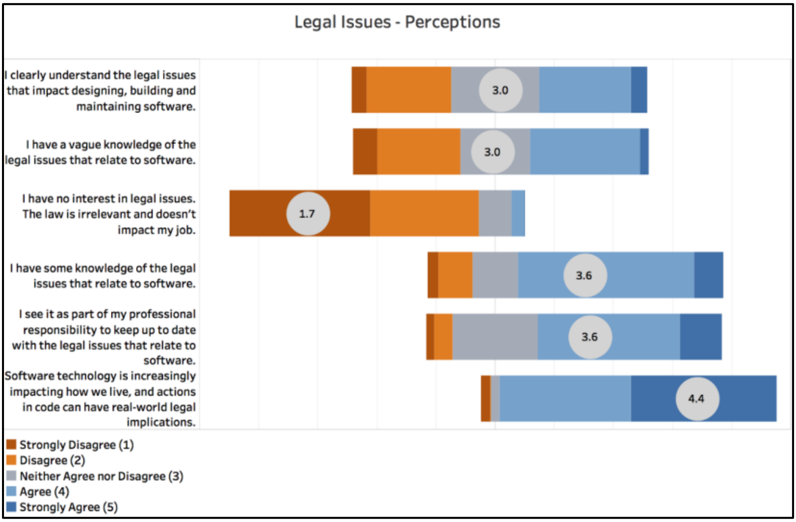


Figure 4.12: Legal issues perception

Technology impact

For the first question stating that: “Software technology is increasingly impacting how we live, and actions in code can have real-world legal implications” there were 424 respondents who provided a response; the mode was “Strongly Agree” (35.4%). Non-parametric Kruskal-Wallis tests and Mann-Whitney U tests were applied to test for any differences in the responses provided for the question based on demographic characteristics. There were no statistically significant differences in the responses based on professional certifications held, memberships of formal professional bodies, experience, country of study and country of work ($p > 0.005$). The responses were not correlated statistically significant with the total legal knowledge score and there were no statistically significant differences in the responses based on the total legal knowledge score ($p > 0.005$).

Understanding of legal issues

The second question “I clearly understand the legal issues that impact designing, building and maintaining software” had 423 responses, with a mode of “neither agree nor disagree”.

Professional responsibility

The third question “I see it as part of my professional responsibility to keep up to date with the legal issues that relate to software” had 423 responses, with a mode of “Agree” (34.4%).

Some knowledge of legal issues

“I have some knowledge of the legal issues that relate to software” had 422 responses, with a mode of “Agree” (42.7%).

Vague knowledge of legal issues

The fifth question “I have a vague knowledge of the legal issues that relate to software” had 414 responses, with a mode of “Agree” (26.1%).

Law is irrelevant

Lastly, the sixth question “I have no interest in legal issues. The law is irrelevant and doesn’t impact my job” had 421 responses, with a mode of “Strongly Disagree” (33.9%).

Free text responses to perceptions

See the following table.

Table 4.11: Perception questions free format responses

Free format responses to perceptions (an excerpt)
Well, for me it is seldom that I reflect so hard on the legal side of things. Maybe I should more.
I feel that most laws applicable to software & data are misguided, unenforceable, counterproductive.
As computers become faster, better, cheaper, and more pervasive, making certain they operate correctly and inobtrusively to enhance our lives becomes increasingly, even critically, important.
I have no interest in legal issues. - Agree, keeping myself up to date on security, performance, maintainability, new tech etc is more than enough of my (extra-curricular)time taken. The law is irrelevant and doesn't impact my job - strongly disagree, it obviously impacts me and the world I operate in, but I'd prefer to see a dedicated "legal eagle" in the same way we have dediacated security or performance specialists.
Real world legal implications are far behind where they should be and often poor legal choices are being made by individuals with little to no understanding of what they are doing.
This is presented in a strange and confusing manner.
It's laborious, a pain in the arse and very counter-productive to efficiency - love the open systems movement/thinking especially open sourcing code
Items 3 and 6 seem strongly biased and evoke negative feelings with the author of the survey in me! Furthermore Item 3 is vague (relate to software) and Item 6 seems to confuse correlation with causality. (Some SW-Laws //are// irrelevant - but they still impact my job very much!)
#21 was a little rough. This one was fine. :)
Software development is so complex and time consuming that I only hope Legal Issues are understood and handled by someone else in my organization. I do not have time to understand and react to legal issues while attempting to nearly meet the incredibly unrealistic deadlines my company sets.
To the extent that i am an employee, I dont have to care much because the legal risk would be with the employer. specifically because they made me sign some IPR document. If I am infringing on copyright or patent, they have to have the systems to catch it.
I am an advocate and creator of open source software, which complicates the legal landscape, especially in companies (like my current employer) that seek to own everything. I do not see open source issues addressed in these questions. They should be.
I wish the last was true but it isn't and sticking your head in the sand is never a good approach
Most of the applications we develop are for internal usage (eg Enterprise software).

Accessibility & privacy issues matter none to little in the situations we encounter (eg employees that handle potentially dangerous physical equipment must have eyesight; we therefor don’t design for blind users). We do spend a lot of time on usability in general. We consider physical abilities and computing abilities by our users as part of the proces of designing usable software.
I used to joke when I worked for a Wall Street firm that when their software broke, the only loss was money, whereas the software running a piece of industrial machinery can kill someone when it breaks. The ineptitude at the project-management level that I have witnessed over the years has me feel that lawsuits are way, way underfiled – the tip of the iceberg, so to speak.
I believe most of the laws pertaining to software (especially patent law) are artificial and irrelevant / not-applicable. Patent law must be made non-applicable for cases where it is the software that enables (partially or fully) the feature being patented.
These issues are important, but as they’re not a clear deliverable, they are often sidelined in favour of tangible functionality
My opinion is a bit subtler than this. I do not feel the need nor responsibility to understand or comply to laws that don’t make any sense to me. Accessibility and IP are not (always) in this category.
Just an idea… as we have QM/QA folks part of the development process assuring quality, performance and compliance to standards, one can imagine a new Legal Assurance (LA) dept/profession to be an integral part of the specific software deliverables.
in our organization a lot of the specifics of these questions are specialized in different groups. It is possible for a single developer to not understand the specifics. Esp. as it relates to evalution of 3rd party relationships and contracts etc.
Risk management/mitigation of compliance issues should be part of an overall crisis leadership business strategy and execution. This should permeate every part of the business. As software providers to business customers, we have a responsibility to permeate our software development, sales, and support processes with the same high level of focus on risk.
I worry most about IP and licensing issues when looking to use 3rd party code in our products.
4 and 5 overlap
I feel enterprise platforms should use security based on configurable metadata. I have used my (poor) attorneys in the past for questions regarding software legals issues.
These questions don’t seem to be structured properly
Although I believe that software vendors should consider legal issues in the design phase, the ultimate responsibility for which web services are consumed and how the software is configured and used lies with each customer. You also might want to distinguish between SaaS and on-premise - the legal responsibilities of SaaS vendors are arguably more stringent.

Some of the questions are negative of previous questions
4: “I have some knowledge of the legal issues that relate to software.” 5: “I have a vague knowledge of the legal issues that relate to software.” WTF?
Delivering software to government organisations imposes obligation to adhere to all legislation as well as security obligations.
In questions 19+20, you speak of assessing / understanding the risks of 3rd party services. But you left me no wiggle room to indicate how I might want to *compensate* for such risks. For example, you spoke about accessibility risks. I understand the question, but it’s incomplete – in most cases, it should be possible for me to compensate, by layering on software features in my software, that abstract away deficiencies in the underlying services. The same idea applies – to a lesser or greater degree – to all of the dimensions of risk you list…
I’ve not had to consider legal issues other than accessibility issues in the software I’ve worked on. If I had to, then I would. It just so happens that the particular systems I’ve worked on haven’t involved those issues.
As a contracted developer I mostly rely on the requirements by the customer. Most applications run in a companies intranet.

4.10.1 Commentary on perceptions

The first question highlighted the awareness in the respondents of the interaction between code and law, and most respondents agreed that software code has real world legal implications. This corroborates the sixth question, which essentially asks the opposite question. Questions two, three and four reinforce the point that many software developers are unsure about legal issues. 62% of respondents either agreed or strongly agreed that it is part of their professional responsibility to keep up with the legal issues that relate to software.

The free format text responses for Question 24 are useful on two levels. Firstly, a few respondents point out their issues with Question 24’s design.

Secondly, the comments highlight the developer frustrations, concerns and suggestions:

- Lack of training
- Limited time to focus on legal issues
- Frustration with IP models.
- Suggestions for process improvement
- The tension between corporation IP and open source.

4.11 Final free text section

There were 132 comments at the end of the survey. Some were simply comments such as good luck, thanks for the survey, let me know how it goes. A few comments raised concerns with Question 24, but many were pleased with the survey design.

The comments about the survey context are cited in the table below.

Table 4.12: Final question free format responses

Free format responses extract from the end of the survey
Some of the survey questions made me give consideration to issues that I had not recently looked at. This was a useful prompt though it could slightly distort your survey results!
Your survey is targeted at developers of particular types of software (I work on tools used by other developers – so while my code does process private information, that's really the responsibility of my users: the people who build the applications with my tools).
Question 19: you don't ask what specific web service scenario, but my answer would have been completely different had I thought of a different scenario. Questions 21 and 23: The choices you give the respondent do not seem sufficient. For example, we build accessibility into our product (mostly) and not for moral reasons or because of our target market but simply because we try to conform to general customer expectations. We use external legal consultants, but it is up to the development manager's discretion to decide when that is appropriate and no training or formal guidelines exist for when it would be appropriate. Technically, this is a 'yes' answer, but …
Interesting and thought provoking questions. Now you're forcing me to think and address the contradictions of some of my answers.
Interesting and thought provoking – will make me think further about the legal etc implications of s/w production in the future

I have the feeling that independent and free software developers were a bit neglected in the conception of the survey.
all fine, good luck. if you can push a recommendation - it'd be for a short video/audio summary of key legislation that would enable SME's (who can't afford the legal fees) to get up to speed on the issues.
I'm really interested in the privacy implications of a world of mashups and webservices, especially when this practice is embedded into products away from the computer. We do some work with building API's into building services and energy monitoring, and the it's something we constantly have to think about, but it's a fascinating area, and if we don't engage it early, we'll never enter a world of ubiquitous computing on terms we agree with.
Very worthwhile topic. I think licensing issues in particular should be better understood by developers.
There is a lot of law that simply shouldn't apply to software development, i.e. copyright and patent. And much that is applied nefariously (trademark). You might consider addressing this in another survey.
Good survey. I would recommend having it reviewed (or rather, the next one reviewed) by a native English speaker, as there were some ambiguities (imho) in the English. I am Swedish myself, but have lived in the UK and US for 17 years. It is a hard thing to become perfect. ;)
The survey has actually helped me highlight some areas where I feel I don't have as much knowledge as I should. Many thanks, & good luck with the PhD!
Questions 16 and 21 are worded in a way that I perceive as offending! They both strongly imply a concept of "You're either with me or against me" and leave no room for a "third opinion". I suggest offering a "You're Answer" field for those as well. Cheers Michael Mahlberg
Somewhere between scary & terrifying. Gulp.
I am going to make sure that I get a lawyer to sit next to me when I am coding.
It really an eyeopener for most of the people who believe that writing code is sufficient.
It is a wonderful survey and some of the questions have made me think beyond this survey.
I feel that the understanding of software developers and the law and license agreements should be better addressed in formal education. Most developers that I have encountered have a misconception even of the "Open Source" license agreements thinking that the code could be used for free but not realising that using that code in a proprietary solution have very real legal implications.

I consider legal issues to be a non-value adding aspect of systems development. As such a quick and easy method to asses legal issues would be very useful. For instance a checklist to see whether a given application design should consider none/some/critical legal & privacy issues.
I liked the survey. Some questions are very relevent and in future these topics are going to be more complex with Globalization. I have been with SAP developing and delivering products that need to have legal compliance built into the products. Feel free to contact me with any help
Our software isn't "web services" and it doesn't deal with consumers or collect personal data. You need a "does not apply" answer to some of your questions because you're assuming all software out there collects personal data. It does not…
I think this was one of the best survey's I've done, very clearly written, always having the answer that I want available (without having to resort to the 'other…' option). Good luck with your research!
My specific involvement with this subject matter has been primarily in relation to the implementation of systems to be in compliance with wage and hour laws and FMLA in the US.
Copyright and intelectual property rights are the most important legal regulations for my work in software development. In several cases we have analyzed opportunities to integrate source code owned by partners or open source. Copyright regulations and IP laws were important for the decisions we have taken.
This survey has made me think more about the impact of the software I'm involved in delivering - legal implications are usually vaguely discussed but usually no one has an exact idea of what the specific details or requirements are. Accessibility is never discussed - sometimes even basic usability is seen as a 'nice to have - we can make it look nice once it's working'
Software development, like any other business activity, is governed by and has to take into account laws, regulations and good business practices. To do otherwise, will often lead to risks that can otherwise be mitigated at usually reasonable cost.
You have not explicitly considered Intellectual Property in your survey; do you intend to cover this under the Patent theme?
I really hope the restricting laws such as patent law be made irrelevant for software - they are not worth the hassles it creates in creating software. Copyright and Trademark laws are fine.
It is very interesting to come across this survey. Mostly for the perspective this survey tries to bring in. However, if a service provider is implementing, does the onus of managing the parameters like copyright, patent, privacy etc lie with the service provider or with the customer asking for such an application to be built? I guess this is exactly this survey would bring out. All the very best.

Great topic! I hope your work can make some positive impact on closing this gap in our business practices.
Good topic. As product managers we always violate laws anytime we open our mouth about the product roadmap. Any such comment can be considered against GAAP laws. It is a ridiculous situation with no clear way out.
I wish I could have made some comments on the perceived risk of external services grid. I think a lot of risk depends on quality/comprehensiveness of contract and usage.
Important topic, takes more and more time even in setting up captive or third party development and software management centers as part of outsourcing or offshoring.
I’m excited to see this survey (found on linked in). I used to manage a lot of the legal issues in a software development team, and it was gaps between what the developers knew and what the lawyers knew was amazing. And the things the lawyers didn’t know to look at was scary! You should consider sharing your results with legal journals as well as technical ones.
The “do you pay attention to accessibility?” question was missing an option for “we follow standards rigorously, which results in excellent accessibility, but accessibility is not the reason for it”.
I made some comments throughout. One last comment on the section I left blank about risk of consuming 3rd party web services: risk to whom? The customer or legal risk to the vendor? There is a fine line of difference from a vendor point of view. Once a customer has the product in hand the vendor looses some degree of control.
You helped me to recognize something that I should invest some time in. I work in global financial markets and feel that a transparent understanding of the legality of software and privacy needs to take some precedence in our lives.
Excellent survey. Well thought out, clear and unambiguous questions, well written and informative. With links to help sources - that was awesome and unexpected bonus!
Code is thoughtstuff (like law! ;)). The survey seems to imply that a static, passive relationship to these risks is needed (“Have you understood all the risks? Are you safe? OK, box checked?”). But good software has an active, dynamic relationship with these issues, as in “Due to all the weird 3rd party services we’re using, it may be mathematically impossible (in a probabilistic sense) to assess the degree of exposure to patent risk (at any given point in time, as it will also fluctuate). So how can we design the software to use what we need, and minimise the problem? Without ever understanding our total exposure?” That sort of thing…
Legal liability is one of those topics that I don’t think much about until I see something like this and think that I probably should!
Thanks this survey is a great idea for an area that I now realize is quite underserved.
Your research focus is very important and valuable, and I hope you are able to produce clear insights and recommendations.

Nicely done. I wish something actionable will come of this. I know that my re-assessing my answers has caused me to realize how poorly educated I am in this field. Thank you.
Very interesting and relevant. Taking the survey makes me think more about the issue. Looking forward to the results. Thanks!

A significant number of the respondents commented that the survey made them realize the importance of the topic, and has triggered an interest to invest time in learning more.

4.12 Summary: What did the survey confirm?

The survey confirms that this international group of largely experienced, enterprise focused, educated software developers are in the main untrained and uninformed about the legal concepts that impact enterprise software. They also have mixed perceptions of the commitment of their employers to accessibility, privacy and web services risk. The majority of the respondents voiced their desire for better education and clearer guidance.

Nearly 600 respondents completed the survey. The survey was never assumed to be probabilistic in that the results and findings can be extended beyond the respondents with any precise statistical confidence; nevertheless, the high-level findings should be relevant for broader enterprise software industry research.

5 A cursory overview of accessibility law and disability concepts

5.1 Chapter purpose: Explaining disability and accessibility

A significant component of this work examines web accessibility. In order to understand web accessibility correctly, it would be appropriate to briefly explain disability, and how accessibility law and practice has developed in the built world and for the web. This chapter sets the groundwork for the lab test that follows.

5.2 Introducing disability research

Disability studies research notes two models of how society views and approaches people with disabilities:

- Medical model (sometimes called welfare model)
- Human rights model (sometimes called social model)

5.2.1 Medical model

Throughout history, people with disabilities[1] have been isolated and neglected,[2] and sometimes pitied.[3] For instance, Law describes the traditional approach as the medical approach to disability.

[1] Some authors use the abbreviation PWD for people with disabilities. This work does not.

> *The medical model of disability has dominated the history of PWDs in society. Separating PWDs from the rest of society because of their disability (through institutionalization and asylums) was the norm for PWDs in the 19th century and well into the 20th century. This separation based on medical diagnosis came with a view that PWDs did not have the same rights as others in society.*[4]

In the medical model, a person who cannot read because of a visual impairment has a medical condition. The person, rather than the mechanisms by which we read, requires treatment. The welfare element means people with disabilities are then supported or cared for by the state, family or perhaps charities.

> *Disability, on this understanding, is seen as a problem located within the individual. Unless that individual can be cured or somehow adapted, they will not be able to participate in the life of mainstream society. It is they that must change or be changed in order to fit within a society designed for non-disabled people.* [5]

For most of history, this model has dominated how society viewed people with disabilities. Since the middle of the last century, societies have been on a slow shift to the human rights model. This shift is by no means complete.

[2] In 1887, a reporter, Nellie Bly, pretended to be insane. She was incarcerated in New York's Blackwell asylum and exposed the awful treatment inmates received. There are many other instances of mistreatment, abuse and neglect, even today.

[3] Anna Lawson, 'The EU Rights Based Approach to Disability: Strategies for Shaping an Inclusive Society' (2005) 6 International Journal of Discrimination and the Law 269.

[4] Chris M Law, 'Responding to Accessibility Issues in Business' (RMIT Australia 2010) 12.

[5] Jarlath Clifford, 'The UN Disability Convention and Its Impact on European Equality Law' (2011) 6 The Equal Rights Review 11.

5.2.2 Human rights model

Law describes the social model of disability.

> *In the social model, the underlying assumption is that disability is a function of how society is constructed and designed. In this model, someone who is blind cannot read print because the print has not been rendered in such a way that allows them to read it (e.g. tactually with Braille, or electronically allowing the use of speech output). The social model allows for design (designing organizational and socio-technical systems, designing interfaces, etc.) as an approach to accessibility problems.*[6]

This is also known as the human rights based approach.[7] While this model has established itself in convention and law, the medical model still often influences the way much of society views disability. Nevertheless, the last 40 years have seen a shift from a dominating medical model to a more rights based approach to disability civil rights.[8]

Waldschmidt notes that the social model implies three assumptions:

- Disability is a form of social inequality and disabled persons are a minority group that is discriminated against and excluded from mainstream society.
- Impairment and disability need to be distinguished and do not have a causal relation; it is not impairments per se which disable, but societal practices of 'disablement' which result in disability

[6] Law 12.

[7] Cynthia Waddell, 'Overview of Law and Guidelines' in Jim et al Thatcher (ed), *Web Accessibility* (Springer 2006).

[8] Law 12.

- In the Human Rights model, it is a society's responsibility to remove the obstacles that persons with disabilities are facing.[9]

Disability studies is a complex field, and this work merely skims the surface, see Waldschmidt et al, Heyer, etc.[10]

This work will rely on the description of disability outlined in Article 1 of the UNCPRD.[11] This clearly illustrates the shift from medical to human rights, at least in terminology.

> *The purpose of the present Convention is to promote, protect and ensure the full and equal enjoyment of all human rights and fundamental freedoms by all persons with disabilities, and to promote respect for their inherent dignity.*
>
> *Persons with disabilities include those who have long-term physical, mental, intellectual or sensory impairments which in interaction with various barriers may hinder their full and effective participation in society on an equal basis with others.*

[9] Anne Waldschmidt, Hanjo Berressem and Moritz Ingwersen, *Encounters between Disability Studies and Cultural Studies* (2017) 21.

[10] The following provide a good insight into disability theory and studies. Waldschmidt, Berressem and Ingwersen; Katharina Heyer, *Rights Enabled: The Disability Revolution, from the US, to Germany and Japan, to the United Nations* (University of Michigan 2015); Anna Lawson, 'The United Nations Convention on the Rights of Persons with Disabilities: New Era or False Dawn' (2006) 34 Syracuse Journal of International Law and Commerce; Lawson, 'The EU Rights Based Approach to Disability: Strategies for Shaping an Inclusive Society'; P Blanck, *eQuality: The Struggle for Web Accessibility by Persons with Cognitive Disabilities* (2014); Law.

[11] UNCPRD is discussed further below.

The path from the medical model to the human rights model has been long and it has been a political struggle that bears several similarities to other human rights struggles, such as those against racism or gender discrimination.[12]

There are a variety of definitions of accessibility, but the European Commission defines it as follows:

“Accessibility is defined as meaning that people with disabilities have access, on an equal basis with others, to the physical environment, transportation, information and communications technologies and systems (ICT), and other facilities and services.”[13]

In Germany, the definition of accessibility is based on the *Behindertengleichstellungsgesetz* (BGG). Section 4 describes accessibility: “Buildings and other structures, means of transport, technical devices, information processing systems, acoustic and visual information sources and communications equipment are considered accessible if people with disabilities have access to them and can use them as customary, without particular impediments, and basically without assistance.”[14] This is a more inclusive definition.

Accessibility involves a wide range of disabilities, including visual, auditory, physical, speech, cognitive, language, learning and neurological disabilities. In this work, the accessibility assessment lab test focuses on the specific case of visual impairment, but it is important to be aware that other forms of disability require accommodation in software design. Cognitive disabilities in particular have not received the attention required

[12] Heyer, *Rights Enabled: The Disability Revolution, from the US, to Germany and Japan, to the United Nations*.

[13] European Disability Strategy 2010-2020: A Renewed Commitment to a Barrier-Free Europe

[14] Translation from *http://www.bmu.de/fileadmin/Daten_BMU/Pools/Broschueren/barrierefreies_bauen_leitfaden_en_bf.pdf*

from software designers, see Blanck for further analysis.[15] Sohiab's[16] table, reproduced below, provides examples of disability forms, symptoms and potential interventions.

Table 5.1: Disability types and website accessibility issues

Disability form	Symptoms
Visual impairment	Partial vision; color blindness; may require usage of screen readers, or screen magnifier tools
Hearing impairment	Hearing difficulties; may require sound caption
Cognitive disability	Reading or comprehension difficulties; dyslexia; memory loss
Motor skills impairment	Inability to use keyboard/mouse; inability to make fine movements; may require usage of special assistive devices such as a voice browser, special joysticks and trackballs, and special keyboards that can be manipulated by fingers or using a head-wand

5.3 US: Disability and accessibility, civil rights

The rights for people with disabilities movement had its roots in the US. Several studies provide detailed historical commentary on the political and legal struggles.[17] For the purposes of this work, it is worth highlighting the following:

[15] Peter Blanck, 'eQuality' [2014] eQuality: The Struggle for Web Accessibility by Persons with Cognitive Disabilities 1.

[16] Osama Sohaib and Kyeong Kang, 'E-Commerce Web Accessibility for People with Disabilities', *Complexity in Information Systems Development* (Springer, Cham 2017) 87 89.

[17] Selwyn Goldsmith, *Designing for the Disabled: The New Paradigm* (Architectural Press 1997); Heyer, *Rights Enabled: The Disability Revolution, from the US, to Germany and Japan, to the United Nations*.

- The pioneering work of Tim Nugent led to “the barrier free standard for making buildings accessible to and usable by the physically handicapped,” becoming the US ANSI 1171.1 standard in 1961. Nugent also campaigned for the 1968 Architectural Barriers Act.
- In 1973, Congress passed the Rehabilitation Act. Activists such as Ed Roberts were key to driving this forward. The Rehabilitation Act was important in that Section 504 established the idea that PWD were deserving of civil rights protections.[18] It took 5 years of further protests for the regulations for deployment to be signed.
- In 1990, the Americans with Disabilities Act was passed. Heyer notes this was the world’s first comprehensive civil rights law for PWD. It defines disability as a civil rights issue and mandates equal opportunities, integration and accommodations for difference.
- In 1998, Congress amended the Rehabilitation Act of 1973[19] to require Federal agencies to make their electronic and information technology (EIT) accessible to people with disabilities. In 2000, the US Access Board published the Section 508 Standards for Electronic and Information Technology.
- The 2008 ADA Amendments Act strengthened the definitions of disability, reversing court decisions that had taken a very narrow view of disability (again, after significant protest).

5.3.1 US: Looking at the web specifically

The publication of the Section 508 standards in 2000 established a set of standards for the US public sector. Various states of the US enacted similar state level regulations. The Section 508 standards of 2000 were similar

[18] Arlene Mayerson, ‘The History of Americans with Disabilities Act: A Movement Perspective’ (*Disability Rights Education & Defense Fund*, 1992) <https://dredf.org/news/publications/the-history-of-the-ada/> accessed 28 August 2017; Susan Schweik, ‘Lomax’s Matrix: Disability, Solidarity, and the Black Power of 504’ (2011) 31 Disability Studies Quarterly.

[19] Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. Section 794 (d)).

to the WCAG 1.0, but not exactly the same, as Section 508 were agreed before the WCAG standards were finalized. The position for public sector websites is clear, given Section 508. In order to show compliance with the standard, software vendors produce a Voluntary Product Accessibility Template (VPAT). Section 508 compliant is often used as shorthand for “accessible”. This is problematic, as it perpetuates the myth that accessibility is “just a public sector thing.”

By 2006, the original Section 508 standards were showing signs of obsolescence,[20] and an advisory committee was formed to refresh the standards. They delivered their findings in 2008, and 8 years later, after many revisions and delays, the final rule was published in January 2017.

5.3.2 What is the WCAG standard, briefly?

It is worth briefly outlining the WCAG here.[21] The WCAG is produced by the Web Accessibility Initiative (WAI) of the World Wide Web Consortium (W3C). The first standard, WCAG 1.0 was published in 1999, and it has since become widely adopted as the basis for many governmental and organizational policies around the world.[22] WCAG 1.0 had 14 guidelines, and created 3 priority levels (priority 1, the most basic level of web accessibility; priority 2, addressing the biggest barriers; and priority 3, making significant improvements to web accessibility). As with the Section 508 standards, rapid technical advancements and the need for a clearer objective measure of compliance meant that they needed revision. WCAG 2.0 came into force in 2008, with the goal of being technology independent and more measureable.

[20] The emergence of the smartphone in particular made the original taxonomy problematic.

[21] Chapter 7 explores the issues with the standard in more detail.

[22] Wendy Chisholm and Matt May, *Universal Design for Web Applications: Web Applications That Reach Everyone* (2008) 17.

It has 4 principles:[23]

- Perceivable: Users must be able to perceive the information being presented (it must not be undetectable by any of their senses)
- Operable: Users must be able to operate the interface (the interface cannot require interaction that a user cannot perform)
- Understandable: Users must be able to understand the information as well as the operation of the user interface (the content or operation cannot be beyond their understanding)
- Robust: Users must be able to access the content as technologies advance (the content should remain accessible as technologies and user agents evolve)

Each of the principles has specific guidelines. It has 3 levels of conformance: Level A -most basic features-; Level AA- deals with the biggest and most common barrier -; and Level AAA - the highest level. Level AA is typically used as the benchmark for an accessible web site. For each guideline, there are testable success criteria.[24]

There are other guidelines relating to accessibility that the WAI manages, including the Authoring Tool Accessibility Guidelines (ATAG). User Agent Accessibility Guidelines (UAAG) relate to assistive technology operability with operating systems, browsers, etc. and the Accessible Rich Internet Applications suite (WAI-ARIA).

5.3.3 The vexing question of public accommodation

It took decades for legislators, regulators and the courts to define precisely how to apply the ADA to the built world. How and if the ADA applies to

[23] Fernando Alonso and others, ‘On the Testability of WCAG 2.0 for Beginners’, *Proceedings of the 2010 International Cross Disciplinary Conference on Web Accessibility (W4A) - W4A ’10* (2010).

[24] In the lab test, the career sites are assessed against many of these criteria.

the web has been even more convoluted. For the private sector, it is far from straightforward. The issue largely rests on whether a website is a public accommodation or not, as per Title III of the ADA.

To qualify as a public accommodation, a private entity must effect commerce, and fall into one of twelve categories. These are broad and cover pretty much any physical establishment such as stadiums, shopping centres, etc. The case that helped define the broad physical definition was PGA Tour Inc v Martin.[25]

As Brunner notes, a Title III claim includes 3 elements:

- The plaintiff must be disabled
- The defendant must be a private entity that owns, leases or operates a place of public accommodation
- The plantiff must have been denied public accommodation because of the disability

The courts have been split as to whether a website is a public accommodation:

- First and Seventh Circuits held that non-physical facilities can be public accommodations.
- The Third and Sixth Circuits held the opposite position, that public accommodations are expressly only a physical place.
- The Second, Ninth and Eleventh Circuits applied the “nexus” test, which held that the non-physical space could be a place of public accommodation if it had some connection to a physical space.

In June 2017, a case reached the federal court in Florida. This was eagerly awaited, as the judgment would help resolve the confusion that the lower courts’ split judgments had created. The case involved Juan Carlos Gil, who is blind. Gil wished to use the online coupon service to order his

[25] PGA Tour, Inc v Martin, 532 U.S. 661, 676-77 (2001)

medication at Winn-Dixie, a supermarket chain. The site was inaccessible with a screen-reader.

The judge made several important rulings:

- That the website was a place of public accommodation (The judge did not rule on whether the website would have been a place of accommodation if it was "only" a website, as the Nexus applied to Winn-Dixie).
- That making the site WCAG 2.0 compliant is an appropriate remedy.
- That Winn-Dixie should "provide mandatory web accessibility training to all employees who write or develop programs or code for, or who publish final content to, www.winndixie.com on how to conform all web content and services with WCAG 2.0 criteria."
- The Court also found that the fact that "third party vendors operate certain parts of the Winn-Dixie website is not a legal impediment to Winn-Dixie's obligation to make its website accessible to the disabled. First, many, if not most, of the third party vendors may already be accessible to the disabled and, if not, Winn-Dixie has a legal obligation to require them to be accessible if they choose to operate within the Winn-Dixie website."
- Winn-Dixie should post an accessibility policy on the website.

This judgment will help drive some clarity, but it does not fully conclude the question of whether a website is a place of public accommodation when there is no nexus. Other judgments have not seen WCAG in the same light.

Litigation volumes are dramatically increasing, yet lack coherent regulation guidelines.

A number of law firm sites and law commentators point to the massive increase in web accessibility cases over the last 5 years. Both lawyers and activists have been emboldened by recent judgments.[26] In Florida, there were 1,663 ADA cases filed in 2016 and California had approximately 2,468 ADA Title III filings in federal court in 2016.[27]

While the courts play a vital role in interpreting the law, the DOJ is responsible for setting regulations and guidelines. A clear set of regulations would make the job of the courts easier, and also provide clarity for website users and creators, often avoiding the need for the courts' involvement in the first place. In several cases during 2016, the DOJ made representations in ADA Title III cases, typically siding for a more expansive reading of the public accommodation provisions than some of the courts had taken.

The DOJ promised guidelines in 2010, but these were delayed several times.[28] There was an extensive consultation process (Supplemental Advance Notice of Proposed Rulemaking) in 2016, with a proposed set of rules.[29] The plan was for the guidelines to be implemented in 2018. However, with the shift of leadership in the White House, these guidelines were placed on the list of 2017 inactive actions. This has disappointed disability activists and commentators. It is unlikely that there will be guidelines in the short or medium term. With the general shift to regulation aversion in the White House, it will be up to the courts to provide short term guidance.

With the massive spike in litigation, it is likely that we will see organizations in the US taking web accessibility more seriously, especially in the retail sector. This is long overdue. While the ADA has helped shift the

[26] In Nevada, there are reports of one activist / law firm filing 274 cases. *https://www.reviewjournal.com/news/news-columns/jane-ann-morrison/ag-intervenes-in-ada-litigation-to-protect-the-publics-interest/*

[27] *https://www.adatitleiii.com/2017/11/florida-lawmakers-take-action-to-curb-access-suits-but-will-it-work/*

[28] The process has been very slow. See *https://www.adatitleiii.com/doj/*

[29] *https://www.gpo.gov/fdsys/pkg/FR-2016-05-09/pdf/2016-10464.pdf*

attitude of building architects, it is yet to achieve the same in software development.

At the time of writing, there is a proposed reform bill of the ADA,[30] which, according to disability experts,[31]will significantly reduce the power of the ADA. For those proposing the reform, the changes are necessary to reduce "drive-by" lawsuits. So, the trend of strengthening disability rights in the US is by no means assured.

5.3.4 US Web accessibility summary

The public sector position has been clear for some time, thanks to Section 508 of the Rehabilitation Act and Title II of the ADA. But there is no precise clarity on the applicability of the ADA to private sector websites, despite it being 20 years since the first cases came to court. However, the trend from the courts points to an obligation to make websites accessible, especially in cases where there is a nexus of physical commerce and web commerce.

5.4 Germany: Disability rights context and accessibility law

The concept of the welfare state in Germany can be traced back to Bismarck's comprehensive enactment of the social insurance system. The Cripples Welfare Law of 1920 *Krüppelfürsorgegesetz*[32] guaranteed medical treatment and also education and vocational training to people with

[30] *https://judiciary.house.gov/press-release/house-judiciary-committee-passes-ada-reform-bill/*

[31] See *https://www.americanprogress.org/issues/disability/news/2017/09/22/439464/quiet-attack-ada-making-way-congress/*

[32] Preußisches Gesetz, betr. Die öffentliche Krüppelfürsorge. Vom 6. Mai 1920.

physical difficulties. Heyer notes that for the time, the German rehabilitation system was the most advanced in the world.[33]

It is estimated that over 300,000 disabled people were killed by Nazi euthanasia programmes.[34] Immediate post war efforts focused largely on those injured by the war, but, in 1953, the federal law on the employment of the severely disabled established and mandated employment quotas. The principle of the social state is a cornerstone of the German constitution. The Federal Republic is a social state (Articles 20(1) and 28(1) of Germany's Basic Law [*Grundgesetz or GG]*) and this underpins the extensive involvement of the German state in social welfare. The principle of the social state focuses on remedying social inequality and protection of the socially weak. In the disability context, this was reflected in the medical approach, for instance with separate schooling.

Over the course of the late 1970s and 1980s, persons with disabilities in Germany began to campaign for disability rights, eventually creating the *Düsseldorfer Appell*, a demand for an ADA-like law in Germany. With the reunification of Germany, there was significant work to revise the constitution, and this, in essence, created the window to drive through the disability discrimination clause. As in the US, it was the combination of determined activism and political expediency that brought about the change. Prior to reunification, there was no explicit mention of disability rights in the GG, but the new Article 3 of the GG now includes the phrase, "Nobody shall be discriminated against because of disability."

This was followed by further campaigning, leading to major reforms of the SGB IX in 2001 and the passage of the Disability Equalizing Llaw (*Behindertengleichstellungsgesetz* or BGG). This also brings German law more in line with EU anti-discrimination law.

[33] Katharina C Heyer, 'The ADA on the Road: Disability Rights in Germany' (2002) 27 Law & Social Inquiry 723.

[34] Swantje Köbsell, 'Towards Self-Determination and Equalization: A Short History of the German Disability Rights Movement' (2006) 26 Disability Studies Quaterly o. A., 1.

The SGB IX demands that employers adapt the workplace for people with disabilities, for instance Section 81(4) 5 "*Ausstattung ihres Arbeitsplatzes mit den erforderlichen technischen Arbeitshilfen*."

General anti-discrimination law in Germany was also further strengthened with the passage of the General Equal Treatment Act (*Allgemeines Gleichbehandlungsgesetz* or AGG) in 2006. The passage of this law was relatively fraught.[35] The AGG, amongst other things, prohibits discrimination on the basis of a disability. It also includes "all areas of working life, from vocational education and training to job applications to rules on ending an employment relationship."[36]

Also, the Works Constitution Act (*Betriebsverfassungsgesetz* or BetrVG), which governs the workplace and co-determination, creates an obligation for works councils at Section 80(1)4 "to promote the rehabilitation of severely handicapped persons and other persons in particular need of assistance."

Regulations for building accessibility are relatively well defined and coherent.[37] There are accessibility DIN standards, which help define the "*Stand der Techik*" and building regulations that include specific accessibility requirements exist at federal, state and sometimes town/city level. There are also clear regulations for public transport, including railways and stations. There are various ongoing reforms of the disability laws, including the *Bundesteilhabegesetz* (BTHG) which has a long roadmap.

[35] Mario Peucker, 'Equality and Anti-Discrimination Approaches in Germany' [2007] European Forum for Migration Studies 1.

[36] As per the English language guide to the AGG via the BMAS website. *http://www.antidiskriminierungsstelle.de/SharedDocs/Downloads/EN/publikationen/agg_wegweiser_engl_guide_to_the_general_equal_treatment_act.html*

[37] For an overview, see the guide from the Federal Ministry for Environment, Nature Conservation, Building and Nuclear Safety. *http://www.bmu.de/fileadmin/Daten_BMU/Pools/Broschueren/barrierefreies_bauen_leitfaden_en_bf.pdf*

There is a second National Action Plan, NAP 2.0[38] to accommodate the UNCRPD requirements.

5.4.1 What is the German legal position for web accessibility?

Public sector:

In 2002, the Federal Ministry of the Interior and the Ministry of Labour and Social Affairs issued the Ordinance on the Creation of Barrier-Free Information Technology (BITV), as per the BGG Section 11 1(2). This only applies to federal information technologies. The BITV was updated in 2011 to BITV 2.0 and is now closely aligned with WCAG 2.0, with some additions for non-web technologies. At state level, it is more disjointed, with an inconsistent application of the BITV standard.[39]

Private sector:

German law does not create a direct obligation on private companies to make their websites accessible, and there is no equivalent in German law to the US concept of a place of public accommodation. The BGB does create the possibility of target agreements (*Zielvereinbarungen*) between companies and organizations representing people with disabilities, but only a small number of these agreements has been negotiated.[40] The BRK-Allianz note that over a period of ten years, only 25 target agreements have been negotiated. The most recent one was in 2015.[41] In the private sector, work councils and the specific representatives of people

[38] *http://www.bmas.de/DE/Schwerpunkte/Inklusion/nationaler-aktionsplan-2-0.html*

[39] Discussion with Dr Thorsten Schwarz, at the SZS KIT, December 2017.

[40] First Civil Society Report on the Implementation of the UN Convention on the Rights of Persons with Disabilities in Germany available at *http://www.brk-allianz.de/attachments/article/93/Alternative_Report_German_CRPD_Alliance_final.doc*

[41] The target agreement register at *http://www.bmas.de/DE/Themen/Teilhabe-behinderter-Menschen/Zielvereinbarungen/Zielvereinbarungsregister/inhalt.html*

with disabilities (*Schwerbehindertenvertretung*) play a role in encouraging corporations to improve their accessibility efforts, but it is a negotiation, rather than an obligation to meet a standard, as in the public sector. Some companies in Germany are more proactive, for instance Allianz has a *Kompetenzzentrums Ergonomie & Usability.*[42] This group works with suppliers and internal developers to make solutions more accessible. Some organizations have created voluntary UNCRPD action plans.

5.4.2 German web accessibility law summary

At federal level, accessibility is clearly defined in law with the BITV 2.0. The lack of a clear, defined obligation for web accessibility in the private sector is puzzling, given the SGB IX obligations for an accessible workplace, as is the lack of case law to challenge that position. The moves to align German law with both EU law and the UNCRPD is progressing, but very slowly.

5.5 UK: Pioneering law: The Disability Discrimination Act of 1995

As with the US and Germany, activism and direct action from people with disabilities drove the push for anti-discrimination legislation in the UK in the 1980s and 1990s.[43]

With regards to website accessibility, the UK disability discrimination law position is far clearer and more straightforward than either the German or

[42] See *http://www.barrierefreiheit.de/tl_files/bkb-downloads/barrierefrei_arbeiten/vorausschauende_barrierefreiheit_im_arbeitsleben_teil2_barrierefrei.pdf* and *https://www.allianz.com/de/nachhaltigkeit/artikel/barrierefreie-software/*

[43] Alison Adam and David Kreps, 'DISABILITY AND DISCOURSES OF WEB ACCESSIBILITY' (2009) 12 Information, Communication & Society 1041, 1049.

the US position. The law clearly outlines the rights of people with disabilities, and there is little debate about the applicability of the disability law to websites. The DDA stated:

> *"It is unlawful for a provider of services to discriminate against a disabled person [...] in refusing to provide, or deliberately not providing, to the disabled person any service which he provides, or is prepared to provide, to members of the public."*[44]

and

> *"Where a provider of services has a practice, policy or procedure which makes it impossible or unreasonably difficult for disabled persons to make use of a service which he provides, or is prepared to provide, to other members of the public, it is his duty to take such steps as it is reasonable, in all the circumstances of the case, for him to have to take in order to change that practice, policy or procedure so that it no longer has that effect."*[45]

At first, there was some confusion whether this applied to websites or not, but in 2002 a binding code of practice was published. This makes it clear that websites providing services must be accessible. The code includes the following example, "An airline company provides a flight reservation and booking service to the public on its website. This is a provision of a service and is subject to the Act."[46]

Under the DDA, public sector website operators have stricter obligations than do private sector organizations such as retailers to provide accessible

[44] Disability Discrimination Act 1995 19(1)(a)

[45] DDA 21(1)

[46] The Disability Discrimination Code of Practice (Goods, Facilities, Services and Premises) Order 2002

content. The code requires the public sector organizations to have due regard to the need to promote disability equality in everything they do. This includes considering disability equality in the procedure of services. In 2010, the DDA and other anti-discrimination laws (Equal Pay Act, Sex Discrimination Act, and the Race Relations Act) were combined into a single law. This was in part to bring UK law into alignment with EU law (Equal Treatment Directive), but also to clean up what was apparently a rather inconsistent and overlapping situation.

The British Standards Institute has also published standards guidelines to help organizations comply with the Equality Act. The work on the standards began with the 2006 PAS 78, which was then superseded by BS8878. The BSI notes “BS 8878 has been designed to introduce accessibility, usability and user experience for disabled people to non-technical professionals, some of whom may be completely new to this subject. It gives guidance on process, rather than on technical and design issues, but refers to WCAG standards. BS 8878 will be of interest to web developers and those who have an interest in the success of an organization’s website (as employee or customer).”[47]

5.5.1 The curious lack of case law

Adams and Kreps note “Although the UK DDA (1995) was the first legislation of its type in Europe it was regarded as weak and difficult to apply – importantly cost and ease of access to legal representation was seen as a major barrier.”[48] The lack of case law would seem to validate this. Until 2012, there was no case law in the UK addressing web accessibility. Previously, the RNIB (Royal National Institute for Blind People) had threatened two organizations with legal action and they settled out of court, without being named. In 2000, the RNIB named and shamed various UK organizations for their failure to address web accessibility. The RNIB has

[47] *https://www.abilitynet.org.uk/accessibility-services/BS8878-Summary*

[48] ibid.

been involved in working with a number of organizations to improve their accessibility. Tesco, a major supermarket, actually launched a separate accessible website for its online channel and then found that sighted users actually preferred that version.[49]

BMI Baby was the low cost airline subsidiary of BMI. In 2010, a member of the RNIB complained about the accessibility of the site. According to the RNIB, it tried to work with BMI to improve website accessibility, but made little progress. They then decided to take the matter to court. Given that the UK guidelines for web accessibility actually reference an airline website scenario, it seemed unlikely that BMI's defence would succeed. The case did not progress, as BMI stopped operating as a business soon after.

UK law is clear and without much ambiguity. The code of conduct clearly spells out the obligations of organizations, and the BS standard also provides solid guidance for developers to build accessible websites. There has not been aggressive litigation in the UK, but the RNIB has been effective in the situations where it has been actively involved. The charity organization, AbilityNet, has been active in auditing websites for accessibility issues, and then naming and shaming those that fail, and praising those that succeed.

However, the charity chair recently highlighted his frustration with the lack of government action in terms of enforcement:

> *"This Global Accessibility Awareness Day (GAAD), I'm writing an open letter to the UK government asking it to*

[49] *http://isolani.co.uk/blog/access/TescoAccess*
October 2003 Julie Howell, digital policy development officer at RNIB, told me: "Work undertaken by Tesco.com to make their home grocery service more accessible to blind customers has resulted in revenue in excess of £13m per annum, revenue that simply wasn't available to the company when the website was inaccessible to blind customers."
http://www.sean.co.uk/a/webdesign/accessibility.shtm

> *check that the websites and apps of companies, organisations and public sector adhere to the accessibility standards legally required under the Equality Act 2010. You can barely leave your car one minute over time without getting a parking ticket, but where are the government's wardens of the internet? Why can't every law be enforced equally? The Equality Act states that those supplying goods and services, as well as employers and schools, should make reasonable adjustments to ensure that what they offer is accessible to people with disabilities. The standards are clear and reflect global requirements - the trouble is that our authorities don't appear to feel that checking for compliance is their job?*[50]

The UK government was recently criticized by the UNCRPD committee in an "Inquiry concerning the United Kingdom of Great Britain and Northern Ireland carried out by the Committee under article 6 of the Optional Protocol to the Convention."[51] The report makes uncomfortable reading.

"Consequently, the Committee considers that there is reliable evidence that the threshold of grave or systematic violations of the rights of persons with disabilities has been met in the State party." The UK government disagreed with the findings, but the response of the disability organizations to the report and the government response is illustrative of the extent of issues for people with disabilities in the UK.[52] In an environment where broader accessibility and disability support mechanisms are being cut, it is unlikely that web accessibility will receive assertive or adequate government attention.

[50] *https://www.abilitynet.org.uk/news-blogs/open-letter-government-please-ensure-websites-and-apps-comply-legal-accessibility*

[51] CRPD/C/15/R.2/Rev.1 *http://www.ohchr.org/EN/HRBodies/CRPD/Pages/InquiryProcedure.aspx*

[52] See *http://www.ohchr.org/Documents/HRBodies/CRPD/FollowUpSubmissionUK.doc*

5.5.2 UK Web accessibility law summary

Both public sector and private sector positions are well defined in law and there are clear guidelines via the BS 8878 standard. However, there is a curious lack of case law, and government has been unwilling to drive much in the way of assertive enforcement. The current government is perceived by accessibility advocates and the UNCRPD as being regressive.

5.6 The role of the United Nations in disability rights

Just over a decade ago, the first major Human Rights instrument of this century was adopted, The United Nations Convention on the Rights of Persons with Disabilities. It was negotiated in less than 4 years, which makes it the fastest human rights treaty negotiation, and it has a very high level of signatories and ratifications. The convention requires states, in accordance with their legal and administrative systems, to maintain, strengthen, designate or establish a framework to promote, protect and monitor implementation of the convention.[53] It was rapidly adopted and ratified by the vast majority of countries.[54]

> *The convention has been lauded as innovative because it actually involved disabled persons and their representatives in its drafting, rather than being simply drafted from on high.*
>
> *Tantamount in importance, Member States were formally encouraged by the Ad Hoc Committee to incorporate persons with disabilities and/ or other experts on disability into*

[53] See *https://www.un.org/development/desa/disabilities/resources/general-assembly/convention-on-the-rights-of-persons-with-disabilities-ares61106.html*

[54] It is unfortunate the US has not yet ratified the convention.

> *their official delegations at meetings, as well as to consult with them at home in the preparatory process in establishing positions and priorities. Virtually all Member States obliged, actively incorporating persons with disabilities either as official heads of delegation…or as official advisors.* [55]

The CRPD was greeted with considerable enthusiasm by disability experts.[56] For instance, Ferri called it "revolutionary".[57] States party to the convention are obliged to bring their legal frameworks in line with the CRPD's core concepts of self-determination, equality, non-discrimination, participation, inclusion and accessibility. The CRPD's central purpose is to promote, protect and ensure the full and equal enjoyment of all human rights and fundamental freedoms by all persons with disabilities and to promote respect for their inherent dignity." Accessibility features as a general principle in Article 3, and it is laid down more fully as a specific obligation in Article 9. It places information accessibility in the same context as physical accessibility. Article 9.2(g) calls on countries to promote accessibility to new information technologies, such as the internet. Article 9.2(h) calls on countries "To promote the design, development, production and distribution of accessible information and communications technologies and systems at an early stage, so that these technologies and systems become accessible at minimum cost." This is basically a call for both universal design and AT systems investment.

[55] Tracy Justesen and Troy Justesen, 'An Analysis of the Development and Adoption of the United Nations Convention Recognizing the Rights of Individuals with Disabilities: Why the United States Refuses to Sign This UN Convention.' (2007) 14 Human Rights Brief 36, 47.

[56] Catherine Easton, 'Revisiting the Law on Website Accessibility in the Light of the UK's Equality Act 2010 and the United Nations Convention on the Rights of Persons with Disabilities' (2012) 20 International Journal of Law and Information Technology 19; Justesen and Justesen; Blanck, 'eQuality'.

[57] Delia Ferri, G Anthony Giannoumis and Charles Edward O'Sullivan, 'Fostering Accessible Technology and Sculpting an Inclusive Market through Regulation' (2015) 29 *International Review of Law, Computers and Technology* 81.

Article 2 states "universal design" means the design of products, environments, programmes and services to be usable by all people, to the greatest extent possible, without the need for adaptation or specialized design. "Universal design" shall not exclude assistive devices for particular groups of persons with disabilities where this is needed. Article 4(f) requires countries to promote universal design. Article 4 (g) demands that countries promote R&D research.

The CRPD is a comprehensive treaty, and it clearly lays out both anti-discrimination (i.e. first generation rights) and positive rights. It promotes independent living, mobility and rehabilitation, and emphasizes the rights of women and children with disabilities.[58] It clearly articulates the positive role technology can play in helping people to enjoy their fundamental human rights.

5.6.1 Moving from UN treaty into national actor action

Many things are discussed and signed at UN level, but they do not always lead to improved human rights at national level.[59] However, the CRPD has led to the passage of legislation, strategies or progress in that direction in many countries. An example of the influence of the CRPD is the dialogue between the CPRD and the EU. In 2016, the EU published a report outlining its progress towards meeting the requirements of the CRPD.[60]

[58] Michael Ashley Stein, 'Quick Overview of the United Nations Convention on the Rights of Persons with Disabilities and Its Implications for Americans with Disabilities' (2007) 31 Mental & Physical Disability Law Reporter.

[59] Eric Neumayer, 'Do International Human Rights Treaties Improve Respect for Human Rights?' 925.

[60] European Disability Strategy 2010-2020, COM (2010) 636 final, available at: *http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0636:FIN:en:PDF*; see also *http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/536347/EPRS_IDA(2016)536347_EN.pdf*

For instance, the CRPD committee has urged the EU to swiftly adopt a European Accessibility Act. Uerpmann-Wittzack notes that the Committee on the Rights of Persons with Disabilities has developed a highly qualified advocacy capability.[61] While the US has signed the treaty, it has so far failed to ratify it. While the ADA was the inspiration for the CRPD, the CRPD goes beyond the scope of the ADA.

5.6.2 UN accessibility law summary

There is a well formulated UN treaty for the rights of people with disabilities, which clearly establishes right to accessible technologies and highlights the positive benefits of technology to assist people with disabilities to exercise their human rights. This treaty is bringing about a shift in national laws in many countries, and the UN is being relatively assertive in its efforts to enforce the treaty, monitoring disability rights (see UK example above).

5.7 EU law and activity

In 2010, the Commission outlined its 10-year strategy for a renewed Commitment to a Barrier-Free Europe.[62] It notes the importance of the UNCRPD and outlines the main areas for action: Accessibility, Participation, Equality, Employment, Education and Training, Social Protection, Health and External Action.

[61] Robert Uerpmann-Wittzack, 'Die UN-Behindertenrechtskonvention in Der Praxis Des Ausschusses Für Die Rechte von Menschen Mit Behinderungen' (2016) 54 Archiv des Völkerrechts 181.

[62] See http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2010/0636/COM_COM(2010)0636_EN.pdf

There is a variety of EU level instruments that relate to specific elements of disability rights, but as of yet there is no comprehensive disability / accessibility legislation in force. Disability is mentioned for instance in the Directive 2000/78/EC (General framework for equal treatment in employment and occupation). In terms of accessibility, there are regulations for transport,[63] for instance, and there is a variety of regulations relating to the built world accessibility, but this is rather fragmented.

5.7.1 EU web accessibility

Public procurement is used by both national governments and the EU to influence vendor behaviour across many industries[64], for instance to address negative externalities. Example mandates include EU Mandate 389 for standardized sunscreen testing and labelling, and Mandate 420 to support European accessibility requirements for public procurement in the built environment.

In 2005, the Commission sent a standardization mandate (Mandate 376). This was an instruction to the European standards organizations (CEN, CENELEC and ETSI) to "assist with the harmonisation of public procurement practices in Europe by developing a standard that specifies the functional accessibility requirements for publicly procured ICT products and services."[65] One of the aims of Mandate 376 was to create a requirement that was similar to the Section 508 standards in the US.[66]

[63] *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R1300*
see Commission Regulation (EU) No 1300/2014 of 18 November 2014 on the technical specifications for interoperability relating to accessibility of the Union's rail system for persons with disabilities and persons with reduced mobility.

[64] Jakob Edler and Luke Georghiou, 'Public Procurement and Innovation-Resurrecting the Demand Side' (2007) 36 Research Policy 949.

[65] *http://mandate376.standards.eu/background*

[66] Jonathan Lazar, Daniel (Lawyer) Goldstein and Anne Taylor, *Ensuring Digital Accessibility through Process and Policy*.

The mandate created two deliverables:

- The Standard EN 301 549
- The Accessible procurement toolkit

The standard was adopted in 2014. At the time of writing, use of the standard is voluntary. The toolkit is detailed, enabling procurement managers to generate specific tender requirements.[67] Adoption of the toolkit and EN 301 549 in public sector procurement is ongoing, for example Sweden's post and telecom authority has issued guidelines, and note that compliance is now mandatory under Swedish law.[68] Other countries outside Europe are adopting the standard, for instance, Australia.[69] Vendors are reacting to the mandate, for example, Microsoft have published a position paper and have declared their conformance for various products, publishing VPATs publically.[70]

Of specific relevance to public sector web accessibility, Directive 2016/2102, On the Accessibility of the Websites and Mobile Applications of Public Sector Bodies, sometimes called the web accessibility or the Digital Accessibility Directive is key. Member states have until September 2018 to implement this Directive into national law. The Commission will publish implementing acts by December 2018 with details of the technical standards. These will consist of:

- A model accessibility statement
- Technical specifications for the accessibility requirements in the Directive

[67] See *http://mandate376.standards.eu/*

[68] *https://www.pts.se/globalassets/startpage/dokument/icke-legala-dokument/rapporter/2016/ovrigt/guidance-for-the-accessibility-standard-en-301-5491.pdf*

[69] Gunela Astbrink and William Tibben, 'The Role of Public Procurement in Improving Accessibility to ICT' (2013) 63 Telecommunications Journal of Australia.

[70] *https://enterprise.microsoft.com/en-us/articles/industries/government/en-301-549-reports-for-microsoft-products/*

- A methodology for monitoring the conformity of websites and mobile applications with the accessibility requirements in the Directive
- Arrangements for reporting by Member States to the Commission

In the meantime, public sector bodies should be using standard EN 301 549 for procurement and development of solutions. By September 2019, all websites created after September 2018 need to be accessible. By Sept 2020, all websites should be accessible and, by June 2021, all mobile applications should be accessible.[71]

The Directive notes in the recitals the need to function more consistently as a harmonized market, the importance of consistent technical standards, and the need for an effective remedy procedure.

Article 4 makes direct use of the wording of the WCAG principles, i.e. “perceivable, operable, understandable and robust.” and article 6 (2) establishes the EN 301 549 compliance as the minimum standard. The Directive does not determine enforcement procedures, leaving that to the individual countries.

The mandate and this Directive will drive a more coherent and consistent web accessibility strategy in the public sector. However, the position in the private sectors remains highly fragmented, as illustrated by the lack of formal obligations in Germany for accessibility.

The regulation of private sector accessibility has been slow in coming, but it is on the way, given the Proposal for a Directive of the European Parliament and of the Council on the approximation of the laws, regulations and administrative provisions of the Member States as regards the accessibility requirements for products and services.[72] It is known as the

[71] For a good overview of the Directive, see the European Disability forum toolkit. *http://www.edf-feph.org/newsroom/news/edf-toolkit-web-accessibility-Directive*

[72] *http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/603973/EPRS_BRI(2017)603973_EN.pdf*

European Accessibility Act (EEA). It was originally planned to be adopted in 2012, but it has been delayed several times. The proposal is currently at an advanced stage (the trilogue talks began in March 2018), having been approved in the EU Parliament. The act aims to regulate a variety of products and services in a variety of fields: phones, computers, cash machines, public transport, including underground, rail, trams and buses. The EBU (European Blind Union, an NGO) recently raised concerns that the act has been watered down considerably, as have other NGOs. Business forums are concerned about the cost of compliance.

Expect further work on the Accessibility Act during 2018. However, given the slow progress to date, the timing and extent of the impact on web accessibility requirements is hard to quantify.

5.7.2 EU web accessibility summary

European-wide standards are now defined, building upon the WCAG 2.0 principles, via EN 301 459. European efforts to bring about EU-wide regulations for accessibility, in alignment with the CPRD, are moving forward gradually. In the shorter term, the public sector procurement instruments should help drive a more consistent and diligent approach to web accessibility in the public sector. Private sector web accessibility will face closer scrutiny, but it will be several years until there is a consistent legal framework for driving better web accessibility at a national level.

5.8 Summary: Web accessibility law generally

The research observation noted more than 10% of the world's population has some form of disability. Accessibility is well established as a human right in UN, EU and many national laws, yet most web applications are not accessible. This chapter has shown that law-makers have largely failed to create a legal framework that effectively encourages or enforces accessible web software development. The position of web accessibility in law remains messy, but it is gradually moving toward a clearer enforcement of the WCAG principles. The UNCRPD is helping to drive broader international consistency, even though the US has yet to ratify it. Enforcement remains sporadic at best.

By exploring the laws that relate to accessibility, this chapter has provided a foundation for the lab test in chapter 6.

6 Assessing accessibility empirically

6.1 Chapter purpose: Assessing accessibility in a practical context

The main purpose of this chapter is to examine the career site accessibility of 10 German organizations through a combination of lab testing with blind and visually impaired testers, and also two automated tests: one of the websites, the other of PDFs.

It is useful to briefly review some of the other accessibility tests that have been done over the last 15 years or so. The review is by no means exhaustive. Other than the Lazar[1] and Bruyere[2] studies in the US, no other studies of corporate career site accessibility were found in the literature search.

Before examining the career site, the chapter provides a brief overview of modern recruitment software usage in order to place the empirical assessment in context.

6.1.1 Accessibility test literature review

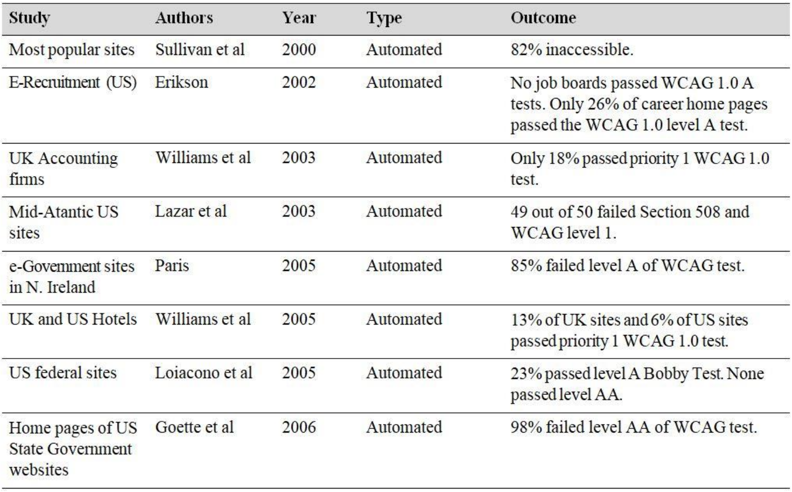
The author performed a literature review of web accessibility tests. These tests typically assess websites using automated tools. Some tests do manual assessments, and yet fewer actually involve people with disabilities

[1] Jonathan Lazar, Abiodun Olalere and Brian Wentz, 'Investigating the Accessibility and Usability of Job Application Web Sites for Blind Users' (2012) 7 Journal of Usability Studies 68.

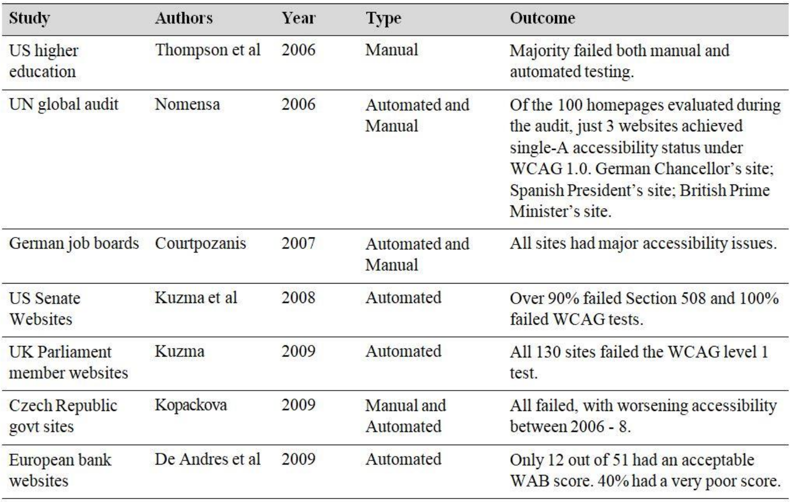
[2] Susanne M Bruyère and others, 'Information Technology and the Workplace: Implications for Persons with Disabilities' (2005) 25 Disability Studies Quarterly.

to do the testing. Irrespective of the method, the tests all bring back generally similar results. The search failed to discover any research that showed a research sample with a majority of sites that were highly accessible. The pervasive theme over the last 20 years or so is that websites are generally not accessible. Several papers did point-in-time assessments, and showed little or no improvements over time. Some actually noted a regression, as websites deployed more sophisticated features that lack accessibility. The list below is by no means complete, but it is extensive.

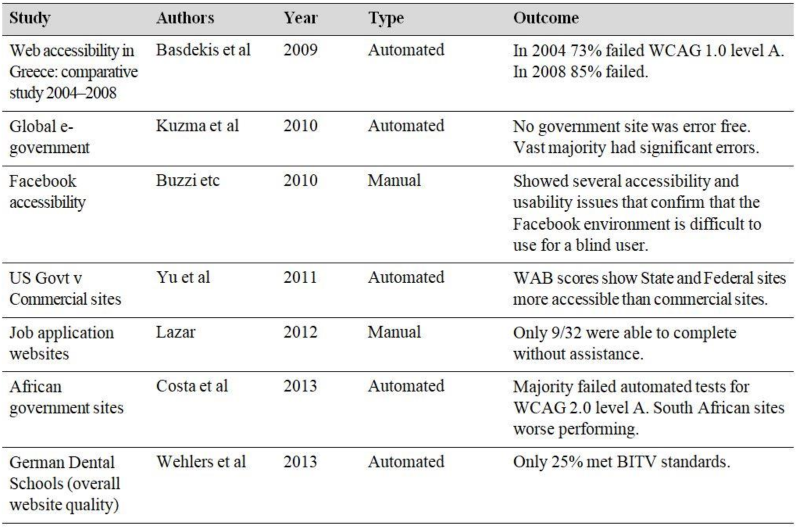
Table 6.1: Summary of various accessibility tests



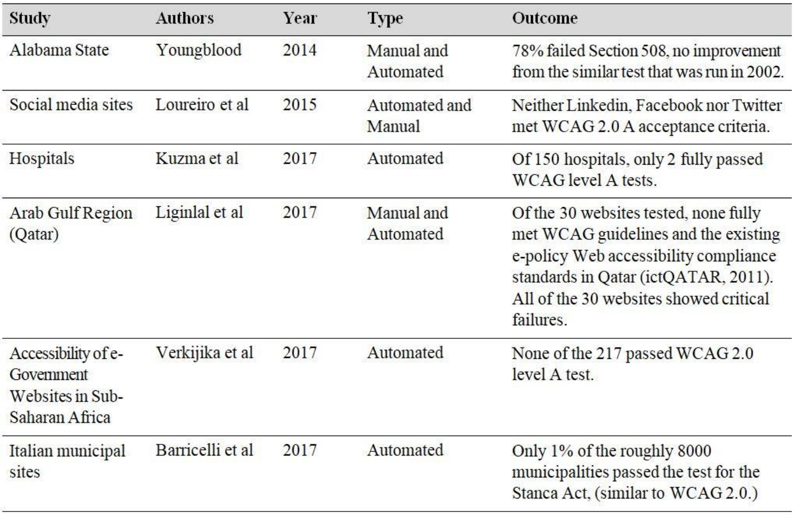
Study	Authors	Year	Type	Outcome
Most popular sites	Sullivan et al	2000	Automated	82% inaccessible.
E-Recruitment (US)	Erikson	2002	Automated	No job boards passed WCAG 1.0 A tests. Only 26% of career home pages passed the WCAG 1.0 level A test.
UK Accounting firms	Williams et al	2003	Automated	Only 18% passed priority 1 WCAG 1.0 test.
Mid-Atantic US sites	Lazar et al	2003	Automated	49 out of 50 failed Section 508 and WCAG level 1.
e-Government sites in N. Ireland	Paris	2005	Automated	85% failed level A of WCAG test.
UK and US Hotels	Williams et al	2005	Automated	13% of UK sites and 6% of US sites passed priority 1 WCAG 1.0 test.
US federal sites	Loiacono et al	2005	Automated	23% passed level A Bobby Test. None passed level AA.
Home pages of US State Government websites	Goette et al	2006	Automated	98% failed level AA of WCAG test.



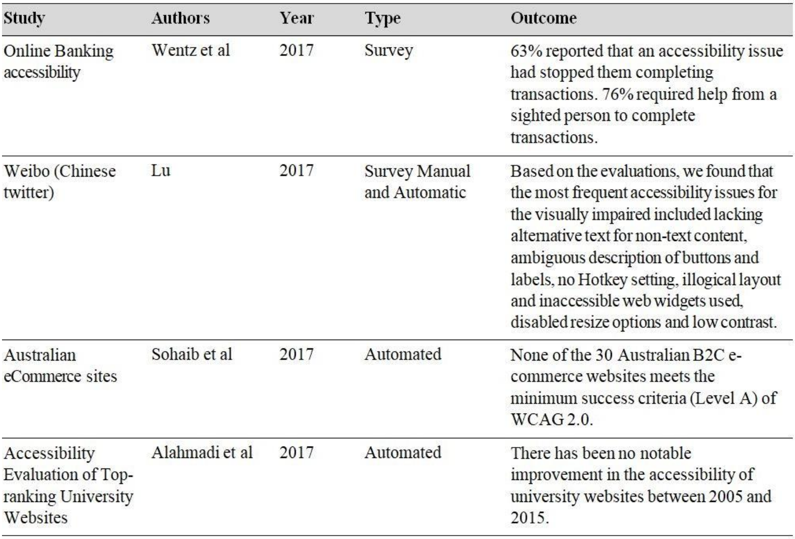
Study	Authors	Year	Type	Outcome
US higher education	Thompson et al	2006	Manual	Majority failed both manual and automated testing.
UN global audit	Nomensa	2006	Automated and Manual	Of the 100 homepages evaluated during the audit, just 3 websites achieved single-A accessibility status under WCAG 1.0. German Chancellor's site; Spanish President's site; British Prime Minister's site.
German job boards	Courtpozanis	2007	Automated and Manual	All sites had major accessibility issues.
US Senate Websites	Kuzma et al	2008	Automated	Over 90% failed Section 508 and 100% failed WCAG tests.
UK Parliament member websites	Kuzma	2009	Automated	All 130 sites failed the WCAG level 1 test.
Czech Republic govt sites	Kopackova	2009	Manual and Automated	All failed, with worsening accessibility between 2006 - 8.
European bank websites	De Andres et al	2009	Automated	Only 12 out of 51 had an acceptable WAB score. 40% had a very poor score.



Study	Authors	Year	Type	Outcome
Web accessibility in Greece: comparative study 2004–2008	Basdekis et al	2009	Automated	In 2004 73% failed WCAG 1.0 level A. In 2008 85% failed.
Global e-government	Kuzma et al	2010	Automated	No government site was error free. Vast majority had significant errors.
Facebook accessibility	Buzzi etc	2010	Manual	Showed several accessibility and usability issues that confirm that the Facebook environment is difficult to use for a blind user.
US Govt v Commercial sites	Yu et al	2011	Automated	WAB scores show State and Federal sites more accessible than commercial sites.
Job application websites	Lazar	2012	Manual	Only 9/32 were able to complete without assistance.
African government sites	Costa et al	2013	Automated	Majority failed automated tests for WCAG 2.0 level A. South African sites worse performing.
German Dental Schools (overall website quality)	Wehlers et al	2013	Automated	Only 25% met BITV standards.



Study	Authors	Year	Type	Outcome
Alabama State	Youngblood	2014	Manual and Automated	78% failed Section 508, no improvement from the similar test that was run in 2002.
Social media sites	Loureiro et al	2015	Automated and Manual	Neither Linkedin, Facebook nor Twitter met WCAG 2.0 A acceptance criteria.
Hospitals	Kuzma et al	2017	Automated	Of 150 hospitals, only 2 fully passed WCAG level A tests.
Arab Gulf Region (Qatar)	Liginlal et al	2017	Manual and Automated	Of the 30 websites tested, none fully met WCAG guidelines and the existing e-policy Web accessibility compliance standards in Qatar (ictQATAR, 2011). All of the 30 websites showed critical failures.
Accessibility of e-Government Websites in Sub-Saharan Africa	Verkijika et al	2017	Automated	None of the 217 passed WCAG 2.0 level A test.
Italian municipal sites	Barricelli et al	2017	Automated	Only 1% of the roughly 8000 municipalities passed the test for the Stanca Act, (similar to WCAG 2.0.)



Study	Authors	Year	Type	Outcome
Online Banking accessibility	Wentz et al	2017	Survey	63% reported that an accessibility issue had stopped them completing transactions. 76% required help from a sighted person to complete transactions.
Weibo (Chinese twitter)	Lu	2017	Survey Manual and Automatic	Based on the evaluations, we found that the most frequent accessibility issues for the visually impaired included lacking alternative text for non-text content, ambiguous description of buttons and labels, no Hotkey setting, illogical layout and inaccessible web widgets used, disabled resize options and low contrast.
Australian eCommerce sites	Sohaib et al	2017	Automated	None of the 30 Australian B2C e-commerce websites meets the minimum success criteria (Level A) of WCAG 2.0.
Accessibility Evaluation of Top-ranking University Websites	Alahmadi et al	2017	Automated	There has been no notable improvement in the accessibility of university websites between 2005 and 2015.

6.1.2 Key findings from the web site accessibility literature review

- The vast majority of sites fail basic accessibility tests, whether those tests are conducted with automated tools or by manual testing.
- Many sites have usability issues, which compound accessibility issues.
- There is little sign of improvement between the early 2000s and today.
- Countries with accessibility laws are only marginally more accessible than those without.
- Public sector organizations are better than private sector organizations, but not significantly better.
- Many of the studies note that the majority of errors are easy to fix.
- “Improvements” in application design can result in a reduction in accessibility.

6.1.3 The alt-text problem in web sites

It is clear that the most common problem is the non-use or incorrect use of alt-text.[3] Alt-text is a word or phrase that can be inserted into the website or document to describe an attribute, for instance an image or field. McEwan did an extensive meta-study of accessibility reports and noted that alt-text is the most fundamental accessibility problem in commercial website development. A more recent study of Australian e-Commerce sites noted that 65% of pages had some sort of alt-text error, such as a label missing. 55% of pages had problems with labels on input fields.[4]

[3] Tom McEwan and Ben Weerts, ‘ALT Text and Basic Accessibility’, *Proceedings of the 21st British HCI Group Annual Conference on People and Computers: HCI...but not as we know it - Volume 2* (British Computer Society 2007).

[4] Sohaib and Kang.

As noted in the flowing chapter, automated testing tools cannot identify all of the accessibility problems on a site. However, automated testing tools can easily note the absence of alt text. Alt text is also easy to fix. This means:

- Either organizations are not doing much accessibility testing.
- Or they do the testing, but then fail to fix the errors.

Causes of accessibility failure will be explored in more detail in the next chapter.

6.2 Human rights, disability, accessibility and employment

This section will provide the context for the lab assessment. Recruitment is a sophisticated business process, and one that has significant legal and ethical implications. The study will examine how the recruitment websites of organizations treat people with disabilities.

Employment is a fundamental element of modern society. There is a significant relationship between self-esteem and job satisfaction. This has been well established in workplace research since the 1930s, and also in the context of people with disabilities.[5]

The right to work is enshrined in Article 23 of the Universal Declaration of Human Rights, for instance:

> *Everyone has the right to work, to free choice of employment, to just and favourable conditions of work and to protection against unemployment.*

[5] D Griffin and others, ‘A Comparison of Self-Esteem and Job Satisfaction of Adults with Mild Mental Retardation in Sheltered Workshops and Supported Employment’ (1996) 31 Education and Training in Mental Retardation and Developmental Disabilities 142.

A significant portion of accessibility legislation is concerned with access to employment, and employment conditions. Article 27 UNCRPD recognizes

> *The right of persons with disabilities to work, on an equal basis with others; this includes the right to the opportunity to gain a living by work freely chosen or accepted in a labour market and work environment that is open, inclusive and accessible to persons with disabilities.*

The ADA requires employers to accommodate disabled workers and outlaws discrimination against the disabled in hiring, firing and pay. As noted earlier, the first disability legislation during World War I focused on making disabled soldiers more employable. In the UK, the DDA[6] and its successor, the 2010 Equality Act, also focus on removing employment discrimination for people with disabilities.

In Germany, the AGG, the *Betriebsverfassungsgesetz* (BetrVG) and the SGB IX create rights for disabled employees. For instance, organizations with more than 20 employees are required to fill 5% of jobs with people with severe disabilities.[7] Most companies do not achieve this, choosing instead to pay a modest compensation penalty. This levy is used to fund training and other rehabilitation initiatives.[8].

In Germany, the unemployment rate for severely disabled people reached 14.8% in 2011, while the general unemployment rate was 7.9%.[9] In the US, unemployment levels for people with disabilities are more than double

[6] Disability Discrimination Act of 1995. *http://www.legislation.gov.uk/ukpga/1995/50/contents*

[7] §71 SGB IX. Neuntes Buch des Sozialgesetzbuches.

[8] Martin Kock, 'Disability Law in Germany: An Overview of Employment, Education and Access Rights' (2002) 5 German Law Journal 1373.

[9] See Alliance of German Non-Governmental Organizations Regarding the UN Convention on the Rights of Persons with Disabilities Report at *http://www.brk-allianz.de/attachments/article/93/Alternative_Report_German_CRPD_Alliance_final.doc* page 6.

for those without a disability[10]. The ratio in the EU is similar.[11] While legislation supposedly protects and promotes the employment of people with disabilities, it has been firmly argued that the law has not really helped in increasing employment levels. For instance, ADA has not helped to improve the employment rate of people with disabilities[12]. A similar criticism has been made of the UK DDA.[13]

6.3 The war for talent, employer branding and recruiting software

The strategies and processes that modern organizations deploy in recruiting their workforce are increasingly sophisticated. This section will provide a brief overview of modern recruiting and the technologies that support it.

In 1998, McKinsey Consulting published a study called the War for Talent.[14] It was widely cited by business media, and has set much of the agenda for recruitment strategy ever since. A search on 'war for talent' brings up numerous academic and business magazine articles, herewith a

[10] Bureau of Labor Statistics, 'Persons with a Disability: Labor Force Characteristics Summary' (2017) <https://www.bls.gov/news.release/disabl.nr0.htm> accessed 26 October 2017.

[11] Eurostat, 'Disability Statistics - Labour Market Access' [2014] 2014.

[12] Daron Acemoglu and Joshua D Angrist, 'Consequences of Employment Protection? The Case of the Americans with Disabilities Act' (2001) 109 Journal of Political Economy 915.

[13] David Bell and Axel Heitmueller, 'The Disability Discrimination Act in the UK: Helping or Hindering Employment among the Disabled?' (2009) 28 Journal of Health Economics 465.

[14] Elizabeth G Chambers and others, 'The War for Talent' [1998] McKinsey Quarterly 44.

sample.[15] While the headline caught the imagination of business and HR leaders, the underlying message was that the competition for top talent would intensify. Organizations would need to invest more strategically in their processes and techniques to source and recruit. This provided a sales hook for software vendors to aggressively sell recruitment software.

Also, since the mid 1990s, Employer Brand Management developed as a corporate practice and a topic of academic interest, in both Human Resources Management and Marketing research.[16] Employer branding

[15] Anthony McDonnell, 'Still Fighting the "War for Talent"? Bridging the Science Versus Practice Gap' (2011) 26 Journal of Business and Psychology 169; Christine Quinn Trank, Sara L Rynes and Robert D Bretz, Jr., 'Attracting Applicants in the War for Talent: Differences in Work Preferences Among High Achievers' (2002) 16 Journal of Business and Psychology 331; Schon Beechler and Ian C Woodward, 'The Global "War for Talent"' (2009) 15 Journal of International Management 273; Chambers and others; Klaus Heim, 'The War for Talent' (2012) 2 MTZ industrial 72; Sarah Cliffe, 'Human Resources – Winning the War for Talent'; David Burkus and Bramwell Osula, 'Faulty Intel in the War for Talent: Replacing the Assumptions of Talent Management with Evidence-Based Strategies' (2011) 3 Journal of Business Studies Quarterly 1; E Michaels, H Handfield-Jones and B Axelrod, 'The War For Talent: Harvard Business School Press' [2001] MA., USA; Wim JL Elving and others, 'The War for Talent? The Relevance of Employer Branding in Job Advertisements for Becoming an Employer of Choice' (2013) 20 Journal of Brand Management 355; Michael Hay, 'Strategies for Survival in the War of Talent' (2002) 7 Career Development International 52; Anthony Palmer, 'The War for Talent' (2003) 148 The RUSI Journal 62.

[16] Tim Ambler and Simon Barrow, 'The Employer Brand' (1996) 4 Journal of Brand Management 185; Ralf Wilden and others, 'Employer Branding' [2013] Lebensmittel Zeitung; Eva Grobe, 'Employer Branding' (2008); Kristin Backhaus, 'Employer Branding Revisited' [2016] Organisation Management Journal; J Latzel and others, 'Perspektivwechsel Im Employer Branding', *Perspektivwechsel im Employer Branding* (2015); Jens Mattmüller, Roland; Hugo Grote, Jasper; Reif, Marcus K.; Buckmann, Jörg; Hesse, Gero; Mahlodji, Ali; Diercks, Joachim; Kupka, Kristof; Flohr, Benita; Bender, 'Fallstudien Zu Aktuellen Herausforderungen Im Employer Branding Und Personalmarketing', *Perspektivwechsel im Employer Branding* (2015); Florian Schuhmacher and Roland Geschwill, 'Employer Branding: Anleitung Zur Erarbeitung Einer Employer-Branding-Strategie', *Employer Branding Human Resources Management für die Unternehmensführung* (2009); Armin Trost, *Employer Branding* (Luchterhand in Wolters Kluwer Deutschland 2009).

represents a firm’s efforts to promote, both within and outside the firm, a clear view of what makes it different and desirable as an employer.[17] Many organizations now take a more focused and thoughtful approach to both the recruitment and retention of employees, akin to a marketing strategy.

The use of the internet for recruitment has grown dramatically, with the job board being one of the first commercial applications of the internet in the 1990s. For some time, the internet has been the dominant channel for organizations to seek out candidates, and for candidates to search for and apply for jobs.[18] By as early as 2002, 75% of HR managers used the web to advertise jobs.[19] The recruitment website plays a critical role in setting the candidate’s perception of the organization.[20]Today, it is hard to conceive of any organization, except perhaps the smallest, not using the internet as its primary recruitment channel. Over the last decade, the technologies to support the recruitment process have become ever more sophisticated,[21] with candidate relationship management applying many of the techniques of modern marketing customer relationship management to develop talent pools. In many cases, recruitment is as sophisticated as online marketing.

[17] Kristin Backhaus and Surinder Tikoo, ‘Conceptualizing and Researching Employer Branding’ (2004) 9 Career Development International 501.

[18] In Lee, ‘The Evolution of E-Recruiting: A Content Analysis of Fortune 100 Career Web Sites’ (2005) 3 Journal of Electronic Commerce in Organizations 57.

[19] Daniel C Feldman and Brian S Klaas, ‘Internet Job Hunting: A Field Study of Applicant Experiences with on-Line Recruiting’ (2002) 41 Human resource management 175.

[20] H Jack Walker and others, ‘So What Do You Think of the Organization? A Contextual Priming Explanation for Recruitment Web Site Characteristics as Antecedents of Job Seekers’ Organizational Image Perceptions’ (2011) 114 Organizational Behavior and Human Decision Processes 165.

[21] Brian R Dineen and Raymond A Noe, ‘Effects of Customization on Application Decisions and Applicant Pool Characteristics in a Web-Based Recruitment Context.’ (2009) 94 Journal of Applied Psychology 224.

Employers use social channels such as Twitter, Facebook, LinkedIn and Xing to identify and engage with potential employees.[22] Applicant feedback on use of these channels is positive, for instance, with nurse recruitment[23] or engineer recruitment.[24] There is increasing use of video and other rich media in recruitment marketing.[25] Video-based interviewing is now commonplace[26] as is online testing.[27] Software developer recruiters now mine GitHub and other developer forums for candidates.[28] This is part of the business model of these services.

While tools such as LinkedIn and Facebook provide employers with a richer information source than a traditional resume, with some caveats[29],

[22] Sherrie A Madia, 'Best Practices for Using Social Media as a Recruitment Strategy' (2011) 10 Strategic HR Review 19; Ralf Caers and Vanessa Castelyns, 'LinkedIn and Facebook in Belgium' (2011) 29 Social Science Computer Review 437.

[23] Marieke Carpentier and others, 'Recruiting Nurses through Social Media: Effects on Employer Brand and Attractiveness' (2017) 73 Journal of Advanced Nursing 2696.

[24] Anne-Mette Sivertzen, Etty Ragnhild Nilsen and Anja H Olafsen, 'Employer Branding: Employer Attractiveness and the Use of Social Media' (2013) 22 Journal of Product & Brand Management 473.

[25] Keely J Frasca and Martin R Edwards, 'Web-Based Corporate, Social and Video Recruitment Media: Effects of Media Richness and Source Credibility on Organizational Attraction' (2017) 25 International Journal of Selection and Assessment 125.

[26] Katherine Campbell and Mary Loyland, 'Video as a Recruitment Tool at " Big Four" Public Accounting Firms: Why Video Should Be Part of Accounting Curricula' (2013) 17 Academy of Educational Leadership Journal 95; Edward Hendrick, 'What Are the Pros and Cons of Using Video for Recruitment?' (2011) 10 Strategic HR Review shr. 2011.37210faa.006.

[27] Markus Langer and others, 'Dear Computer, Teach Me Manners: Testing Virtual Employment Interview Training' (2016) 24 International Journal of Selection and Assessment 312; Melanie Fröhlich, Janine Kahmann and Martina Kadmon, 'Development and Psychometric Examination of a German Video-Based Situational Judgement Test for Social Competencies in Medical School Applicants' (2017) 25 International Journal of Selection and Assessment 94.

[28] Jennifer Marlow and Laura Dabbish, 'Activity Traces and Signals in Software Developer Recruitment and Hiring', *Proceedings of the 2013 conference on Computer supported cooperative work - CSCW '13* (ACM Press 2013).

[29] Jamie Guillory and Jeffrey T Hancock, 'The Effect of LinkedIn on Deception in Resumes' (2012) 15 Cyberpsychology, Behavior, and Social Networking 135.

tools such as Glassdoor[30] provide candidates with a level of detail and transparency about the hiring organization that would have been very difficult to source even a few years ago.[31]

Nikolaou makes a strong plea for further research into the effectiveness of social networking websites, noting that despite their widespread use, it is an under-investigated topic.[32]

The search, selection and acquisition of "talent" has changed dramatically over the last 20 years. It has become an industry in its own right. The internet is the dominant channel for candidates to search for jobs and learn about employers, and for employers to engage with candidates.

The market for software solutions to manage the recruitment or the talent acquisition process, as it is sometimes known, is a significant and dynamic subset of the enterprise software market. There are various estimates of market size and growth. Pang[33] notes that the market for talent acquisition software is expected to reach 4 billion USD by 2020. It is growing at a CAGR of 7%.[34]

[30] See Glassdoor.com. It has a database of millions of interview reviews, CEO ratings, salary levels, and company reviews.

[31] Juliet F Poujol, Jeff John Tanner and Christophe Fournier, 'The Employer Brand as Perceived by Salespeople: A Study Based on Glassdoor Reviews' (2017) 4 World Academy of Science, Engineering and Technology, International Journal of Economics and Management Engineering; Ning Luo, Yilu Zhou and John Shon, 'Employee Satisfaction and Corporate Performance: Mining Employee Reviews on Glassdoor.com' [2016] ICIS 2016 Proceedings; SH DeKay, 'Peering Through Glassdoor.com. What Social Media Can Tell Us About Employee Satisfaction', *CCI Conference on Corporate Communication 2013* (2013).

[32] Ioannis Nikolaou, 'Social Networking Web Sites in Job Search and Employee Recruitment' (2014) 22 International Journal of Selection and Assessment 179.

[33] Albert Pang is a well-known software industry analyst. He analyses the market size for several software markets. https://www.appsruntheworld.com

[34] *https://www.appsruntheworld.com/top-10-talent-acquisition-software-vendors-market-forecast-2015-2020-and-customer-wins/*

While the top 10 vendors hold 60% of the market, it is an attractive market for smaller and start-up software vendors, with well over 1000 vendors offering some component of the recruitment life cycle. There is an extensive market of niche solutions to add with specific elements of the process, as well as suite vendors offering broad functionality. It is a complex ecosystem, with shifting partnerships and competition.

6.3.1 Sporadic inclusion and diversity in the recruitment process

Baron noted in 1995 that the selection and assessment of people with disabilities is a topic that has been much neglected by occupational psychologists.[35] Little has changed since then. In scanning the journals on recruitment selection, the author could find little mention of accommodation of people with disabilities in selection, despite significant discussion of justice, and ethnic,[36]physical attractiveness[37] or gender discrimination[38] in selection and advertising.

[35] Helen Baron, 'Occupational Testing of People with Disabilities: What Have We Learnt?' (1995) 3 International Journal of Selection and Assessment 207; Adrienne J Coletta and Susanne M Bruyère, 'Disability and Employment: New Directions for Industrial and Organizational Psychology'.

[36] Anne M Fiedler, 'Adverse Impact on Hispanic Job Applicants during Assessment Center Evaluations' (2001) 23 Hispanic Journal of Behavioral Sciences 102; Kathryn M Neckerman and Joleen Kirschenman, 'Hiring Strategies, Racial Bias, and Inner-City Workers' (1991) 38 Social Problems 433; Franciska Krings and José Olivares, 'At the Doorstep to Employment: Discrimination against Immigrants as a Function of Applicant Ethnicity, Job Type, and Raters' Prejudice' (2007) 42 International Journal of Psychology 406.

[37] Lucy M Watkins and Lucy Johnston, 'Screening Job Applicants: The Impact of Physical Attractiveness and Application Quality' (2000) 8 International Journal of Selection and Assessment 76; Pascale Desrumaux, Sabine De Bosscher and Véronique Léoni, 'Effects of Facial Attractiveness, Gender, and Competence of Applicants on Job Recruitment' (2009) 68 Swiss Journal of Psychology 33.

In particular, gender bias in recruitment is receiving increased academic[39] and corporate[40] interest. In the wake of recent controversies, the technology industry in particular is under pressure to become more "diverse". Being perceived as gender diverse is shown to make an organization more attractive. [41] The work on gendered wording in job advertisements[42] has encouraged the development of software solutions to detect and reduce gender bias in job advertisement texts.[43] These solutions are receiving

[38] The last few years have seen a marked increase in efforts by many organizations to improve gender diversity. Stephen L Cohen, 'The Basis of Sex Bias in the Job Recruitment Situation' (1976) 15 Human Resource Management 8; Desrumaux, De Bosscher and Léoni. Over the past 2 years, the software industry has been vocal in admitting it has a gender and ethnic diversity problem. Jeremy B Bernerth, 'Perceptions of Justice in Employment Selection Decisions: The Role of Applicant Gender' (2005) 13 International Journal of Selection and Assessment 206. A recent welcome development is the interest of some employers in neurodiversity. Janine Bosak and Sabine Sczesny, 'Gender Bias in Leader Selection? Evidence from a Hiring Simulation Study' (2011) 65 Sex Roles 234; Corinne A Moss-Racusin and others, 'Science Faculty's Subtle Gender Biases Favor Male Students.' (2012) 109 Proceedings of the National Academy of Sciences of the United States of America 16474.

[39] Danielle Gaucher, Justin Friesen and Aaron C Kay, 'Evidence That Gendered Wording in Job Advertisements Exists and Sustains Gender Inequality.' (2011) 101 Journal of Personality and Social Psychology 109.

[40] Over the past 5 years, the software industry has been vocal in admitting it has a gender and ethnic diversity problem. See for instance, SAP Business Beyond Bias, and the announcements of salesforce CEO, Marc Benioff on pay gaps.
http://www.businessinsider.com/salesforce-ceo-mark-benioff-is-trying-to-close-the-gender-pay-gap-2017-9?IR=T

[41] Cameron Wilson and Cameron, 'Hour of Code' (2014) 5 ACM Inroads 22; Christine L Hanlon, 'Recruiting G.I. Jane: An Analysis of the United States Military's Advertising Messages on Recruitment Websites.' (2016); Luis L Martins and Charles K Parsons, 'Effects of Gender Diversity Management on Perceptions of Organizational Attractiveness: The Role of Individual Differences in Attitudes and Beliefs.' (2007) 92 Journal of Applied Psychology 865.

[42] Gaucher, Friesen and Kay.

[43] See for instance Textio.com
https://globenewswire.com/news-release/2017/06/21/1027130/0/en/Textio-Ushers-In-the-Era-of-Augmented-Writing-Secures-20-Million-in-Financing-Led-by-Scale-Venture-Partners.html and Talentsonar.com. The major HR technology vendors are working on similar solutions.

considerable market and press attention. A recent welcome development is the interest of some employers in neurodiversity.

6.3.2 The job market for first level jobs and work placements in Germany

The 2016 unemployment rate for people under the age of 25 in Germany was 6.7 percent; in France, it was more than 23 percent.[44] One factor for this low level in Germany is the success of the collaborative model between tertiary education institutions and employers.

Apprenticeships and structured job placements during studies play a role in the job market in Germany. Employers of all sizes and across industries compete aggressively for entry level candidates.[45] As Trost notes, the German employment market is really tight and it will only get tighter.[46]

There is a variety of tertiary education and employer collaboration models, including work experience, paid internships, bachelors, masters or PhD thesis collaboration, dual-track undergraduate programmes and longer-term apprentice placements.

[44] *http://ec.europa.eu/eurostat/statistics-explained/index.php/Unemployment_statistics#Unemployment_trends*

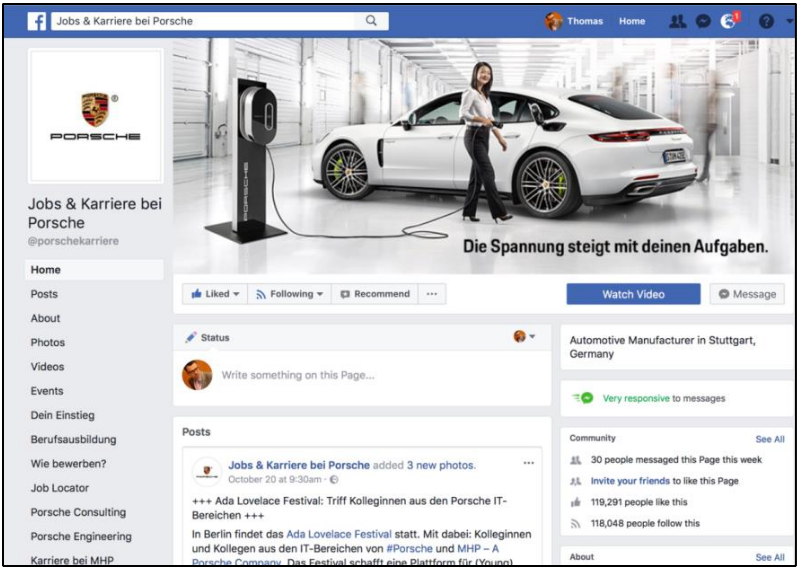
[45] For example, see *https://www.wsj.com/articles/in-germany-demand-for-engineers-outruns-supply-1474930223* in Germany, Demand for Engineers Outruns Supply. Industrial heartland's move to embrace cyberspace is hampered by shortage of engineering graduates.

[46] Armin Trost, *Talent Relationship Management. Personalgewinnung in Zeiten Des Fachkräftemangels* (Springer 2012) 2. „Die meisten Unternehmen in Deutschland werden in Zukunft ein Problem haben, das man gerne als „Luxusproblem " abtun könnte. Sie werden händeringend nach guten, neuen Mitarbeitern suchen. Es wird richtig eng auf dem deutschen Arbeitsmarkt."

6.3.3 Engaging with young job seekers: An example

As part of their employer brand initiatives, many German employers use Facebook and other social media channels as an engagement platform for reaching candidates. The use of these tools is now quite advanced. See example from Porsche below.

Note the mention of the Ada Lovelace Festival, a major event aimed at improving gender diversity in technology; also note the relatively high level of followers.



Automotive Manufacturer in Stuttgart, Germany

Very responsive to messages

30 people messaged this Page this week

Invite your friends to like this Page

119,291 people like this

118,048 people follow this

Jobs & Karriere bei Porsche added 3 new photos.
October 20 at 9:30am ·

+++ Ada Lovelace Festival: Triff Kolleginnen aus den Porsche IT-Bereichen +++

In Berlin findet das Ada Lovelace Festival statt. Mit dabei: Kolleginnen und Kollegen aus den IT-Bereichen von #Porsche und MHP – A Porsche Company. Das Festival schafft eine Plattform für (Young)

Figure 6.1: Image of Porsche Facebook page

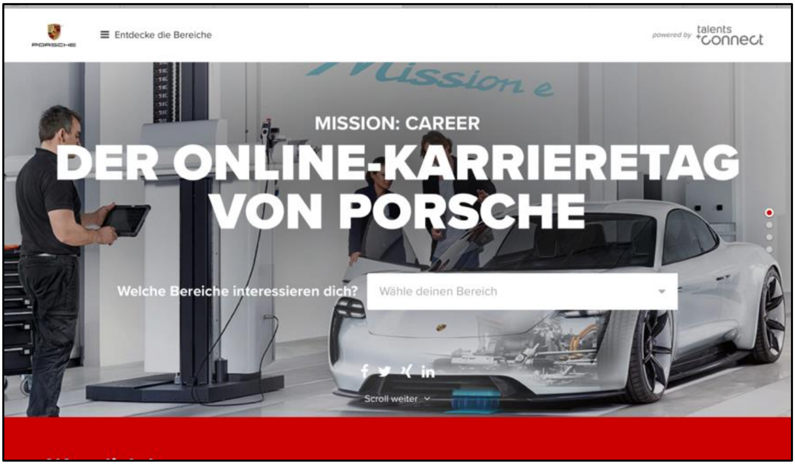

PORSCHE
Entdecke die Bereiche
powered by talents connect
Mission e
MISSION: CAREER
DER ONLINE-KARRIERETAG VON PORSCHE
Welche Bereiche interessieren dich?
Wähle deinen Bereich
Scroll weiter

Figure 6.2: Online Career Day Porsche

Porsche AG has a sophisticated talent acquisition strategy, and other leading German organizations have deployed or are likely to deploy a similar strategy. Porsche uses software solutions from several vendors to manage the recruitment process. Through these channels, students and others are able to learn about the employer, and make informed decisions about where they would like to apply. Porsche and other employers also advertise via social media. Anecdotally, the author noted an increase in targeted job advertisements for student placements in the automobile industry in his personal social media as a result of this research.

To summarize:

- The battle for entry level hires in Germany today is fierce.
- Diversity has become a major executive messaging theme in the larger German multinationals.
- Organizations are deploying ever more sophisticated technologies and business practices for talent acquisition and employer branding.

- The online channel is the dominant channel for employment opportunity discovery and application.
- People with disabilities are often willing and able to work.
- German public sector employers have clear legal obligations to provide accessible recruitment websites.
- German private sector employees do not have clear legal obligations to provide accessible recruitment websites.

With this in mind, it would be appropriate to analyze the state of career site accessibility across several German organizations.

6.4 A new accessibility study of German corporate career sites

While there have been various studies of website accessibility (see earlier) and some on career sites, there has been no recent study of German corporate career sites. A study by Lazar et al in 2012 in the US investigated the accessibility and usability of job application websites for the blind.[47] This study did not just test for standards compliance, but it tested real world usability by having blind users conduct hands-on applications. The results showed that less than 1/3 of the application attempts could be done without assistance. In the UK, a major study of 300 recruiter (i.e. recruitment agency) websites found that the vast majority of recruiter websites were inaccessible. [48] Amongst other things, Tynan's study tested for the presence of an accessibility / diversity statement, and found that over 50% of sites did not even have one. Only one of the 300 websites provided a specific website accessibility statement.

[47] Lazar, Olalere and Wentz.

[48] Anne Tynan, 'Recruitment Equality: Accessibility, Equality and Diversity on Recruitment Websites' (2011).

There was a detailed study of German career portals in 2007.[49] This report tested both accessibility standards and practical screen reader usage. This did not test individual company boards, but it did test major job portals. It showed that all the career portals had significant accessibility and usability issues.

The techniques used in these studies have informed the design of this study. This study examines the accessibility of the career sites of 7 large German multinationals and 3 public sector organizations, using both automated testing tools, and blind and visually impaired users using the website.

6.4.1 Approach to testing, test subjects and test design

Automated testing, while it is useful in picking up many accessibility errors, has many limitations. The most effective way to test for accessibility is to have testers who have the disability you wish to test. Automated testing, screen recordings, a user survey, video interviews and direct observation were deployed to assess the websites as completely as possible, and to explore the gap between automated testing assessment and actual user feedback.

Accessibility research and assistance at KIT

The SZS[50] at the Karlsruhe Institute of Technology provides assistance to visually impaired and blind students in their studies, and researches assistive technologies.

[49] Anna Courtpozanis and Benjamin Grießmann, ‘Test von 30 Online-Jobbörsen Auf Barrierefreiheit’ (2007).

[50] See *http://www.szs.kit.edu/english/287_1037.php* Study centre for the visually impaired.

6.4.2 Lab assessment and observation

4 students volunteered for the testing. The testing was run over the course of 4 days in November / December 2017, with two students per session.

Table 6.2: Background of users for lab test

Name	Disability level	Assistive technology	Academic field	Academic degree level
Max	<5% view left	NVDA (screen reader)	Chemistry	Masters
Philipp	15% view left	Magnifer (zoomtext)	Computer Science (FH)	Bachelors
Florian	Blind	NVDA/Braille	Computer Science (FH)	Bachelors
Joshua	Blind	NVDA/Braille	Computer Science	Bachelors

All screen activity and computer voice were recorded, and the author attended all the sessions, took notes, asked questions and made video of the testers in action, and interviewed them at the end of the assessment. The choice of organizations was based on those that the testers were curious to test, taken from a longer list of large German companies. For the public sector, a mix of large and smaller organizations was chosen. The following organizations were tested.

The testers were asked to find a role that they would potentially be interested in applying for, for instance, student placement in the IT department, thesis assignment or an entry level job.

The testers were provided with Google mail users and a fictional surname for the exercise. This was firstly not to compromise their own email accounts with several communications from the would-be employers. After all, they may wish to work for these organizations one day.

Table 6.3: Organizations for lab assessment

No.	Company name	Industry	Testers
1	BASF	Chemical	Max and Joshua
2	Deutsche Bundesbank	Public Sector (mid)	Max and Joshua
3	Deutsche Bahn AG	Public Sector (large)	Florian and Philipp
4	Commerzbank AG	Banking	Florian and Philipp
5	Bosch (Robert Bosch GmbH)	Manufacturing	Florian and Philipp
6	Porsche AG	Automotive	Max and Joshua and Florian
7	Daimler AG	Automotive	Max and Joshua and Florian
8	Deutsche Auswärtiges Amt	Public Sector (mid)	Max
9	Volksbank	Banking	Joshua
10	Zalando SE	On-line retailer	Joshua and Philipp and Florian

Secondly, it enabled the author to monitor the communications from the recruiter via the google mail account and to revisit the applications, if need be. Thirdly, it also made it easy for employers to purge the records, as they were clearly labelled as being for test purposes. In order to minimize disruption to the employers that were tested, at least one free text field was used to note that this was for accessibility test purposes. Instead of a resume, the test subjects uploaded a letter describing the research project and providing contact details of the author. Several organizations replied, wanting to know more about the research. There is a plan to follow up with the organizations and suggest accessibility improvements once this research has been concluded.

SurveyMonkey was used to collect written responses immediately after each session. The survey was split into the following sections. All questions had a 5-point scale, and free format text for comments.

- How easy was it to find general career information about the organization?
- How easy was it to search for a specific job or job posting?
- How easy was it to register as a candidate or applicant on the career site?
- How easy was it to apply for a specific role?
- Did you find an accessibility statement on the site?
- Was there an alternative channel of communication available? (for instance, chat or phone).
- Please comment on your overall experience with the site and application process? What worked well or frustrated you?

The testers were able to compete the survey in SurveyMonkey[51] without assistance, usually within 10 minutes. One tester used his mobile phone to complete the survey as he found this the easiest accessibility method.

6.5 Author observations and tester feedback

6.5.1 Key finding summarized

None of the sites was completely accessible without some assistance.

In some cases, the assistance was minimal; in others, it involved actually taking control of the computer. Most of the private sector sites had many basic accessibility errors. Public sector sites were somewhat more compliant in terms of accessibility navigation and controls, but were sometimes overly complex from a generic usability perspective. While the goal was not to rank the sites, Zalando was by far the most usable and accessible site.

[51] All the testers found SurveyMonkey's accessibility to be good.

This next section will highlight some of the issues and also some examples of good practice. The descriptions below are based on the real time perceptions, frustrations and successes of the users, and a detailed analysis of the screen recordings.

The high level WCAG 2.0 principles influenced the analysis (Perceivable, Operable, Understandable and Robust).

As the exercise went on, the testers became familiar with the structure of the recruitment process. This made it easier for them to understand the process flow, HR jargon and overcome navigational issues so the organizations later in the test received better scores. In hindsight, we could have had them test in a different order, but the purpose of the assessment is not to rank the sites, merely to assess them for accessibility and usability issues.

6.5.2 Finding the career and job site

Rather than going to the corporate home page and then searching through the menu for the career or jobs section, all the testers went to Google and searched on company name / jobs. In almost all cases, this brought up the correct site as the first link on the Google search, although in one case the user clicked onto an external job board which had bought the advert listing at the top of the search result. The test users commented that they found Google search easier to navigate than trying to guess menu names and navigation paths on the corporate website. No one used the website's own search bar to find the career page starting point.

6.5.3 Confusion between job and career sites

At first, the testers were unsure about the difference between what the career portal did and what the job board did. This led to confusion with log-ons and frustration with navigation. Some websites had separate user id for the career portal and the job board. Navigation, screen behaviour and usability differed between the career portal and the job board in many cases, causing further confusion. Large organizations with different divisions and geographic organizations also added to the complexity. For instance, the Bosch site was confusing in that the main Bosch business was using two different applications depending on geography, and the Bosch software department was using what seemed to be yet another different application or application version.

6.5.4 Search navigation

All sites had some navigational issues, but searching /narrowing down the selection was often very problematic.

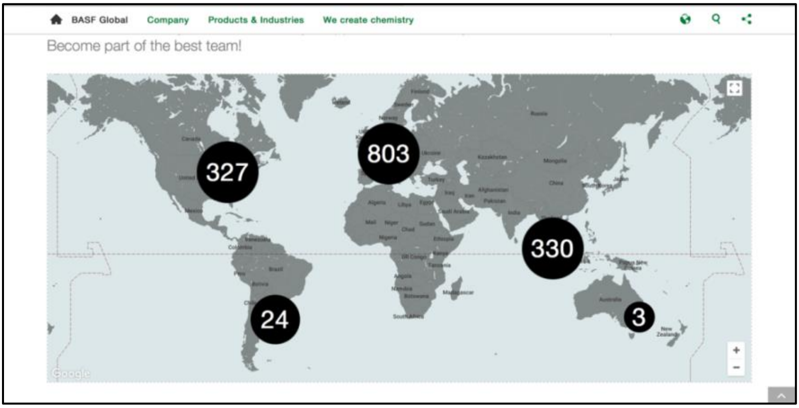
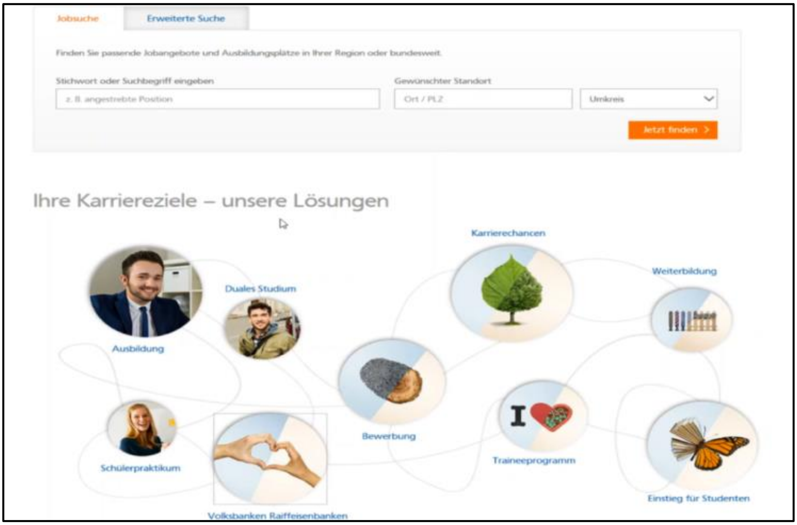


Figure 6.3: BASF: Map inaccessible for screen reader

Several sites used maps for search navigation. These were generally inaccessible. In the case of Volksbank, the high-level selection of the type of role was overly ornate, and without alt text. To navigate this, the tester required sighted user assistance.



Finden Sie passende Jobangebote und Ausbildungsplätze in Ihrer Region oder bundesweit.

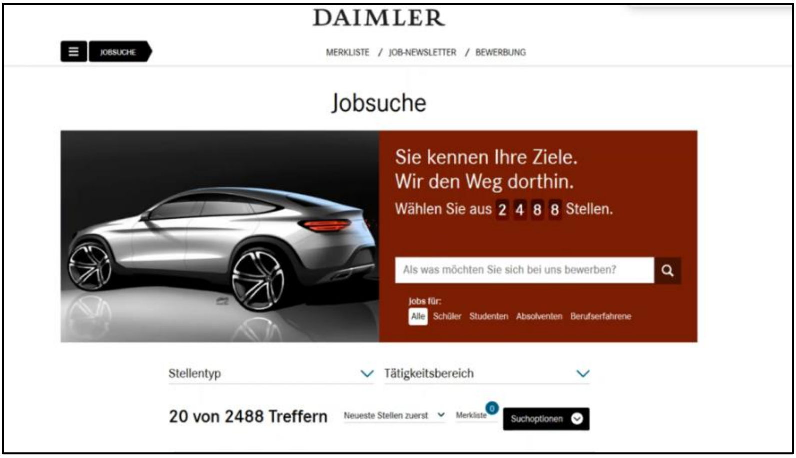
Stichwort oder Suchbegriff eingeben: z. B. angestrebte Position

Gewünschter Standort: Ort / PLZ

Umkreis

Ihre Karriereziele – unsere Lösungen

Figure 6.4: Volksbank: Pretty but awkward navigational metaphor



Jobsuche

Sie kennen Ihre Ziele.
Wir den Weg dorthin.
Wählen Sie aus 2 4 8 8 Stellen.

Als was möchten Sie sich bei uns bewerben?

Jobs für:
Alle Schüler Studenten Absolventen Berufserfahrene

20 von 2488 Treffern

Figure 6.5: Daimler: Search screen reader issue

While the Daimler search was essentially simple and the testers liked how the jobs were listed below the search, the counter in the display field caused major issues with the screenreaders, requiring sighted user support to complete.

The search at Zalando was a mix of simple free text and simple dropdown lists (location), with the option to list all jobs. While Zalando has fewer jobs, there is no reason why this sort of more natural search would not work at the scale of the other organizations.

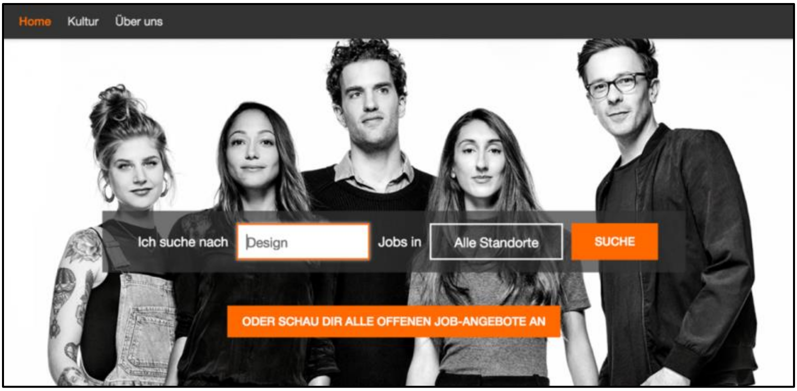


Figure 6.6: Zalando: Powerful search with obvious list option

6.5.5 PDFs for help, policy, directions, etc.

When the test users realized that they needed to open a PDF, they all mentioned that PDFs are often a major accessibility challenge. This mirrors other research on PDF experience.[52]

[52] Gian Wild and Daniel Craddock, ‘Are PDFs an Accessible Solution?’ 355.

The document below from BASF, describing the application process and flow, was completely inaccessible to the screen reader. It would read every letter out. All other PDFs they encountered were also difficult to read, as they were not formatted to be accessible. Typically, this meant that the whole document needed to be clicked through word by word, or even letter by letter. Most images in the PDFs lacked alt text. For long documents such as privacy statements requiring acknowledgement, this was particularly problematic and, without sighted assistance, PDFs were a showstopper on several sites.

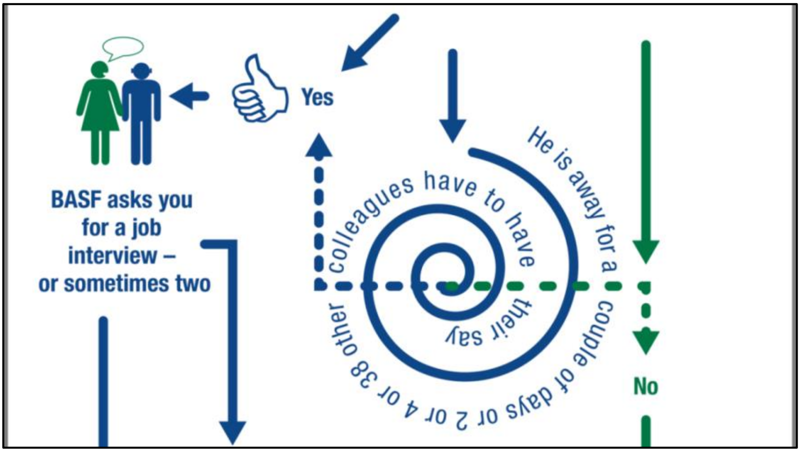
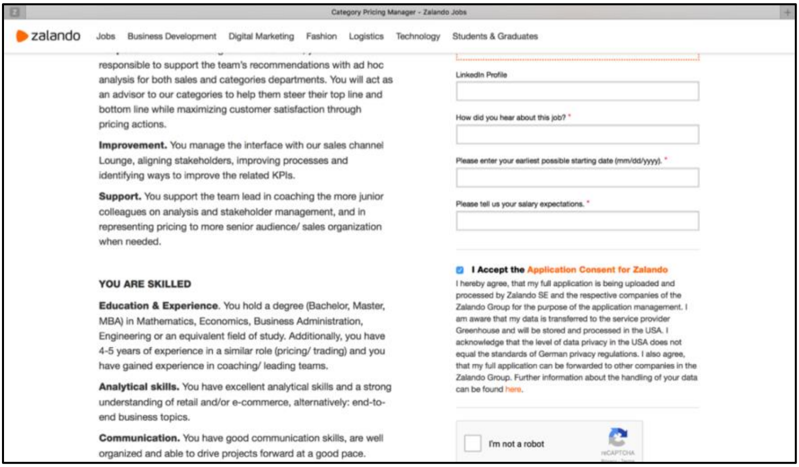

Yes
BASF asks you for a job interview – or sometimes two
colleagues have to have their say
He is away for a couple of days or 2 or 4 or 38 other
No

Figure 6.7: BASF: Impossible PDF for screen reader

For instance, while the Bosch career site and software group job application process were generally viewed positively by the testers, the data protection statement was only available as a difficult to access PDF (read button not labelled correctly, and the PDF without navigation). This required sited user assistance to complete.

The Zalando site had the simplest notification, as the policy is relatively straight forward and embedded in the form, not in a pop up. (The policy is questionable in terms of data protection regulation, but that is not the concern of this chapter).



responsible to support the team's recommendations with ad hoc analysis for both sales and categories departments. You will act as an advisor to our categories to help them steer their top line and bottom line while maximizing customer satisfaction through pricing actions.

Improvement. You manage the interface with our sales channel Lounge, aligning stakeholders, improving processes and identifying ways to improve the related KPIs.

Support. You support the team lead in coaching the more junior colleagues on analysis and stakeholder management, and in representing pricing to more senior audience/ sales organization when needed.

YOU ARE SKILLED

Education & Experience. You hold a degree (Bachelor, Master, MBA) in Mathematics, Economics, Business Administration, Engineering or an equivalent field of study. Additionally, you have 4-5 years of experience in a similar role (pricing/ trading) and you have gained experience in coaching/ leading teams.

Analytical skills. You have excellent analytical skills and a strong understanding of retail and/or e-commerce, alternatively: end-to-end business topics.

Communication. You have good communication skills, are well organized and able to drive projects forward at a good pace.

LinkedIn Profile

How did you hear about this job? *

Please enter your earliest possible starting date (mm/dd/yyyy). *

Please tell us your salary expectations. *

☑ **I Accept the Application Consent for Zalando**

I hereby agree, that my full application is being uploaded and processed by Zalando SE and the respective companies of the Zalando Group for the purpose of the application management. I am aware that my data is transferred to the service provider Greenhouse and will be stored and processed in the USA. I acknowledge that the level of data privacy in the USA does not equal the standards of German privacy regulations. I also agree, that my full application can be forwarded to other companies in the Zalando Group. Further information about the handling of your data can be found here.

□ I'm not a robot

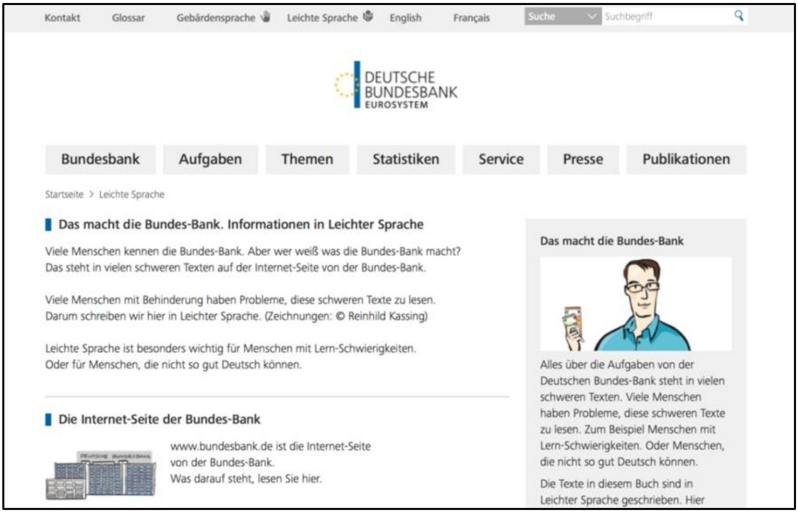
Figure 6.8: Zalando: Privacy statement

6.5.6 Verbosity of text and images

Most of the career sites had a lot of marketing text and images, which a sighted person would skim over. Screen reader users do not have the opportunity to skim text and, when the text is both verbose and awkward to navigate past, frustration levels rise. Users who have to listen to the sound of the screen-reader appreciate concise marketing. Zalando was praised for its brevity; Daimler was seen as long winded.

Poor text readability becomes a bigger usability issue for users with disabilities.

The Bundesbank site has a feature for cognitive disability which we did not see elsewhere in this lab test. By clicking on the "*Leichte Sprache*" button, the website changed to a much simpler reading level. It also has features for sign language. These capabilities have only been deployed to the main part of the corporate site, but it is a welcome development.



Das macht die Bundes-Bank. Informationen in Leichter Sprache

Viele Menschen kennen die Bundes-Bank. Aber wer weiß was die Bundes-Bank macht?
Das steht in vielen schweren Texten auf der Internet-Seite von der Bundes-Bank.

Viele Menschen mit Behinderung haben Probleme, diese schweren Texte zu lesen.
Darum schreiben wir hier in Leichter Sprache. (Zeichnungen: © Reinhild Kassing)

Leichte Sprache ist besonders wichtig für Menschen mit Lern-Schwierigkeiten.
Oder für Menschen, die nicht so gut Deutsch können.

Die Internet-Seite der Bundes-Bank

www.bundesbank.de ist die Internet-Seite
von der Bundes-Bank.
Was darauf steht, lesen Sie hier.

Das macht die Bundes-Bank

Alles über die Aufgaben von der Deutschen Bundes-Bank steht in vielen schweren Texten. Viele Menschen haben Probleme, diese schweren Texte zu lesen. Zum Beispiel Menschen mit Lern-Schwierigkeiten. Oder Menschen, die nicht so gut Deutsch können.

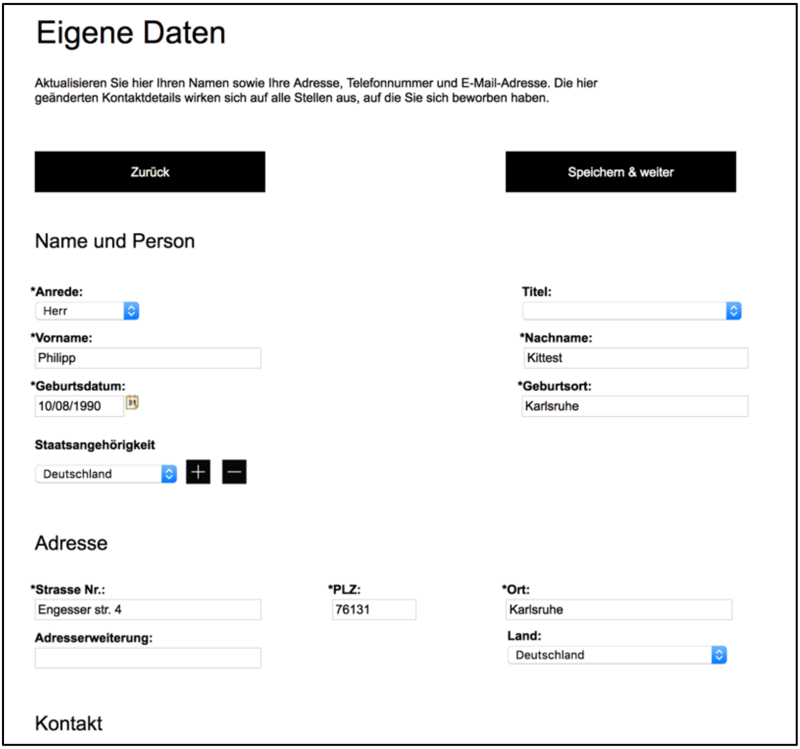
Die Texte in diesem Buch sind in Leichter Sprache geschrieben. Hier

Figure 6.9: Bundesbank: Simplified language version

6.5.7 Differing responses by user

The lab test illustrated every user is different; there is no standard blind user. The challenges, successes and frustrations were not precisely the same for the 4 users. Perceived factors influencing this included the nature and level of disability itself, knowledge of the recruitment process and corporate websites more generally, choice of assistive technology and even browser. One user was particularly adept at working around navigation issues that other users were not able to solve quite so easily.

For example, the Daimler website navigation was seen as challenging and difficult by the blind users, but one user with visual impairment found the black and white contrast buttons easier to use with the screen magnifier.



Eigene Daten

Aktualisieren Sie hier Ihren Namen sowie Ihre Adresse, Telefonnummer und E-Mail-Adresse. Die hier geänderten Kontaktdetails wirken sich auf alle Stellen aus, auf die Sie sich beworben haben.

Name und Person

*Anrede: Herr	Titel:
*Vorname: Philipp	*Nachname: Kittest
*Geburtsdatum: 10/08/1990	*Geburtsort: Karlsruhe

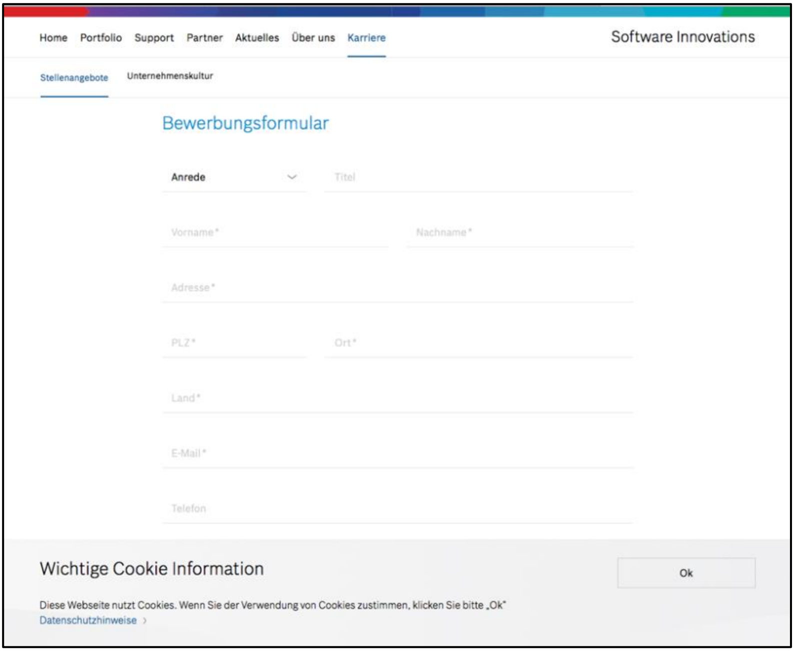
Staatsangehörigkeit: Deutschland

Adresse

*Strasse Nr.: Engesser str. 4	*PLZ: 76131	*Ort: Karlsruhe
Adresserweiterung:		Land: Deutschland

Kontakt

Figure 6.10: Daimler: Good contrast example for visually impaired users, but blind users found the navigation awkward.



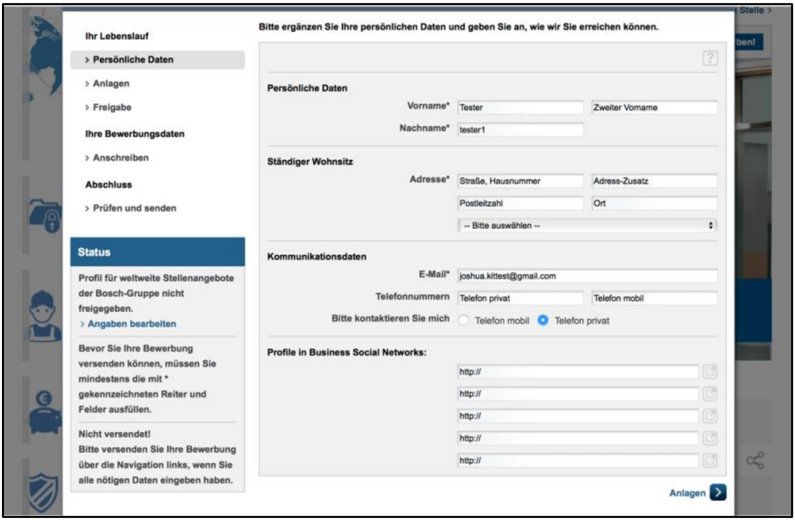
Bewerbungsformular

Wichtige Cookie Information

Diese Webseite nutzt Cookies. Wenn Sie der Verwendung von Cookies zustimmen, klicken Sie bitte „Ok"

Figure 6.11: Bosch: Screen contrast poor but good field navigation

Blind users found this Bosch screen easy to complete, as field names were directly noted in the field itself, making for simple and rapid navigation via the screen-reader and tab key. However, for partially sighted users, the light colouring made the screen illegible, even with strong screen magnification. A different part of the Bosch site used a different, likely older application screen.



Ihr Lebenslauf

- Persönliche Daten
- Anlagen
- Freigabe

Ihre Bewerbungsdaten

- Anschreiben

Abschluss

- Prüfen und senden

Status

Profil für weltweite Stellenangebote der Bosch-Gruppe nicht freigegeben.
> Angaben bearbeiten

Bevor Sie Ihre Bewerbung versenden können, müssen Sie mindestens die mit * gekennzeichneten Reiter und Felder ausfüllen.

Nicht versendet!
Bitte versenden Sie Ihre Bewerbung über die Navigation links, wenn Sie alle nötigen Daten eingeben haben.

Bitte ergänzen Sie Ihre persönlichen Daten und geben Sie an, wie wir Sie erreichen können.

Persönliche Daten

Vorname*	Tester	Zweiter Vorname
Nachname*	tester1	

Ständiger Wohnsitz

Adresse*	Straße, Hausnummer	Adress-Zusatz
	Postleitzahl	Ort
	-- Bitte auswählen --	

Kommunikationsdaten

E-Mail*	joshua.kittest@gmail.com	
Telefonnummern	Telefon privat	Telefon mobil
Bitte kontaktieren Sie mich	○ Telefon mobil	● Telefon privat

Profile in Business Social Networks:

http://
http://
http://
http://
http://

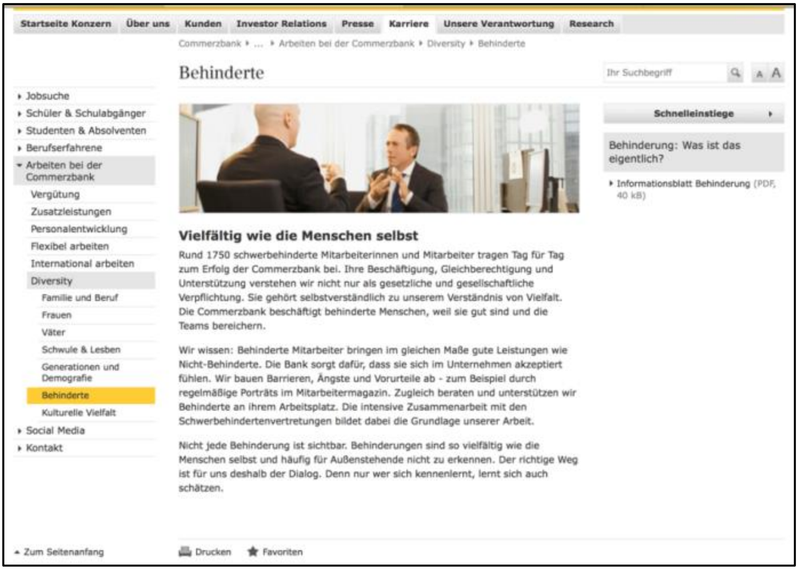
Anlagen

Figure 6.12: Bosch: Main data entry screen design. Good accessibility for blind and visually impaired

The Zalando site was easy for all the users, but not in all browsers. One user initially used Explorer because of the screen-reader tool, rather than Firefox, and critical search fields were not visible in Explorer, rendering the site inaccessible. The site worked well in Firefox, Safari and Chrome.

6.5.8 Diversity statements, certifications, information and data

We were not able to find any career site that advertised compliance with WCAG, either on the website imprint page or on the career site itself. Some career sites discussed accessibility in the context of their diversity behaviours and highlighted their diversity credentials.



Behinderte

Vielfältig wie die Menschen selbst

Rund 1750 schwerbehinderte Mitarbeiterinnen und Mitarbeiter tragen Tag für Tag zum Erfolg der Commerzbank bei. Ihre Beschäftigung, Gleichberechtigung und Unterstützung verstehen wir nicht nur als gesetzliche und gesellschaftliche Verpflichtung. Sie gehört selbstverständlich zu unserem Verständnis von Vielfalt. Die Commerzbank beschäftigt behinderte Menschen, weil sie gut sind und die Teams bereichern.

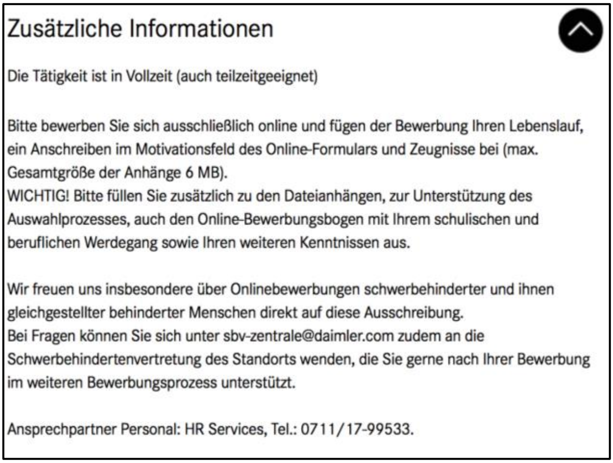
Wir wissen: Behinderte Mitarbeiter bringen im gleichen Maße gute Leistungen wie Nicht-Behinderte. Die Bank sorgt dafür, dass sie sich im Unternehmen akzeptiert fühlen. Wir bauen Barrieren, Ängste und Vorurteile ab - zum Beispiel durch regelmäßige Porträts im Mitarbeitermagazin. Zugleich beraten und unterstützen wir Behinderte an ihrem Arbeitsplatz. Die intensive Zusammenarbeit mit den Schwerbehindertenvertretungen bildet dabei die Grundlage unserer Arbeit.

Nicht jede Behinderung ist sichtbar. Behinderungen sind so vielfältig wie die Menschen selbst und häufig für Außenstehende nicht zu erkennen. Der richtige Weg ist für uns deshalb der Dialog. Denn nur wer sich kennenlernt, lernt sich auch schätzen.

Figure 6.13: Commerzbank: High level diversity statement

See above for the diversity statement from Commerzbank, with clear mention of persons with disability, but no mention of website accessibility. While most corporate sites have an extensive section on diversity, people with disabilities generally receive little or no mention. Porsche, for instance, has an extensive section on gender inclusion, but only one short sentence on disability.

Daimler, by comparison to other sites, was strong in terms of accessibility communication and positioning, providing direct support in the job posting description.



Zusätzliche Informationen

Die Tätigkeit ist in Vollzeit (auch teilzeitgeeignet)

Bitte bewerben Sie sich ausschließlich online und fügen der Bewerbung Ihren Lebenslauf, ein Anschreiben im Motivationsfeld des Online-Formulars und Zeugnisse bei (max. Gesamtgröße der Anhänge 6 MB).
WICHTIG! Bitte füllen Sie zusätzlich zu den Dateianhängen, zur Unterstützung des Auswahlprozesses, auch den Online-Bewerbungsbogen mit Ihrem schulischen und beruflichen Werdegang sowie Ihren weiteren Kenntnissen aus.

Wir freuen uns insbesondere über Onlinebewerbungen schwerbehinderter und ihnen gleichgestellter behinderter Menschen direkt auf diese Ausschreibung.
Bei Fragen können Sie sich unter sbv-zentrale@daimler.com zudem an die Schwerbehindertenvertretung des Standorts wenden, die Sie gerne nach Ihrer Bewerbung im weiteren Bewerbungsprozess unterstützt.

Ansprechpartner Personal: HR Services, Tel.: 0711/17-99533.

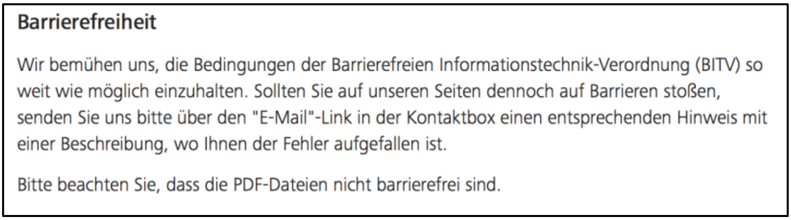
Figure 6.14: Daimler: Accessibility contact information

In its diversity report,[53] Daimler notes:

> *The employment of severely disabled people at Daimler has already been solidly based on an integration agreement since 2002. In Germany we exceed the legally prescribed employment quota of five percent of the work- force every year. Our action plan for trainees with severe disabilities opens up a wide range of commercial and technical professions for young people. We also encourage people with learning challenges to take training, and work together with schools in this sector. More than 30 workshops for handicapped people are our partners. Socially and economically – by no means a contradiction.*

[53] *https://www.daimler.com/documents/company/other/daimler-diversitybroschuere-en-2016.pdf*

Public sector organizations were significantly better at providing information about accessibility obligations and also in terms of capturing disability information about the applicant. The Bundesbank makes clear mention of the BITV, but interestingly not yet BITV 2.0.

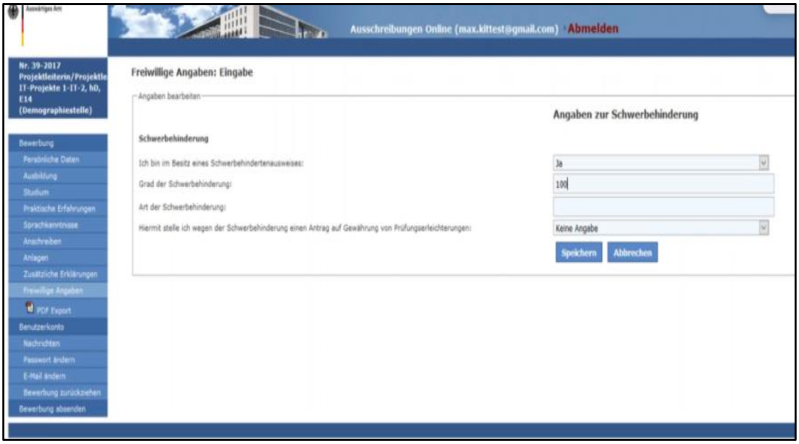


Barrierefreiheit

Wir bemühen uns, die Bedingungen der Barrierefreien Informationstechnik-Verordnung (BITV) so weit wie möglich einzuhalten. Sollten Sie auf unseren Seiten dennoch auf Barrieren stoßen, senden Sie uns bitte über den "E-Mail"-Link in der Kontaktbox einen entsprechenden Hinweis mit einer Beschreibung, wo Ihnen der Fehler aufgefallen ist.

Bitte beachten Sie, dass die PDF-Dateien nicht barrierefrei sind.

Figure 6.15: Deutsche Bundesbank: Accessibility statement



Freiwillige Angaben: Eingabe

Angaben bearbeiten

Angaben zur Schwerbehinderung

Schwerbehinderung

Ich bin im Besitz eines Schwerbehindertenausweises: Ja

Grad der Schwerbehinderung: 100

Art der Schwerbehinderung:

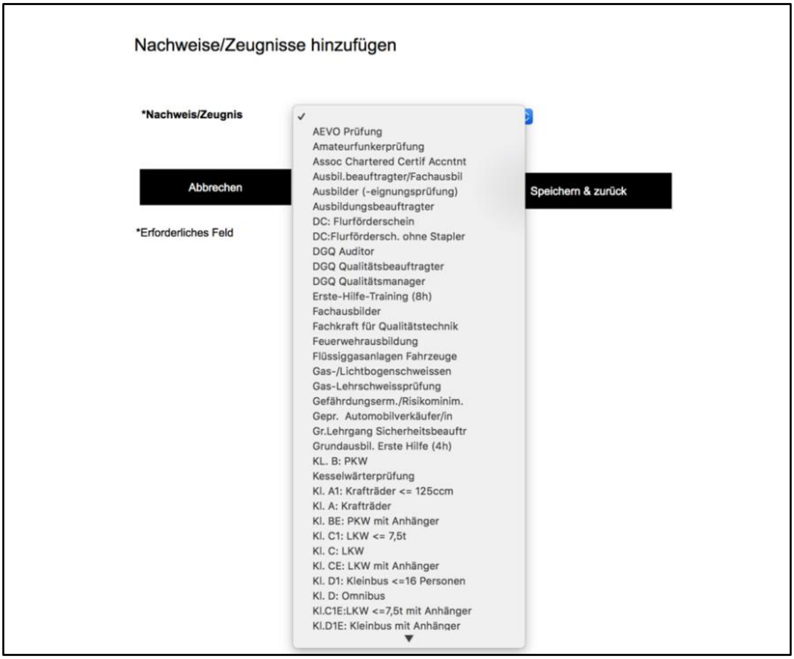
Hiermit stelle ich wegen der Schwerbehinderung einen Antrag auf Gewährung von Prüfungserleichterungen: Keine Angabe

Figure 6.16: Deutsche Auswärtiges Amt: Disability data entry

The Auswärtiges Amt provided a form to capture details of the disability. The testers were very pleased to see this.

6.5.9 Structured data and excessive data collection

Zalando's form was very simple, with just 8 fields, and an easy-to-use ARIA[54] compliant attachment loader. Deutsche Bahn, BASF, Commerzbank, Volksbank and Daimler were significantly more complex. While there may be justification for some of the fields, others are clearly excessive. Bosch and Porsche were somewhat less complex.



Nachweise/Zeugnisse hinzufügen

*Nachweis/Zeugnis

✓
AEVO Prüfung
Amateurfunkerprüfung
Assoc Chartered Certif Accntnt
Ausbil.beauftragter/Fachausbil
Ausbilder (-eignungsprüfung)
Ausbildungsbeauftragter
DC: Flurförderschein
DC:Flurfördersch. ohne Stapler
DGQ Auditor
DGQ Qualitätsbeauftragter
DGQ Qualitätsmanager
Erste-Hilfe-Training (8h)
Fachausbilder
Fachkraft für Qualitätstechnik
Feuerwehrausbildung
Flüssiggasanlagen Fahrzeuge
Gas-/Lichtbogenschweissen
Gas-Lehrschweissprüfung
Gefährdungserm./Risikominim.
Gepr. Automobilverkäufer/in
Gr.Lehrgang Sicherheitsbeauftr
Grundausbil. Erste Hilfe (4h)
KL. B: PKW
Kesselwärterprüfung
Kl. A1: Krafträder <= 125ccm
Kl. A: Krafträder
Kl. BE: PKW mit Anhänger
Kl. C1: LKW <= 7,5t
Kl. C: LKW
Kl. CE: LKW mit Anhänger
Kl. D1: Kleinbus <=16 Personen
Kl. D: Omnibus
Kl.C1E:LKW <=7,5t mit Anhänger
Kl.D1E: Kleinbus mit Anhänger

*Erforderliches Feld

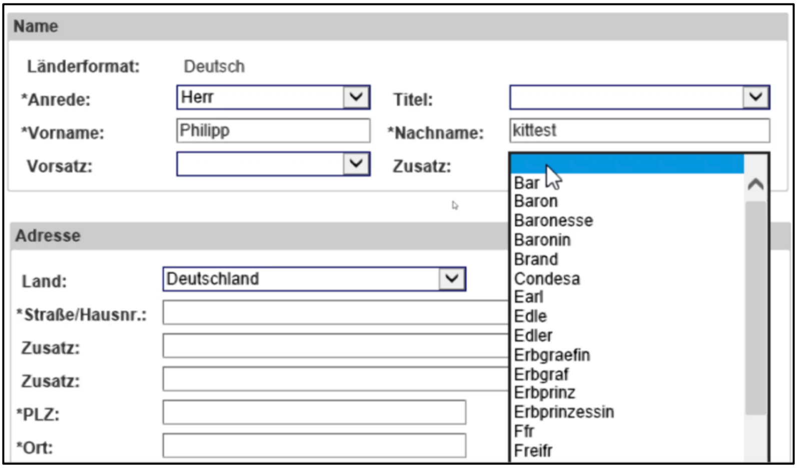
Figure 6.17: Daimler: Lengthy drop-down list

Several sites have very lengthy drop-down lists. This one caused a problem for the students, as the screen was labelled *Zeugnis* (reference) so

[54] ARIA is the W3C guideline for Rich Internet Applications.

they were expecting to upload their CV and degree type information. Instead, it was asking for industry-specific certificate information. Without sighted assistance, the test subjects were not able to progress beyond this point.

On the Deutsche Bahn site, the forms were overly complex, with excessive use of drop-down entries and somewhat cryptic codes. The relevance of the nobility table is highly questionable.



Name

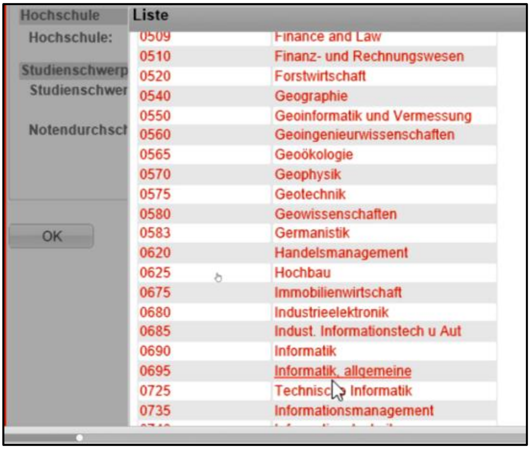
Länderformat:	Deutsch		
*Anrede:	Herr	Titel:	
*Vorname:	Philipp	*Nachname:	kittest
Vorsatz:		Zusatz:	

Adresse

Land:	Deutschland
*Straße/Hausnr.:	
Zusatz:	
Zusatz:	
*PLZ:	
*Ort:	

Figure 6.18: Deutsche Bahn: Nobility titles on the recruitment form

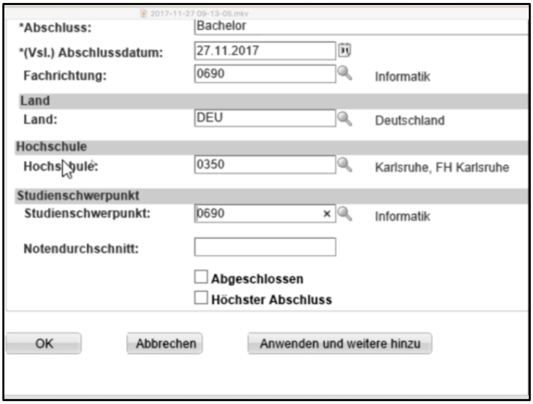
This was even more problematic with job and education information, where the pull-down lists were very long, and lacking intuitive search. While highly structured data makes for easy categorization by the recruiter, the effort for a disabled user was such that it required the help of a sighted user to complete the fields. There were at least 10 such fields, some of which had several hundred potential data items. Even the list of tertiary institutions was a pull down, meaning scrolling through hundreds of entries.



Liste

0509	Finance and Law
0510	Finanz- und Rechnungswesen
0520	Forstwirtschaft
0540	Geographie
0550	Geoinformatik und Vermessung
0560	Geoingenieurwissenschaften
0565	Geoökologie
0570	Geophysik
0575	Geotechnik
0580	Geowissenschaften
0583	Germanistik
0620	Handelsmanagement
0625	Hochbau
0675	Immobilienwirtschaft
0680	Industrieelektronik
0685	Indust. Informationstech u Aut
0690	Informatik
0695	Informatik, allgemeine
0725	Technische Informatik
0735	Informationsmanagement

Figure 6.19: Deutsche Bahn: List of study subjects



2017-11-27 09-13-05.mkv

*Abschluss: Bachelor

*(Vsl.) Abschlussdatum: 27.11.2017

Fachrichtung: 0690 Informatik

Land

Land: DEU Deutschland

Hochschule

Hochschule: 0350 Karlsruhe, FH Karlsruhe

Studienschwerpunkt

Studienschwerpunkt: 0690 Informatik

Notendurchschnitt:

□ Abgeschlossen

□ Höchster Abschluss

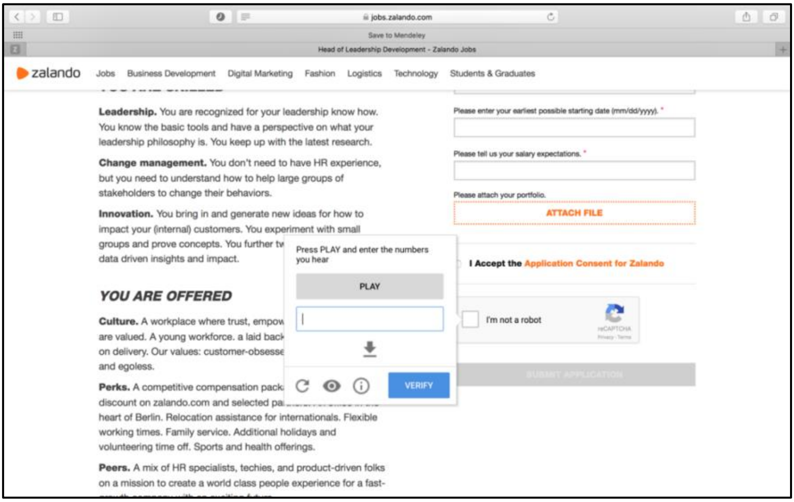
Figure 6.20: Excessive structured data capture

6.5.10 Embedded video

Embedding video, often using YouTube, is widely used, especially in the career portal stage. While these videos are an excellent way to inform and excite sighted applicants and candidates, clearly they are of very little use to visually impaired or blind users. When video replaces other forms of communication, it is actually a hindrance. All sites were haphazard in labelling videos with meaningful labels. In some cases, the video played sound and music on opening the site, and in the background. This was very confusing and in one case discomforting for the tester. Additionally, most videos did not have captions, which is not helpful for deaf or hearing-impaired users.

6.5.11 Captchas, even when standards compliant, are a barrier

While the Zalando process was by far the simplest, the Captcha made it very difficult for those not using a mouse to conclude the process without sighted assistance. The audio captcha is very difficult to follow and provides limited feedback. It also scrambled languages.



Leadership. You are recognized for your leadership know how. You know the basic tools and have a perspective on what your leadership philosophy is. You keep up with the latest research.

Change management. You don't need to have HR experience, but you need to understand how to help large groups of stakeholders to change their behaviors.

Innovation. You bring in and generate new ideas for how to impact your (internal) customers. You experiment with small groups and prove concepts. You further tw
data driven insights and impact.

YOU ARE OFFERED

Culture. A workplace where trust, empow
are valued. A young workforce. a laid back
on delivery. Our values: customer-obsesse
and egoless.

Perks. A competitive compensation pack
discount on zalando.com and selected pa
heart of Berlin. Relocation assistance for internationals. Flexible working times. Family service. Additional holidays and volunteering time off. Sports and health offerings.

Peers. A mix of HR specialists, techies, and product-driven folks on a mission to create a world class people experience for a fast-

Please enter your earliest possible starting date (mm/dd/yyyy). *

Please tell us your salary expectations. *

Please attach your portfolio.

ATTACH FILE

I Accept the Application Consent for Zalando

Press PLAY and enter the numbers you hear

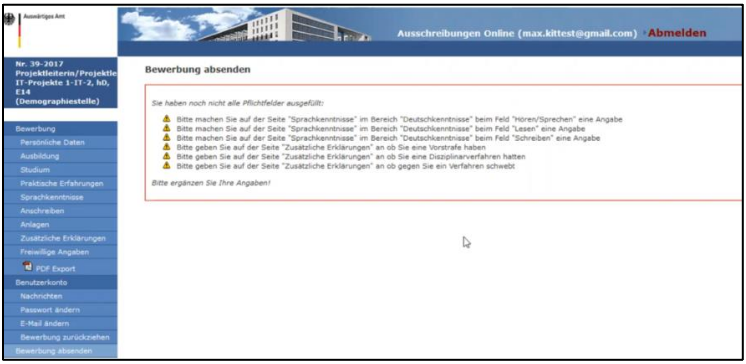
Figure 6.21: Zalando: Captcha

6.5.12 Form and process navigation

On several sites, tab order is not well thought through and, when combined with poorly labelled data fields, it makes data entry very laborious, error prone and frustrating. Some of the screens are very long with poor framing. On the Daimler site for instance, the tab order included the long list of Daimler companies and images. In the course of the application, one user went through that list at least 10 times. In the case of Commerzbank and Volksbank, the users sometimes strayed into banking functionality; in the case of Porsche, car emissions data. Navigation in search results tables also varied from company to company.

6.5.13 Error message handling, pop ups, radio buttons and date entry

Several sites use pop ups to display new data entry screens. This is awkward navigationally, as the screen reader does not always know about the pop up. Pop up error messages are especially problematic if they are not accessible, as the user is then unaware of the error and how to address it. Several sites did not properly document radio buttons so it was hard to figure out what one had clicked yes or no for.



Bewerbung absenden

Sie haben noch nicht alle Pflichtfelder ausgefüllt:

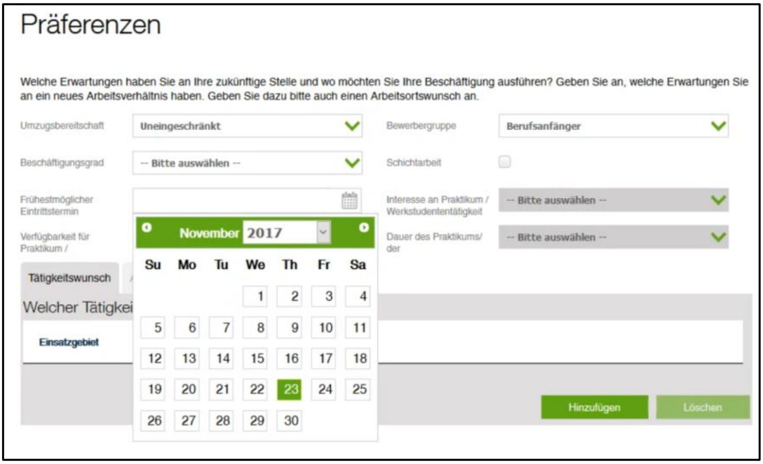
- ⚠ Bitte machen Sie auf der Seite "Sprachkenntnisse" im Bereich "Deutschkenntnisse" beim Feld "Hören/Sprechen" eine Angabe
- ⚠ Bitte machen Sie auf der Seite "Sprachkenntnisse" im Bereich "Deutschkenntnisse" beim Feld "Lesen" eine Angabe
- ⚠ Bitte machen Sie auf der Seite "Sprachkenntnisse" im Bereich "Deutschkenntnisse" beim Feld "Schreiben" eine Angabe
- ⚠ Bitte geben Sie auf der Seite "Zusätzliche Erklärungen" an ob Sie eine Vorstrafe haben
- ⚠ Bitte geben Sie auf der Seite "Zusätzliche Erklärungen" an ob Sie eine Disziplinarverfahren hatten
- ⚠ Bitte geben Sie auf der Seite "Zusätzliche Erklärungen" an ob gegen Sie ein Verfahren schwebt

Bitte ergänzen Sie Ihre Angaben!

Figure 6.4: DAA: Good error message display

Although the Auswärtiges Amt asks for many structured data items, it displays the error messages clearly. This was well received by the testers.

Date handling is often problematic, with rich control calendars often requiring sighted intervention. Date fields require careful attention. In the case below, it was impossible for any of the testers to move beyond the calendar pop up without sighted assistance. At least 3 other sites had similar issues with date handling.



Präferenzen

Welche Erwartungen haben Sie an Ihre zukünftige Stelle und wo möchten Sie Ihre Beschäftigung ausführen? Geben Sie an, welche Erwartungen Sie an ein neues Arbeitsverhältnis haben. Geben Sie dazu bitte auch einen Arbeitsortswunsch an.

Umzugsbereitschaft: Uneingeschränkt

Bewerbergruppe: Berufsanfänger

Beschäftigungsgrad: -- Bitte auswählen --

Schichtarbeit: □

Frühestmöglicher Eintrittstermin:

Interesse an Praktikum / Werkstudententätigkeit: -- Bitte auswählen --

Verfügbarkeit für Praktikum /

Dauer des Praktikums/ der: -- Bitte auswählen --

November 2017

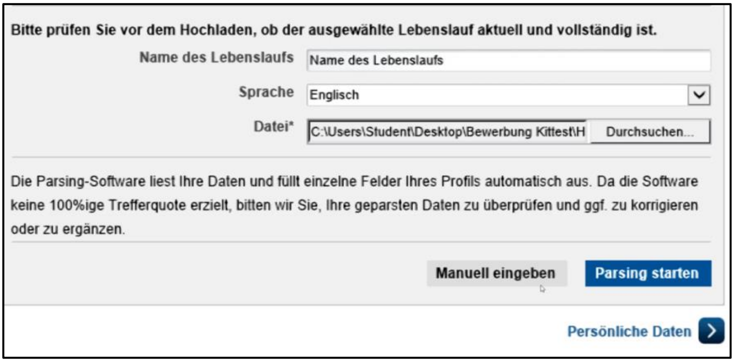
Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

Welcher Tätigkei

Figure 6.5: BASF: Calendar freezes screen reader

6.5.14 Automated data entry, via parsing

Parsing is an effective mechanism to make a CV machine readable in order to automatically perform data entry. So, it was surprising not to see this more widely deployed.



Bitte prüfen Sie vor dem Hochladen, ob der ausgewählte Lebenslauf aktuell und vollständig ist.

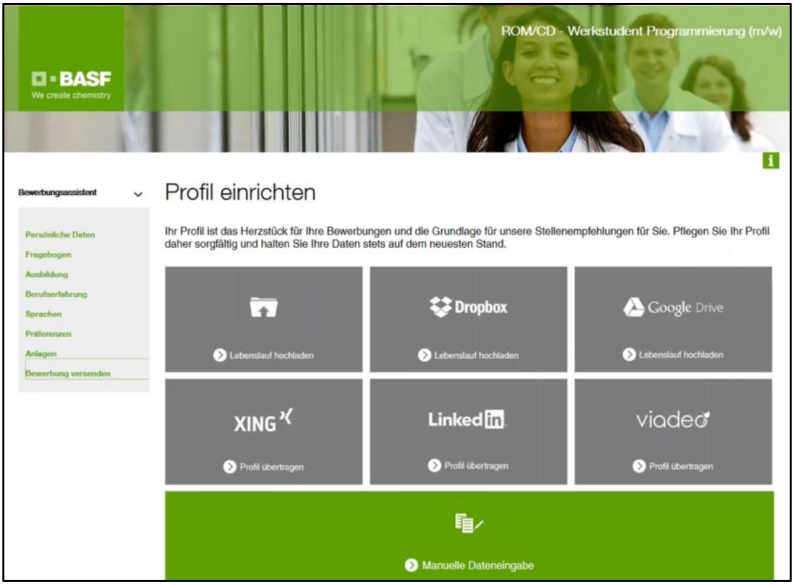
Name des Lebenslaufs: Name des Lebenslaufs

Sprache: Englisch

Datei*: C:\Users\Student\Desktop\Bewerbung Kittest\H

Die Parsing-Software liest Ihre Daten und füllt einzelne Felder Ihres Profils automatisch aus. Da die Software keine 100%ige Trefferquote erzielt, bitten wir Sie, Ihre geparsten Daten zu überprüfen und ggf. zu korrigieren oder zu ergänzen.

Figure 6.22: Bosch: Useful parsing capability



Profil einrichten

Ihr Profil ist das Herzstück für Ihre Bewerbungen und die Grundlage für unsere Stellenempfehlungen für Sie. Pflegen Sie Ihr Profil daher sorgfältig und halten Sie Ihre Daten stets auf dem neuesten Stand.

Figure 6.23: BASF: Upload options, good feature, but not accessible

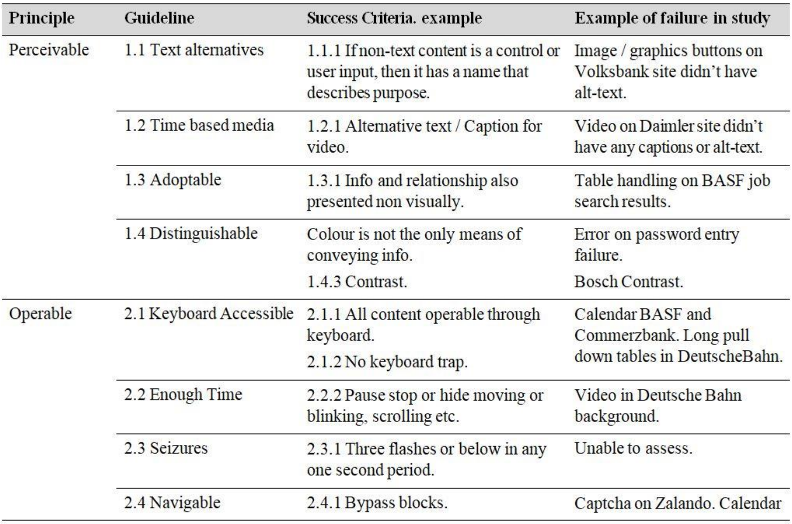
While uploading the CV would be very advantageous from a data capture perspective for people with disabilities, it does require the upload capability itself to be accessible. This screen was problematic in that the field descriptions were not informative enough (alt text). So, without sighted help, this was impossible to use.

The Zalando site also offered LinkedIn integration, removing the need to type in almost everything. We did not notice this capability used to this extent on other sites. None of the sites made use of web identity solutions such as Google ID or Open ID. As password management was seen as a major frustration by the test users, this is a missed opportunity.

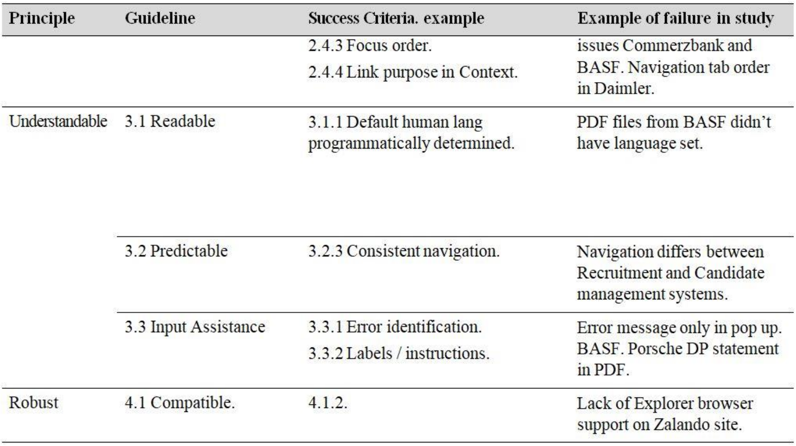
6.6 Issue overview, mapped to the WCAG 2.0 principles

The chart overleaf maps a number of the issues that the testing found against the WCAG 2.0 standard.

Table 6.6: Summary against WCAG 2.0 criteria



Principle	Guideline	Success Criteria. example	Example of failure in study
Perceivable	1.1 Text alternatives	1.1.1 If non-text content is a control or user input, then it has a name that describes purpose.	Image / graphics buttons on Volksbank site didn't have alt-text.
	1.2 Time based media	1.2.1 Alternative text / Caption for video.	Video on Daimler site didn't have any captions or alt-text.
	1.3 Adoptable	1.3.1 Info and relationship also presented non visually.	Table handling on BASF job search results.
	1.4 Distinguishable	Colour is not the only means of conveying info. 1.4.3 Contrast.	Error on password entry failure. Bosch Contrast.
Operable	2.1 Keyboard Accessible	2.1.1 All content operable through keyboard. 2.1.2 No keyboard trap.	Calendar BASF and Commerzbank. Long pull down tables in DeutscheBahn.
	2.2 Enough Time	2.2.2 Pause stop or hide moving or blinking, scrolling etc.	Video in Deutsche Bahn background.
	2.3 Seizures	2.3.1 Three flashes or below in any one second period.	Unable to assess.
	2.4 Navigable	2.4.1 Bypass blocks.	Captcha on Zalando. Calendar



Principle	Guideline	Success Criteria. example	Example of failure in study
		2.4.3 Focus order. 2.4.4 Link purpose in Context.	issues Commerzbank and BASF. Navigation tab order in Daimler.
Understandable	3.1 Readable	3.1.1 Default human lang programmatically determined.	PDF files from BASF didn't have language set.
	3.2 Predictable	3.2.3 Consistent navigation.	Navigation differs between Recruitment and Candidate management systems.
	3.3 Input Assistance	3.3.1 Error identification. 3.3.2 Labels / instructions.	Error message only in pop up. BASF. Porsche DP statement in PDF.
Robust	4.1 Compatible.	4.1.2.	Lack of Explorer browser support on Zalando site.

Tester comments about the exercise

The testers all agreed to record video interviews, herewith translated, lightly edited excerpts from those interviews.

> *Tester: Well, actually… sometimes it was quite good, sometimes it was quite bad. So, in case of public authorities, like the Federal Bank (Bundesbank) or the Foreign Office (Auswärtiges Amt), it worked well, with some small trade-offs, but you could get though them by yourself... application, you could apply, the information was accessible, usually there was an option to state disability. In case of private companies, there was Porsche which was more-less an exemption. It worked there reasonably well. But BASF and Daimler was again a catastrophe because… because at BASF you couldn't even register by yourself, and at Daimler it was impossible to send your application. Yes, Daimler indeed states on its website that they welcome the applications of people with disabilities, but you see things differently ... when you can't apply*

Well, none of them was completely trouble-free, even on the sites where it went really well, in the Foreign Office, or in case of the Federal Bank, there were always a few details, like a text box wasn't properly labelled, so you had to ask someone, or do some research on your own, to find out what you had to write in that field. So none of the sites was completely, hundred percent problem-free, taking into account that in case of the mentioned applications, with a little effort, you could have find out what to write in there by yourself, most likely. In case of the other websites there were so many problems that you couldn't use them without help.

Reporter: And, do you have any advice for those in charge of these websites? What should they do?

Tester: it would really help a lot if the headings would actually be labelled as headings, as this makes navigation a lot easier, and please label the input fields in a way that people would know what they have to write in there, especially in case of yes/no questions, it's often a problem that it's read to you that you can select yes or no, but you don't know for what. Or those fields where you have to agree to some sort of text like privacy policies… the best would be to have "yes, I acknowledge… I have read" or just put it directly into the confirmation field, that it needs to be confirmed, because…

Well, in fact I had consistently bad experiences with PDFs. The one at BASF was completely unreadable, the one at Daimler was readable, but the navigation was impossible within the document, you had to go through it from top to bottom…

> *Tester: Well, we've learnt what we had already thought, that it works quite well in case of public authorities. It's not hundred percent perfect, but you can work with it. And… in case of private companies it is extremely difficult, I mean at Porsche it have worked to some extent, but it was still complicated here and there. And in case of the other companies, it didn't work at all. The private sector which is so terrible that you can't even apply to two out of three companies, or that it's impossible without considerable help from a normal-sighted person. This wasn't necessarily what I expected, but in principle it confirmed what I thought, that in the private sector it's rather worse than in case of public authorities.*

6.7 Automated testing of the career sites

6.7.1 Automated web site testing

As well as the observational test with the users, the study tested the first page of career sites with an automated testing tool for BITV and WCAG 2.0. The tool used was AChecker, as this is used regularly by the SZS department for its testing. AChecker is an open source tool, developed by the Adaptive Technology Research Centre at the University of Toronto.[55] It is widely used, especially in more recent testing research. See Vigo for a detailed benchmark of testing tools.[56] AChecker tests for multiple standards, for instance WCAG 1.0, WCAG 2.0, Section 508, BITV 1.0 and the Italian Stanca Act. AChecker identifies three types of problem.[57]

[55] Greg Gay and Cindy Qi Li, 'AChecker', *Proceedings of the 2010 International Cross Disciplinary Conference on Web Accessibility (W4A) - W4A '10* (ACM Press 2010).

[56] Markel Vigo, Justin Brown and Vivienne Conway, 'Benchmarking Web Accessibility Evaluation Tools', *Proceedings of the 10th International Cross-Disciplinary Conference on Web Accessibility - W4A '13* (ACM Press 2013).

[57] Sohaib and Kang.

- Known Problems: These are problems that must be fixed and have been identified as accessibility barriers.
- Likely Problems: These are problems that are likely to be fixed and have been identified as probable barriers.
- Potential Problems These are problems that require a human decision to modify or not modify your webpage.

Rather than simply giving a pass or fail score, the tool provides a detailed explanation of the issue, suggesting fixes, see example at Figure 6.9 (check). The tables below list the number of problems on the first page of the career site. The first table is for BITV 1.0 level 2, the second table for WCAG 2.0 level AA.

Table 6.7: BITV 1.0 level 2 test with AChecker

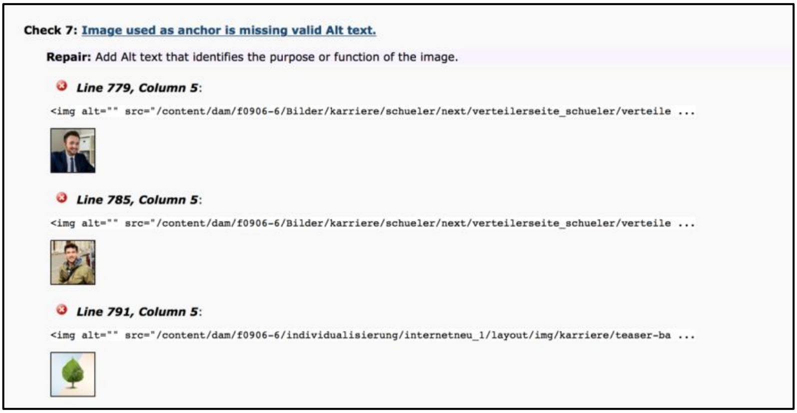
Organization	**Career site first page**	**Problems**		
		Known	**Likely**	**Potential**
BASF	*https://www.basf.com/de/de/company/career.html*	72	124	303
Bosch	*https://www.bosch.de/karriere/*	11	59	188
Bundesbank	*https://www.bundesbank.de/Navigation/DE/Bundesbank/Karriere/karriere.html*	4	138	189
Auswärtiges Amt	*https://www.auswaertiges-amt.de/de/uebersicht-node-ausbildungkarriere/aamt*	1	106	211
Porsche	*https://www.porsche.com/germany/aboutporsche/jobs/employer/*	41	179	362
Commerzbank	*https://www.commerzbank.de/de/hauptnavigation/karriere/karriere.html*	10	138	189
Daimler	*https://www.daimler.com/karriere/*	12	582	765
Zalando	*https://jobs.zalando.com/de/*	0	0	0
Volksbank	*https://www.vr.de/karriere.html*	57	155	344
Deutsche Bahn	*http://www.deutschebahn.com/de/jobs_karriere/*	138	575	740

Table 6.8: WCAG 2.0 level AA test with AChecker

Organization	Known problem	Likely problem	Potential Problem
BASF	66	0	508
Bosch	5	0	289
Bundesbank	1	1	423
Auswärtiges Amt	0	0	0
Porsche	11	0	705
Commerzbank	8	0	370
Daimler	5	0	1449
Zalando	0	0	0
Volksbank	30	0	670
Deutsche Bahn	138	3	499

The vast majority of errors were graphical images that were not labelled. Many of the images on these websites do not serve a particular critical purpose, but, nevertheless, they should be labelled and also avoided in navigation, when appropriate. The landing page of the Deutsche Bahn careers has the highest error count, but the error is a relatively minor one (use of italics, check 117), repeated in the background on many elements. This may impact text resizing for visually impaired users. On the Volksbank site, there are a number of images (at least 10) used for navigation, and these are identified by the tool as being without alt text. These are more severe.

In the lab test, this lack of alt text was a major navigation challenge for the testers, as these images were the springboard to other important parts of the site.



Check 7: Image used as anchor is missing valid Alt text.

Repair: Add Alt text that identifies the purpose or function of the image.

Line 779, Column 5:

```
<img alt="" src="/content/dam/f0906-6/Bilder/karriere/schueler/next/verteilerseite_schueler/verteile ...
```

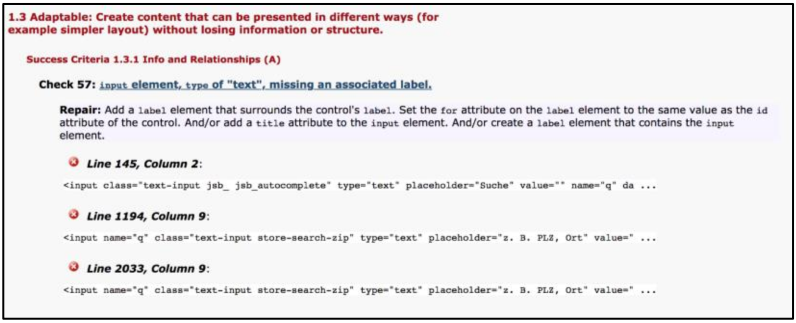
Line 785, Column 5:

```
<img alt="" src="/content/dam/f0906-6/Bilder/karriere/schueler/next/verteilerseite_schueler/verteile ...
```

Line 791, Column 5:

```
<img alt="" src="/content/dam/f0906-6/individualisierung/internetneu_1/layout/img/karriere/teaser-ba ...
```

Figure 6.24: Volksbank alt text error



1.3 Adaptable: Create content that can be presented in different ways (for example simpler layout) without losing information or structure.

Success Criteria 1.3.1 Info and Relationships (A)

Check 57: `input` element, `type` of "text", missing an associated label.

Repair: Add a `label` element that surrounds the control's `label`. Set the `for` attribute on the `label` element to the same value as the `id` attribute of the control. And/or add a `title` attribute to the `input` element. And/or create a `label` element that contains the `input` element.

Line 145, Column 2:

```
<input class="text-input jsb_ jsb_autocomplete" type="text" placeholder="Suche" value="" name="q" da ...
```

Line 1194, Column 9:

```
<input name="q" class="text-input store-search-zip" type="text" placeholder="z. B. PLZ, Ort" value=" ...
```

Line 2033, Column 9:

```
<input name="q" class="text-input store-search-zip" type="text" placeholder="z. B. PLZ, Ort" value=" ...
```

Figure 6.25: Info and relationships success criteria 1.3.1

For this research, we only tested the first page of the career site, not the complete process flow. Just testing the first page obviously does not give visibility into the complete process, but it is a useful start. The author surmises that the further into the process the worse the accessibility standards compliance would be, given the greater complexity of the input screens, and the “Potemkin village” tendency of corporate and government websites. The automated website tests are able to easily identify many but not all of the issues that plagued the test users, and they provide excellent feedback to those responsible for the web-site design and deployment.

The automated test should not be seen as a substitute for user testing, but it should be a key part of the website readiness assessment. At the very least, recruitment managers can use these tools themselves to ask questions of those responsible for website testing. Using the number of errors to rank sites is not accurate, as the severity of the errors is not assessed.

Looking at the test results above, it clear that the testing of career sites for accessibility is haphazard at best. Most of the errors that the tool finds are very simple to repair. The tool is not able to pass judgement on broader usability, but it is effective at highlighting failing based on the standards.

Zalando's perfect score on the automated tests can be attributed to disciplined web design, testing and deployment, as well as the simplicity of the design itself. Given that the Zalando business is completely online, they were more likely to have better accessibility, but, as the Sohiab[58] study notes, this is not a given.

6.7.2 Automated PDF testing

Several of the career sites we examined make use of PDFs, for the reasons discussed above. Several PDF files were selected from the test organizations. They were tested against the ISO-14289:2008 standard, otherwise known as PDF / UA-1. The tool used to do the testing is an open source tool called PAC3 from the *Schweizerische Stiftung zur behindertengerechten Technologienutzung*.[59]

[58] ibid.

[59] *http://www.access-for-all.ch/en/*

The tool provides a detailed report, defining and describing the errors in the documents. All PDFs that the testers engaged with in the lab were either inaccessible or awkward to access. On viewing the automated test results, it illustrates little effort is given to PDF accessibility design or testing before posting on the career sites.

Table 6.9: PDF accessibility test summary

Organization	Daimler	Commerzbank	BASF	Auswärtiges Amt	Bosch
PDF purpose/ name	Diversity brochure	Career path overview	Application process guide	Introductory brochure	Data protection statement
Significance in business process	low	medium	medium	medium	high
Marked as inaccessible	No	No	No	Yes, labelled as "nicht barrierefrei"	No
Test fail	yes	yes	yes	yes	yes
Checkpoint fail	10/11	8/11	7/11	8/11	5/11
PDF usage level	medium	high	medium	low	low

While not all career sites made use of PDFs, most did, and none was easily accessible. Today, it is simple to create an accessible PDF. There are tools with templates to guide content writers to develop accessible content, and there is a growing array of tools to test and correct PDF accessibility errors. The failing on PDF accessibility is hard to justify and the author suspects that the PDFs are written by HR and not checked against standards when saving. This is a relatively trivial process with content tools today.

6.8 Summary: Evidence of negative externalities and their impact

The research question asks, “How does the software industry fail to deliver accessible solutions?”

Firstly, this section showed, in some detail, how this set of German organizations has largely failed to deliver accessible recruitment for people with disabilities. The frustrating experiences of the testers clearly highlights the externality problem at the centre of this dissertation. Code can discriminate.

The private sector organizations were typically poor, with limited regard for accessibility standards compliance. This is despite many of those organizations proclaiming a strong focus on diversity and inclusion. The public-sector websites were somewhat better, due in part to demands of German Barreifreiheit regulations.

Secondly, many of the usability issues that made things very difficult for the testers would also have been frustrating for the sighted user. Overly complex passwords, excessive use of structured data fields, awkward attachment handling, verbose marketing texts, for instance, would be irritating for any user. Fixing usability would help all users.

Thirdly, fixing the vast majority of these issues is not particularly difficult. The accessibility of the career sites would be significantly improved with a more disciplined approach to alt text field labelling and tab navigation flow.

Finally, further study would be required to establish if the accessibility problems are created by the underlying standard software, by bespoke software or by the customization and deployment of standard software. A cursory assessment would suggest that it is a mixture of all three.

This chapter has illustrated that software developers continue to deliver inaccessible solutions. It illustrated the impact of this externality on the testers in that it was difficult for them to use the recruitment channels of some of Germany's leading employers. While employers talk extensively of diversity, the reality of their corporate career sites illustrates the large gap between rhetoric and practice.

The next chapter will explore the reasons for the inaccessibility externality in more detail.

7 Exploring the causes of accessibility failure

7.1 Chapter purpose: The causes of accessibility failure

The many surveys on web accessibility paint a remarkably similar picture. Bluntly put, the web is not accessible. This chapter will explore the reasons behind this in more detail, using the Lessig framework discussed in the context chapter to guide the discussion.

The chapter following this one will include some examples of good accessibility. To paint all technology as a negative externality for people with disabilities would be inaccurate. There are many examples where software technology has dramatically improved the lives of people with disabilities so it would be remiss not to mention them.

Understanding why software fails at accessibility will help to fix it.

7.2 Law: Fragmentation and limited enforcement

While the legal position of web accessibility in the US public sector is clear, the state of web accessibility in the private sector remains unresolved and fraught with dispute. Guidelines from the DOJ are not likely to be forthcoming for the next few years and recent actions point to a rolling back of regulation rather than stricter enforcement. In Germany, the public sector position is clear, but there are no direct private sector law obligations. While the law in the UK creates clear obligations for both the public sector and the private sector, the lack of case law is puzzling.

While the UNRDP is a positive step, the lack of an implemented European directive is problematic. Market: CIO attention or inattention?

In the section on accessibility in the developer survey, the survey population noted that over 60% of organizations that they work for take accessibility into account. This seems rather optimistic, given the current state of accessibility.

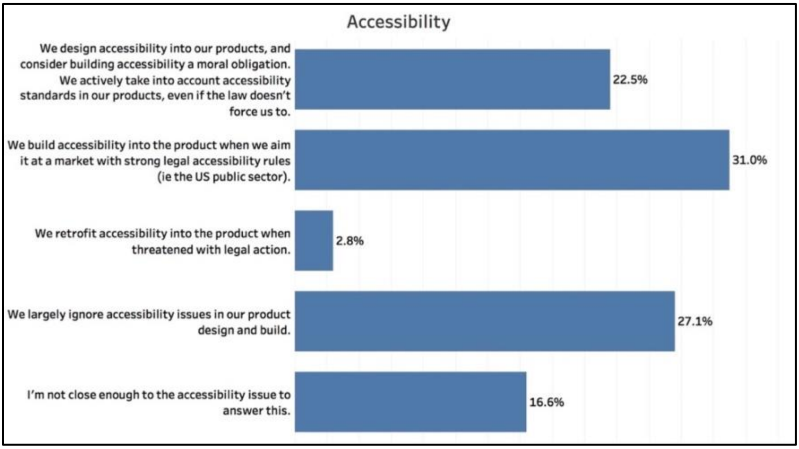


Figure 7.1: Accessibility survey response

Surveying CIOs on accessibility would be one way to assess CIO focus on accessibility. One challenge though is that it is unlikely that CIOs would actually admit a lack of focus on accessibility, at least openly. However, a useful proxy to measure CIO interest would be to assess whether and what the industry analysts have written about accessibility.

Firms such as Gartner[1] and Forrester[2] provide extensive, broad advisory services to IT executives.[3] Tools such as Magic Quadrants, Hype Cycles, Waves, etc. are seen by CIOs as trusted sources of information for IT decision making.[4] Gartner and other firms have a significant influence on CIO attention and focus.[5] The advisory research is generally of a practical nature, aimed at providing advice and guidance to IT leaders and software vendors. Typically, the questions that the clients ask drive the research agenda.[6]

On 4th November 2017, a search was run using the Gartner Research Note Search capability. There are roughly 120,000 notes in the searchable data base. While the research itself is not able to be read without a subscription, the metadata (note title and summary) is adequate for this exercise.

[1] Gartner is listed on the NYSE and employs 13,000 people. 2016 revenues were 2.44 billion USD. Market capitalization as of November 2017 was just over 10 billion USD. Roughly 1,300 employees are classified as analysts as of the 2016 10-k.

[2] Forrester is listed on the NASDAQ. It employs 1400 employees, with 520 in research and consulting. 2016 revenues were 326 million USD. Market capitalization as of November 2017, just over 800 million USD.

[3] David R Firth and E Burton Swanson, 'How Useful Are IT Research and Analysis Services?' (2005) 48 Business Horizons 151; Neil Pollock and Robin Williams, 'Industry Analysts – How to Conceptualise the Distinctive New Forms of IT Market Expertise?' (2015) 28 Accounting, Auditing & Accountability Journal 1373; Daniel E O'Leary, 'Gartner's Hype Cycle and Information System Research Issues' (2008) 9 International Journal of Accounting Information Systems 240.

[4] Neil Pollock and Robin Williams, 'The Sociology of a Market Analysis Tool: How Industry Analysts Sort Vendors and Organize Markets' (2009) 19 Information and Organization 129.

[5] Tom D Burks, 'Use of Information Technology Research Organizations as Innovation Support and Decision Making Tools', *Southern Association for Information Systems 2006 proceedings* (2006).

[6] The Gartner 10-k notes: Our research agenda is defined by clients' needs, focusing on the critical issues, opportunities and challenges they face every day. Our research analysts are in regular contact with both technology providers and technology users, enabling them to identify the most pertinent topics in the IT marketplace and develop relevant product enhancements to meet the evolving needs of users of our research. See https://www.gartner.com/imagesrv/pdf/Gartner_2016_annual_report.pdf

The search was not able to find any report that evaluates accessibility testing tools, and the most recent research notes focused on creating an accessible website were published in 2003 and 2008. Gartner publishes several hundred Magic Quadrants, but only a handful appear in a search on accessibility terms. The Magic Quadrant for Web Content Management was one such note. A few hype cycles also mention solutions for visually impaired users.

Table 7.1: Search term analysis of Gartner Research metadata

Search term	Number of Research Notes (includes duplicates)
WCAG	34
Section 508	89
“Americans with Disabilities Act”	49
“Universal design”	12
“Visually impaired”	75
Dyslexia	6
Section 503	1
UNCRPD	0
EN 301549	0

Mentions of accessibility related topics in analyst research

There was a maverick research note published in 2017 entitled “Maverick* Research: From Disability to Superability, Society and the Workplace Are Changing” with the summary headline: “Emerging technologies will unleash the abilities of 350 million people with disabilities, leading to employment rates on a par with the general population. (Maverick research deliberately exposes unconventional thinking and may not agree with Gartner’s official positions.)” There was also a note published in 2014 “What IT Leaders Need to Know About New Rules and Opportunities When Hiring People With Disabilities.”

A similar search was run on the Forrester website on the same day. (Forrester publishes less research overall than Gartner). There was one note uncovered via an ADA search, published in 2007, mentioning the target case, "Prepare To Be Challenged On Web Accessibility Compliance."[7] There was also a note on "Designing interactions for An Ageing Population" published in 2007.[8]

Gartner and Forrester provide very little research coverage on accessibility. This is simply a reflection of the lack of demand from CIOs and other IT leaders for accessibility advice. If a significant number of corporations were seriously concerned about accessibility, it is likely that there would be a rich series of research notes from the leading analyst firms advising them on accessibility best practice, and an evaluation of accessibility tools such as testing tools.

By way of contrast on the Gartner site, GDPR has 184 mentions in 2017 alone, and many notes providing pertinent advice, including a privacy hype cycle.

7.3 Social norms: Developer knowledge and attitude

Over a decade ago, Sullivan and Matson[9] stated:

> *Advances in development technology are not always paralleled by advances in developer awareness. Guidelines for*

[7] https://www.forrester.com/report/Prepare+To+Be+Challenged+On+Web+Accessibility+Compliance/-/E-RES41644d

[8] *https://www.forrester.com/report/Senior+European+Visitors+Have+Specific+Web+Needs/-/E-RES42096*

[9] Terry Sullivan and Rebecca Matson, 'Barriers to Use: Usability and Content Accessibility on the Web's Most Popular Sites', *Proceedings on the 2000 Conference on Universal Usability - CUU '00* (ACM Press 2000).

> *content accessibility and usability are available to Web developers, and are widely known and heavily publicized. Yet our results suggest that many Web designers either remain ignorant of, or fail to take advantage of, these guidelines.*

The gap in education and training is clearly a problem. In the software developer survey, only 12.5% of respondents had received formal training about accessibility.[10]

But the issue is not merely one of technical training. There is also an ethical challenge. Chisholm and May are accessibility textbook authors,[11] are advocates for accessibility and universal design, and often encounter hesitancy and even hostility to the idea of increasing a site's accessibility. The attitudes and behaviours of some developers should be a major cause for concern.

7.3.1 Examining comments on Slashdot

Scanning through developer chat boards is a useful way of getting a sense of developer perspectives on accessibility. A more rigorous study such as those done to analyze political discourse on chat boards[12] would reveal much more about developer sentiment on a variety of issues.

Slashdot.org is a popular chat board for web developers and those interested in technology. There are several threads on accessibility, with some commentators showing a more enlightened approach to disability, but many not. Examples below, as the tone and choice of language is illustrative.

[10] Q12. 27.27% of the respondents answered that they had received formal training, either at work or as part of their education.

[11] Chisholm and May.

[12] Tony Mullen and Robert Malouf, 'A Preliminary Investigation into Sentiment Analysis of Informal Political Discourse', *American Association for Artificial Intelligence. Spring Symposia* (AAAI 2006).

Example 1:

> *If there's a need for a disabled-friendly Blackberry or iPhone or whatever ... wouldn't the market invent one and sell it? Why should ALL of us pay for features we neither need nor want?*
>
> *I see no disabled-friendly footballs out there. Nor hand grenades. Nor microscopes. Nor National Match quality .22 caliber rifles. Nor Porsche race cars. Perhaps might there be things the disabled should NOT be doing? Like trying to see ANYTHING on a tiny little screen, trying to punch tiny little keys and buttons?*
>
> *As usual the KongressKritters are totally off-base, doing the politically correct thing, and not showing a lick of sense or moderation.*
>
> *Morons*[13]

Example 2:

Another thread discusses a review of computer games from a disability perspective.

> *Instead of suing and getting angry at the world, this guy should just have the serenity to accept the things that he can't change and move on with his life. This is the way the world works, and we can't do anything about it…*
>
> *If you're blind…guess what? You're never doing to drive a car. End of story*

[13] At *http://yro.slashdot.org/comments.pl?sid=1756328&cid=33275014* first accessed on 12.8.2011

> *If you have no legs or can't walk, you're never going to learn karate and becoming a kickboxing champion. End of story*
>
> *There are certain things, of course yes we can make more accessible to the disabled, but I'm sorry, gaming is NOT one of them. A recreation that refines split second reflex and hand eye coordination SHOULD NOT BE MUCKED UP so someone with fucking parkinsons can play it 'easier'.*
>
> *If you have Parkinson? Sorry you simply can play games that require a steady refined hand. END OF STORY. .*[14]

Example 3:

> *I know im going to get modded as troll / flamebait but i am SICK TO DEATH of people who are PHYSICALLY LIMITED EXPECTING TO BE ABLE TO DO THINGS AS IF THEY ARE NOT: REALITY CHECK, YOU CAN'T AND YOU NEVER WILL, DEAL WITH IT*[15]

Example 4:

> *Just because a service offered by a company is popular doesn't mean that you can whine that they are violating your "rights" should they fail to make accommodations for your demographic. That isn't discrimination, that's business. If you dislike it, spend your money elsewhere.*
>
> *I'm a liberal person, but I find it pretty ridiculous that minority groups act like they have a right to any convenient*

[14] At *http://games.slashdot.org/comments.pl?sid=1463644&cid=30295520* first accessed on 12.8.2011.

[15] At *http://games.slashdot.org/comments.pl?sid=1463644&cid=30295956* first accessed on 12.8.2011

> *piece of technology that comes down the pipes being tailored to their particular needs.* [16]

There are many commentators who have a more enlightened view on accessibility.

> *Has anyone participating in this discussion actually done web design for accessibility? I've been looking at it for our course management system. It's not trivial, but it's also not difficult. In increases development time / cost, but probably not more than 10%. It's perfectly possible to design reasonable visual interfaces that work fine with common screen readers. A sighted user won't even be aware that it's been done. It's a combination of avoiding some standard pitfalls that a screen reader can't reasonably work around, and putting appropriate labels and tags on everything. A lot of tools are accessible. jQuery has been doing an increasingly good job. The CK editor has as well.*
>
> *The issue isn't just blind people. Older people (like me, to be honest) sometimes need to increase font size, and would really like it if the web page design doesn't fall apart.*
>
> *There's no way you're going to get away with saying "sorry, they should know they're handicapped." The law won't allow it, and in my opinion shouldn't. I might feel differently if there weren't reasonable approaches to dealing with it. The big problem is getting web developers to think about it, and to try their software with a screen reader now and then.*[17]

[16] At *http://tech.slashdot.org/comments.pl?sid=2040692&cid=35509440* first accessed on 12.8.2011

[17] At *http://tech.slashdot.org/comments.pl?sid=2040692&cid=35511108* first accessed 12.8.2011

While this website is not representative of the whole software community, there is a disturbing level of ignorance and bigotry towards people with disabilities. This does not bode well for accessible software development. While bigotry outlined above is not typical, for many software developers, the idea that a person with disabilities might want to use what they build comes as a surprise.

Tynan commented in the interview when discussing website accessibility:

> *Anne: I think there's a failure because of the lack of understanding of the legal requirement.*
>
> *Thomas: Who has that lack of understanding? Is it the software developers, or is it the people that are commissioning the websites, or is it both?*
>
> *Anne: Well, without knowing many personally, I think it's clear that software developers must have a lack of knowledge, because otherwise they would be more active in this area. But I think that there is a gap between software developers, IT people, if I can just call them that broadly, and lay people.*[18]

While accessibility is often ignored, even when it is not, it is seen as a technical requirement rather than as an ethical obligation to a fellow human being. It points to a mindset of disability as a medical problem rather than the rights model. The blame for this lack of empathy should not be laid at the feet of the individual developers alone; in the main, it is a failure of how they are educated, trained and managed.

[18] See Appendix A

7.4 Social Norms: Design thinking in software design: inclusive or exclusive?

Often, before the software developer develops the application, designers come up with the design. The field of design has developed rapidly over the last 15 years and design thinking is now well established. Design thinking initially gained attention in the late 1980s through the work of Harvard Graduate School of Design professor, Peter Rowe. His book, *Design Thinking*, was the first significant use of the term. The design firm IDEO further popularized and refined the methodology, with David and Tom Kelley. Design thinking is now well established in software development, with many software companies, universities and IT departments applying the principles of design thinking to software development.[19] Design thinking has brought techniques that were previously the domain of the professional designer into more mainstream usage.[20]

There is some debate in design circles on the terminology and marketing of design thinking, and how it relates to participatory design, [21] but this is of peripheral relevance here.[22]

[19] Curedale, *Design Thinking: Process and Models* (3rd edn, DCC 2016).

[20] See for instance *http://www.designthinkersacademy.com/*

[21] Christoph Meinel, Larry Leifer and Hasso Plattner (eds), *Design Thinking* (Springer Berlin Heidelberg 2011); Birgit Jobst and others, 'The Faith-Factor in Design Thinking: Creative Confidence Through Education at the Design Thinking Schools Potsdam and Stanford?', *Design Thinking Research* (Springer Berlin Heidelberg 2012); Ulla Johansson-Sköldberg, Jill Woodilla and Mehves Çetinkaya, 'Design Thinking: Past, Present and Possible Futures' (2013) 22 Creativity and Innovation Management 121; Lucy Kimbell, 'Rethinking Design Thinking: Part I' 3 Design and Culture 285.

Design thinking techniques are now used to rethink business processes and design services, not just products. It is taught at many universities[23] and it has captured the imagination of the business and IT press. Design thinking is seen as a technique to encourage innovation.[24] It is also taught to MBA students.[25] The design thinking process is defined as follows: [26]

1. Define intent
2. Through ethnographic research develop empathy for the point of view of the user
3. Synthesize the research
4. Frame insights
5. Explore concepts
6. Synthesize the concepts
7. Prototype the favoured ideas
8. Test prototype with users
9. Incorporate changes
10. Iterate prototype and testing until a working design is reached
11. Implement
12. Deliver offering

[22] In the interview with Matthew he was asked about design thinking education: "Yes, the leading ones of that would be the school in Potsdam, the school of design thinking. And then also the Stanford d.school and the Institute for Design in Chicago teaches a program around this. There's a couple of other programs that teach it as well. The interesting thing is that the traditional design schools, like the big, powerhouse traditional industrial design and graphic design schools tend not to appreciate it as much. The traditional design community still kind of sees this as an... An affront is too strong of a word, but they see it as a threat, at least, to their role in the product development process as being the creative people."

[23] See *https://dschool.stanford.edu* and *https://emeritus.org/management-certificate-programs/innovation-design-thinking/*

[24] Sara L Beckman and Michael Barry, 'Innovation as a Learning Process: Embedding Design Thinking' (2007) 50 California Management Review 25.

[25] R Glen, C Suciu and C Baughn, 'The Need for Design Thinking in Business Schools' (2014) 13 Academy of Management Learning & Education 653.

[26] Roger L Martin, *Design of Business: Why Design Thinking Is the Next Competitive Advantage* (Harvard Business Press 2009); Curedale.

Design thinking stresses early user involvement and the creation of personas, fictional characters that closely represent the users. This allows the software development team to test design concepts against the personas and build applications that more closely meet user requirements, and that are ultimately more usable. Tim Brown, the CEO of IDEO, stated:

> *Design thinking is a human-centered approach to innovation that draws from the designer's toolkit to integrate the needs of people, the possibilities of technology, and the requirements for business success.*[27]

On reading several design thinking text books, manuals and practitioner websites and blogs, while terms such as user centricity, empathy, ethnographic research, human centered, etc. are used extensively, there is little or no mention of designing for or with people with disabilities. The author reviewed other leading textbooks on software design, with similar results. Design thinking, as it is typically practised, largely ignores people with disabilities. Design personas in enterprise software tend to reflect a society bereft of people with disabilities:

> *As Creative Director of the company over the last ten years, I have probably seen hundreds of briefs for different projects. In my experience, I have to tell you, designing solutions to be as inclusive as possible has never been a primary, secondary, or even tertiary requirement of any.*[28]

In 2011, the author interviewed a leading design thinking expert, who has worked at several leading software companies.[29]

[27] See *https://www.ideou.com/pages/design-thinking*

[28] Law 31.

[29] Interview lightly edited for brevity. See Appendix D.

Thomas: Do this broadly at an industry level, don't pick out one company. But how does the design process link into accessibility or not.

Matthew: Yeah. It's mostly the "or not" part, unfortunately, I think, from my experience. I think that a lot of companies are willing to play the numbers game and say, there's only such a small percentage of users with this particular disability, therefore, we can write off that part of the market, if they don't like our product or if it's too hard to use. Or we'll just rely on the operating system to take care of this for us, because the major operating systems are much more compliant focused, because they have to sell their products to the government.

Most of the individual software companies, the bigger ones that have government contracts, tend to build in more compliance. But, often times, they make it a modal switch in their application. So, it's kind of like you go into the accessibility mode, as opposed to a graceful degradation kind of thing, into an accessibility path, or building it into the websites, for example.

They rely on the browser to manage most of those issues for them. So, if they need to increase font size or contrast or if they need to do text to speech, they rely on third party applications, the browser and the operating system, to provide that for them. Which is unfortunate, because the sites that do build in the accessibility issues into the style sheets of the websites or into the software that runs on the desktop, have a much better experience with users.

Thomas: They're for disabled and non-disabled users in that context, you mean.

> *Matthew: Yeah.*
>
> *Thomas: So, you'd say that, I don't want to put words in your mouth here, but you would say that the private software companies on the whole's take accessibility as haphazard.*
>
> *Matthew: At best, yeah. And I think, I've worked in some companies where they specifically just take it off the table. I mean, their approach is simply just to say, we're not going to do it. If they get push back from a user group or, you know, there used to be more advocacy groups that seemed to be more prevalent back in the '90s than there are now for this kind of a topic, but unless they're really pressured into doing it, or contractually, they have a requirement to do that, like to sell software to a state or federal level, they usually are pretty much haphazard at it. The exceptions have been companies where family members of the executives actually have these types of logistical challenges. And those people tend to be much more sensitive, because they have a family member who actually has that same issue.*

In addition, the visual paradigm dominates software design practice.

For instance, participatory design expert Sahib[30] makes the point that the tools designers use to show early prototypes and ideas are themselves not accessible. Early designs do not lend themselves to screen reader access. They also note that in the context of interface design, they could not find reported research on the use of scenarios for participatory design with blind users. The use of scenarios is well established in design thinking so the lack of research relating to people with disabilities is in itself revealing.

[30] Nuzhah Gooda Sahib and others, Participatory Design with Blind Users: A Scenario-Based Approach 2013 685.

7.4.1 Social norm: Academic research and teaching silos

As cited throughout this chapter, there is a rich vein of accessibility research in universities, in computer science, law, the social sciences and medical fields. This has not translated into awareness in the student body, and often not in what should be related fields of research. While there is some multi-disciplinary engagement,[31] accessibility awareness is not uniformly distributed across academia either.

Computer science and information technology

A scan of computer science and information systems curricula at several leading universities points to a dearth of student education on accessibility. Universities typically have a course, but it is rarely compulsory. The bestselling user design textbook, *About Face*, does not even mention accessibility. A scan of other leading software engineering text books used in universities for introductory computer science also found no mention of accessibility.

Information technology law

Accessibility is not seen as a mainstream topic in computer law teaching. A website scan of leading technology law LLM programmes also highlighted a lack of any accessibility or disability modules or submodules,

[31] See for instance the cross-disciplinary conference series W4A.

at least that were obviously described as such.[32] A keyword search on accessibility related terms such as WCAG, ADA, accessibility, etc. suggested that accessibility is rarely covered in leading Information Technology Law journals.[33]

7.5 Code: Imperfect standards

Although the WCAG guidance is widely recognized, it is not without its issues. The standards have developed relatively slowly and do not address all forms of disability. Law-makers in many countries have acknowledged either WCAG 1.0 or WCAG 2.0 as the accessibility standard,[34] meaning that it is more than merely a guideline.

[32] The Queen Mary (University of London) has a highly rated LLM in Computer and Communications Law.
http://www.law.qmul.ac.uk/postgraduate/courses/modules/computer-communication/
I could find no mention of accessibility in the online prospectus.
The University of Edinburgh offers several LLM programmes in computer law. For instance, there are modules on the law of robotics and Law, Information and Power, but there was no mention of accessibility in the course introductions.
The University of Strathclyde has been a pioneer in computer law. I could find no mention of accessibility law on the programme website.

[33] One article in the information and communications technology law journal archive. Nothing in the Berkeley Technology Law Journal or Harvard Journal of Law and Technology. The International Review of Law, Computers and Technology was an exception, with an issue focusing on accessibility.
http://www.tandfonline.com/doi/full/10.1080/13600869.2015.1055666

[34] See *https://www.3playmedia.com/2017/08/22/countries-that-have-adopted-wcag-standards-map/*

7.5.1 Limited inclusion

Significant criticism has been levelled at the W3C for its secretive and non-inclusive practices.[35] Easton provides an insightful analysis of the issues with the W3C and limits of self-regulation, noting:

The W3C, with just 2.5% of its membership comprised of user groups and its adherence to the Process Document, has failed to engage with the realities of the disabled experience in the creation of these standards which at present are the nearest approximation to a legally-enforceable measure in the area of Internet accessibility.[36]

This is at odds with the social model of disability and seems more like the medical model of old. If people with disabilities are not involved in the standards creation, then they are disenfranchised and alienated. Easton argues:

> *If disabled Internet users are not involved in the creation of the standards by which barriers to access are assessed, the disenfranchisement that the concept of equal citizenship seeks to eradicate is perpetuated.*[37]

Similar concerns were raised by Adam[38] and Boscarol,[39] who argues robustly that not enough true user research had been done before the standards were created.

[35] JT Richards and VL Hanson, 'Web Accessibility: A Broader View', *WWW* (ACM 2004).

[36] Catherine Easton, 'The Web Content Accessibility Guidelines 2.0: An Analysis of Industry Self-Regulation' (2011) 19 International Journal of Law and Information Technology 74.

[37] ibid 87.

[38] Adam and Kreps.

[39] Maurizio Boscarol, 'A List Apart: ALA : For People Who Make Websites.' (*Accessibility*, 2006) <https://alistapart.com/article/workingwithothers> accessed 9 April 2018.

7.5.2 Code: What are the issues with the standards, tests and tools?

Passing the test does not mean accessiblity. There is a generic issue with all tests. Passing the test can become more important than what the test is attempting to measure. It has been noted by several studies[40] that software developers tend to see passing the technical test as being equivalent to building a solution that is accessible. It was also observed that some designers only pay attention to the letter of the guidelines and regulations, but without understanding the real importance.[41] Passing the test becomes fetishized. The tools, although useful, do not fully measure compliance with the standard and the standard itself does not completely assess accessibility. But various laws and the courts require a measurement standard; without evaluations of web sites to see whether they pass certain tests and checks and comply with the guidelines, these laws cannot be enforced.[42]

Thatcher notes any accessibility testing must be viewed as a process that combines automated software tools with human judgement. He comments that there is no tool that you can run against your website (or web page, for that matter) in order to assert that it is accessible and/or complies with the Section 508 provisions or the WCAG – no matter how much you are willing to pay. It is clear that software tools help, but they are not sufficient. Thatcher splits testing into the algorithmic part and the judgement

[40] Easton, 'The Web Content Accessibility Guidelines 2.0: An Analysis of Industry Self-Regulation' 88.

[41] Hironobu Takagi and others, 'Accessibility Designer: Visualizing Usability for the Blind', *Proceedings of the 6th international ACM SIGACCESS Conference on Computers and Accessibility* (ACM 2004); Chieko Asakawa, 'What's the Web like If You Can't See It?', *Proceedings of the 2005 International Cross-Disciplinary Workshop on Web Accessibility (W4A)* (ACM 2005); DRC, 'Web Access and Inclusion for Disabled People' (2004); NL Bayer and L Pappas, 'Accessibility Testing: Case History of Blind Testers of Enterprise Software.' (2006) 53 Technical Communication 32; Markel Vigo and others, 'User-Tailored Web Accessibility Evaluations', *Proceedings of the eighteenth conference on Hypertext and Hypermedia* (ACM 2007).

[42] Asakawa.

part, noting that virtually no component of an assessment can be done without using judgement. [43] While tools have improved, they are not the complete answer.[44]

Vigo et al evaluated 6 leading automated tools and found at best the tools can only assess 50% of the WCAG 2.0 criteria, and typically identify less than 50% of the errors within that subset.[45] They argue that real harm can be done by just relying on the tools.

Also, there is the challenge for buyers of software in actually assessing if the products they are buying are accessible. Performing a user test in the sales cycle may be appropriate for very large purchases, but, even then, it cannot test for multiple forms of disability, nor can it test the complete product. In order to show compliance, vendors publish VPATs, which are typically the vendor's self-assessment of the product's conformance to an accessibility standard. VPATs were initially produced for Section 508 compliance assessments, but the more recent VPAT 2.0 standard covers the revised Section 508 standards, WCAG 2.0 and also EN 301 549.

Whetstone[46] noted that "A complete and accurate VPAT shows the vendor's commitment to providing a quality experience for all users by documenting and addressing accessibility issues."

However, there are several problems with VPATs and their use to date. Law et al noted, "Many people interviewed in our study said that VPATs were often "a joke" or "a work of fiction," especially when they had

[43] Maria Kapsi and others, 'The Usability of Web Accessibility Guidelines: An Approach for Evaluation' in Constantine Stephanidis (ed), *Universal Access in Human-Computer Interaction. Applications and Services*, vol 5616 (Springer Berlin / Heidelberg 2009).

[44] ibid.

[45] Vigo, Brown and Conway.

[46] Kimarie W Whetstone, 'Upholding Accessibility Standards When Selecting Tech Tools.', *Association Supporting Computer Users in Education* (ASCUE 2017).

obviously been massaged by the vendors' marketing departments."[47] Many vendors do not publish the VPATs, they are not kept up to date, they are too high level and, rather than clearly describing accessibility deficiencies, they seek to limit liability. DeLancey[48] noted in a study of 19 vendors that most overstate their capabilities in the VPATs. "100 percent of sites had at least minor issues with their forms that could result in usability problems for Assistive Technologies, but 75 percent of vendors stated their forms were fully compliant."

VPATs, when published, are a source of competitive information so many vendors keep descriptions vague, defeating the purpose of the VPAT.

7.5.3 Code: Limited methods. Quality on the edge?

Software quality is a fertile field of academic and software industry endeavour. The complexity of modern software systems and our increasing dependence on these systems means that software quality research is funded and extensive. The market for testing tools for application or database performance, for instance, is significant and software development methodologies continue to improve. While the search was not exhaustive, the author was unable to find much mention of accessibility compliance in a scan of quality engineering text books.[49] A search for accessibility, Section 508 or WCAG in the broader software quality journals brings up very few results. Accessibility researchers have examined how accessibility testing is done and they note several concerns.

[47] Chris M Law and others, 'Unresolved Problems in Accessibility and Universal Design Guidelines' (2007) 15 Ergonomics in Design The Quarterly of Human Factors Applications 7, 9.

[48] Laura DeLancey, 'Assessing the Accuracy of Vendor-Supplied Accessibility Documentation' (2015) 33 Library Hi Tech 103.

[49] For instance Sommerville.

- Accessibility testing is usually only done at the end of the development cycle. It is seen as a repair exercise, not a design one.[50]
- Software testing has become more professional, with several institutes providing methods and certification, for instance, The International Software Testing Qualification Board (ISTQB) is such an institution. However, Sanchez-Gordon[51] noted that an accessibility test is only mentioned in the ISTQB glossary and it does not explain how to integrate accessibility testing.
- While the last decade has seen new and improved accessibility testing tools come to market, accessibility tools still largely focus on identifying errors in post-build situations. See section above.

7.5.4 Code: Assistive technologies

Gunderson and others argue that to really address accessibility issues, we need to design inclusive and adaptive technologies.[52]Many people with disabilities experience difficulties with mainstream technologies, as evidenced by the website examples above. Assistive technologies (AT), such as Braille or screen magnifiers, are designed for people with disabilities exclusively. Law argues that historically the design philosophy of product manufacture specifically for people with disabilities has lent itself more to the medical model of disability (i.e. the problem lies with the individual). While assistive technologies have helped many people with disabilities, they have significant disadvantages in terms of cost and "otherness". If the answer to accessibility is always AT, then people with disabilities will

[50] Jon Gunderson, 'Functional Accessibility Testing Using Best Practices', *Proceedings of the 5th International Conference on Universal Access in Human-Computer Interaction. Addressing Diversity. Part I: Held as Part of HCI International 2009* (Springer-Verlag 2009) 504.

[51] Mary-Luz Sánchez-Gordón and Lourdes Moreno, 'Toward an Integration of Web Accessibility into Testing Processes' (2014) 27 Procedia Computer Science 281.

[52] Gunderson.

remain trapped in a world of “special” tools.[53] Support for assistive technologies is not always seamless, as the example below illustrates.

Twitter 140 to 280

While not an enterprise software example, it is nevertheless illustrative. Recently (in November 2017), a leading social media platform, Twitter, introduced a longer character limit. This has had considerable media coverage, and is a significant strategic shift for Twitter. Prior to doing a general release, twitter selected accounts at random to test out the new capability with a subset of users. One of these users happened to be Kit Englard, a deafblind woman, with vision that sometimes enables her to read print. Englard noted that Twitter has had relatively good accessibility, significantly better than Facebook. The Twitter IOS is compatible with screen readers[54], supporting a braille display. Englard typically uses both the standard vision mode, and the optimized for screen reader mode. She noticed that the new 240-character mode did not work with the screen reader mode. She assumed that it was an issue that would be solved with the broader roll out. The error was not caught in testing for the standard release. However, a fix has been promised for the next release, date unknown. This incident highlights the lack of consistent accessibility testing at Twitter and as she notes:

> *This is symptomatic of a systemic issue tech companies fall prey to. This oversight implies that Twitter values the content from blind users less highly than those of sighted users. It also makes it obvious that accessibility is, once again, an afterthought. Though I commend the company on taking the problem seriously and ensuring that these problems will be*

[53] Law and others.

[54] See *https://support.twitter.com/articles/20174660#VoiceOver* for details. The accessibility guidance on the twitter website is not particularly easy to find.

> *fixed in future updates, accessibility is notoriously under-tested during development.* [55]

She also argues that many technology companies overstate their commitment to accessibility and "universal access" and she stresses the utility and significance of tools like Twitter for professionals with disability. The Twitter example above is not unusual. The NFB reported major issues with a recent version of Firefox (57):[56]

> *If you are a screen reader user and also a user of the Mozilla Firefox web browser, please pay close attention to the following information. Do not update to the soon-to-be-released Firefox 57. This upgrade represents such a significant technical and performance change that it's going to be known as Firefox Quantum. The changes in Firefox Quantum are designed to improve the speed and security of the browser. This, unfortunately, also impacts on the user experience for screen reader users, most screen access software is completely incompatible with Firefox Quantum and those that still function will exhibit a serious deterioration in performance. At this stage, the National Federation of the Blind access technology team, VFO, and NV Access are all recommending that users switch to using Firefox's Extended Support Release (ESR) version in order to have the latest browser security features and to avoid 57 until it is suitable for use with screen readers.*

In other words, users who use a screen reader needed to remain on an older, less performant and more vulnerable release. Because software providers typically do not adequately test for accessibility, the burden of

[55] Full story at: *https://theoutline.com/post/2458/there-are-still-some-people-on-twitter-who-don-t-have-280-characters?zd=1&zi=mferja4m*

[56] *https://nfb.org/firefox-57-and-screen-reader-compatibility*

testing falls on activists and volunteers[57], again an example of a negative externality.

7.6 Summary: It isn't just the code

There are multiple causes of inaccessibility: Confusing law, inconsistently enforced; software purchaser apathy; incomplete, inadequate testing methods; designer and developer ignorance / attitude issues, herewith mapped against the Lessig modalities.

Table 7.2: Accessibility failure summary

Modality	Issue	Examples
Law	Fragmentation Poor guidance Weak enforcement	Public v Private. National public accommodation nexus, etc? No UK or German prosecutions
Market	Lack of procurement pressure	CIO inaction
Norms	Developer attitude Designer attitude Academic silos	Slashdot / or just pass the test Design thinking personas? Law and IT research silos
Code	Tools and methods Standards incomplete Assistive technologies	Testing tool status Lack of PWD participation Browser and technology incompatibility

[57] See for instance *http://blog.freedomscientific.com/2017/10/25/important-information-for-users-of-mozilla-firefox/*

8 Fixing accessibility

8.1 Chapter purpose: Suggestions to improve web accessibility

The previous 3 chapters provided a cursory overview of disability law and concepts, examined the web inaccessibility externality in the context of recruitment, and discussed some of the causes of this externality. This chapter will seek to suggest mechanisms to improve accessibility, in part, using the Lessig modalities.

8.2 What is universal design, and how might it help?

There is a vibrant focus in both built architecture and industrial design on universal or inclusive design. Ron Mace[1] is credited with first using the term universal design in the 1980s, and he defined it as a “Common sense approach to making everything we design and produce usable by everyone to the greatest extent possible”. Roger Coleman introduced the idea of inclusive design[2], arguing that needs and abilities change throughout the life course and that by taking account of this in the design process, products, services and environments can be improved for the majority of

[1] Graham Pullin, *Design Meets Disability* (MIT press 2009) xiii.

[2] Roger Coleman and others, ‘From Margins to Mainstream’, *Inclusive Design* (Springer London 2003).

customers in ways that are not associated with negative perceptions of age or disability.[3]

At the risk of treading on semantic toes, this work uses the terms inclusive design and universal design somewhat interchangeably. These are the principles of universal design, as defined by Mace.

- Equitable Use: The design is useful and marketable to people with diverse abilities.
- Flexibility in Use: The design accommodates a wide range of individual preferences and abilities.
- Simple and Intuitive Use: Use of the design is easy to understand, regardless of the user's experience, knowledge, language skills, or current concentration level.
- Perceptible Information: The design communicates necessary information effectively to the user, regardless of ambient conditions or the user's sensory abilities.
- Tolerance for Error: The design minimizes hazards and the adverse consequences of accidental or unintended actions.
- Low Physical Effort: The design can be used efficiently and comfortably and with a minimum of fatigue.
- Size and Space for Approach and Use Appropriate Size and Space is provided for approach, reach, manipulation, and use regardless of user's body size, posture or mobility.

These can be distilled down to:

- Perceptibility is achieved when everyone can perceive the design, regardless of sensory abilities.

[3] Ann Heylighen, Valerie Van der Linden and Iris Van Steenwinkel, 'Ten Questions Concerning Inclusive Design of the Built Environment' (2017) 114 Building and Environment 507, 504.

- Operability is achieved when everyone can use the design, regardless of physical abilities.
- Simplicity is achieved when everyone can easily understand and use the design, regardless of experience, literacy or concentration level.
- Forgiveness is achieved when designs minimize the occurrence and consequences of errors.[4]

Goldsmith, who was a leading architecture academic in the UK, also played a major role in shifting design practice in architecture to be more inclusive. His textbook, *Designing for the Disabled, a New Paradigm*, helped change architecture direction in the UK.[5] He was one of the first architects to actually spend time researching and working with people with disabilities, and it was his work that led to the widespread introduction of the dropped kerb, beloved by wheelchair users and pram pushers everywhere. Goldsmith had a major influence on standards, legislation and designing inclusively. Goldsmith is fulsome of his praise for Nugent, and his work on standards and independent living.[6]

Universal design aims to build solutions that reduce or remove the need for assistance devices. In the best examples, universal design features go unnoticed because they have been fully integrated into thoughtful design solutions that are used by a full spectrum of the population.[7] Objects and environments should be designed to be usable, without modification, by as many people as possible.[8] The argument for inclusive / universal design is

[4] Lidwell, Kritina Holden and Jill Butler, *Universal Principles of Design: 100 Ways to Enhance Usability, Influence Perception, Increase Appeal, Make Better Design Decisions, and Teach through Design* (Rockport Publishers 2003).

[5] Sheelagh Richards, 'Selwyn Goldsmith: 1932 to 2011' (2011) 74 British Journal of Occupational Therapy 359.

[6] Goldsmith, *Designing for the Disabled: The New Paradigm* 8–17.

[7] Molly Follette Story, 'Maximizing Usability: The Principles of Universal Design' (1998) 10 Assistive Technology 4.

[8] Lidwell, Holden and Butler.

compelling and grounded in a human rights approach, as Bianchin and Heylighen show:

> **1.** *there is such considerable diversity in mental and physical capability both across the population and over the length of the life-course that the association of 'normality' with 'able-bodiedness' is neither accurate nor acceptable;*
>
> **2.** *disability arises from interactions with the surrounding environment that are amenable to design and structural interventions, and not inherently from capability levels, health status, or associated degrees of impairment.*[9]

The need for universal design training in the built environment is well understood by regulators. For instance in 2001, The Council of Europe passed a resolution on the introduction of the principle of universal design into the curricula of all occupations working on the built environment.[10] The resolution places significant responsibility and obligation on those educating those working in the building industry.

For instance:

> *Education and training of all occupations working on the built environment should be inspired by the principles of universal design.*
>
> *For the purpose of taking early action to promote a coherent policy to improve accessibility, the concept of universal design should be an integral and compulsory part of the mainstream initial training of all occupations working on the built environment, at all levels and in all sectors.*

[9] Heylighen, Van der Linden and Van Steenwinkel 510.

[10] Council of Europe resolution 15.2.2001 on the introduction of the principle of universal design into the curricula of all occupations working on the built environment via http://www.designforall.it/wp-content/uploads/resap-2001.pdf

and

> *Moreover, they should take steps to ensure that continuing education based on the universal design concept be organised, encouraged and followed by architects, engineers, designers, and town planners.*

The building industry and its regulations are considerably more advanced than the software industry in its approach to educating its designers, architects and planners.

The resolution's general principle states

> *The right of all individuals, including persons with disabilities, to full participation in the life of the community involves the right to access to and use and understanding of the built environment.*
>
> *It is the responsibility and duty of society, and in particular of all occupations working on the built environment, to make it universally accessible to everyone, including persons with disabilities.*

In 2007, a further resolution was adopted, The Resolution "Achieving full participation through Universal Design"[11] stating,

> *Consequently, Universal Design is a concept that extends beyond the issues of mere accessibility of buildings for people with disabilities and should become an integrated part of policies and planning in all aspects of society.*

[11] ResAP(2007)3

and further

> *Member states should take actions incorporating the principles of Universal Design, encompassing all aspects of society, for example the built environment, information and communications technology (ICT) networks, transport, services, tourism, products and goods, information, employment and education.*

This resolution has not made its way into mainstream software design and development practice or awareness. Building architects are more aware of their responsibilities to society and as Ergenoglu notes: "The social responsibility of the architect is an important tool to enhance accessibility awareness in the society."[12]

Universal and inclusive design is also well established in industrial product design. The famous furniture designers, Ray and Charles Eames, worked first for the US Navy designing leg splints. This led them to develop new plywood shaping technology. Later, these techniques were used to make the Eames chairs, manufactured by Herman Miller. (This is an example of a positive externality.) Pullin[13] calls this "where disability inspires design: when the issues around disability catalyze new design thinking and influence a broader design culture in return." He also notes the history of the spectacles. In the 1930s, the NHS in the UK classified spectacles as medical appliances, and wearing them was considered socially humiliating. Today, up to 20% of some brands of spectacles are bought with clear non-prescription lenses. Glasses are a strong metaphor for the shift from medical to social, indeed from medical necessity into fashion accessory. Pullin argues strongly for involved fashion designers in other wearable medical products. The evolution of the wheelchair has parallels for inclusive software design. The wheelchair has, in the main,

[12] Asli Sungur Ergenoglu, 'Universal Design Teaching in Architectural Education' (2015) 174 Procedia - Social and Behavioral Sciences 1397, 1397.

[13] Pullin.

remained a medical appliance, although this is beginning to shift, with leading wheelchair companies now marketing specialized chairs, for instance for sport. The ageing of the baby boomer generation will lead to more demand for differentiated wheelchair products.[14] There is growing synergy between advanced bicycle manufacture and modern wheelchair design. Increasingly, users of bionic limbs, rather than hiding them or having them in flesh-like colours, are customizing and accessorizing them with bold designs.[15] The shift from merely patient to empowered consumer is under way.

The software industry lags behind both industrial design and building architecture. It neither follows accessibility standards rigorously, nor does it follow an inclusive product innovation process. The shift from the medical mindset to the human rights mindset is not merely a matter for legislation. In the case of building architecture, and some elements of industrial design, it is the attitudinal shift of the designers that has been equally important. Universal design is a useful umbrella concept, and it could be applied to software design too. The next section will explore that potential.

8.3 Making design thinking inclusive

The design thinking method (and software design generally) is strongly defined and set by people without disabilities. Making it more inclusive would require involving people with disabilities in the design process. There are two ways this should occur:

[14] L Zimmermann, M Hillman and P John Clarkson, 'Wheelchairs: From Engineering to Inclusive Design', *Include 2005* (2005).

[15] See for instance *http://www.thealternativelimbproject.com* and *https://www.augmentedfuture.com/us/*

1. Involve a more diverse pool of design participants and subjects, and include more diversity relevant concepts into the design and articulation of personas, artefacts, etc. For an example of a more inclusive persona set, see Horton.[16] The current definition of inclusive design in software is rather restrictive.
2. More fundamentally, involve people with disabilities as designers and developers. To do so would require adaptation of the design tools and methods, as most of these are inaccessible, for instance for those with visual impairments. It would also require a more focused hiring effort from software firms.

To develop truly inclusive software, rote compliance with standards will not be enough. This need for a holistic design has been firmly articulated by Thatcher[17], Sloan and Kelly[18] and others.[19]As with building architecture, software development will only become truly inclusive for end users if it becomes inclusive in its design and development methodologies. While consistently designing for people with disabilities would be a significant step forward from where the vast majority of software development is today, designing with people with disabilities is really what is required if software is to become accessible.

[16] Sarah Horton and Whitney Quesenbery, *A Web for Everyone: Designing Accessible User Experiences* (Rosenfeld Media 2014).

[17] Jim Thatcher, Andrew Kirkpatrick and Christian Heilmann, *Web Accessibility: Web Standards and Regulatory Compliance* (friends of ED 2006).

[18] David Sloan and others, 'Contextual Web Accessibility - Maximizing the Benefit of Accessibility Guidelines', *Proceedings of the 2006 international cross-disciplinary workshop on Web accessibility (W4A) Building the mobile web: rediscovering accessibility? – W4A* (ACM Press 2006); David Sloan and Brian Kelly, 'Reflections on the Development of a Holistic Approach to Web Accessibility', *ADDW08 Conference* (University of Bath 2008).

[19] Gabriele Meiselwitz and Brian Wentz, *Universal Usability : Past , Present , and Future*, vol 3 (Now Publishers, Inc 2010); Debra A. Riley-Huff, 'Web Accessibility and Universal Design.' (2012) 48 Library Technology Reports 29; Demosthenes Akoumianakis, 'Managing Universal Accessibility Requirements in Software-Intensive Projects' (2009) 14 Software Process Improvement and Practice 3.

Developers: Mealin et al[20] outline the challenges blind developers face in using developer tools. They note software languages themselves have differing accessibility characteristics, for instance in syntax, which influence the ease or difficulty for blind developers, and note that Python is popular with blind developers. Albusays and Ludi[21] also highlighted the problems blind developers face (limited accessible aids for IDEs, code navigation, diagrams, debugging, and seeking sighted assistance). Petrausch et al[22] reviewed the accessibility of the Eclipse IDE, and created guidelines for visually impaired developers. Welcome developments include code navigation plug-ins for Eclipse[23]. Creating methods for blind developers and designers to read UML diagrams[24] is important, especially given the growth of model-driven engineering.[25]

Designers: In terms of the visually impaired, Sahib et al[26] explain that the tools designers use to show early prototypes and ideas are themselves not accessible. Early designs do not lend themselves to screen reader access. They make two suggestions to help improve design for blind users. Firstly,

[20] Sean Mealin and Emerson Murphy-Hill, ‘An Exploratory Study of Blind Software Developers’, *Proceedings of IEEE Symposium on Visual Languages and Human-Centric Computing, VL/HCC* (IEEE 2012).

[21] Khaled Albusays and Stephanie Ludi, ‘Eliciting Programming Challenges Faced by Developers with Visual Impairments’, *Proceedings of the 9th International Workshop on Cooperative and Human Aspects of Software Engineering - CHASE ’16* (ACM Press 2016).

[22] Vanessa Petrausch and Claudia Loitsch, ‘Accessibility Analysis of the Eclipse IDE for Users with Visual Impairment’, *Studies in Health Technology and Informatics* (2017).

[23] Catherine M Baker, Lauren R Milne and Richard E Ladner, ‘StructJumper: A Tool to Help Blind Programmers Navigate and Understand the Structure of Code’ (2015) 1 Proceedings of the ACM CHI ’15 Conference on Human Factors in Computing Systems 3043.

[24] Vanessa Petrausch, Stephan Seifermann and Karin Müller, ‘Guidelines for Accessible Textual UML Modeling Notations’ (Springer, Cham 2016).

[25] Filipe Del Nero Grillo, Renata Pontin de Mattos Fortes and Daniel Lucrédio, ‘Towards Collaboration between Sighted and Visually Impaired Developers in the Context of Model-Driven Engineering’, *First Workshop on Graphical Modeling Language Development* (2012).

[26] Nuzhah Gooda Sahib and others *Participatory Design with Blind Users: A Scenario-Based Approach.*

involve a blind user in the design team, ideally someone with significant experience in assistive technology and application usage. Secondly, using text-based scenario dialogues to interact with blind users will enable designers to get useful feedback, given that the typical design tools and process focus on the visual design, which makes communication difficult.

> *Similarly, within human-computer interaction, in order to be useful, the way in which interactions are articulated need to take into account the senses and tools at the disposal of the user, as well as the level of granularity at which they interact with the system.*[27]

Advances in Braille technology can potentially enable new forms of prototyping, even at the early, low resolution stage of design:[28] for instance, 3D printed overlay touchplates,[29] physical guides that provide tactile feedback for touch screens in that they are overlaid on the screen and recognized by the underlying application. Eisma et al make the case for the early involvement of impaired users in product design[30] and others suggest guidelines for participatory design for persons with dementia and

[27] ibid 698.

[28] Mei Miao and others, 'Tactile Paper Prototyping with Blind Subjects', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Springer, Berlin, Heidelberg 2009).

[29] Shaun K Kane, Meredith Ringel Morris and Jacob O Wobbrock, 'Touchplates: Low-Cost Tactile Overlays for Visually Impaired Touch Screen Users', *Proceedings of the 15th International ACM SIGACCESS Conference on Computers and Accessibility* (2013).

[30] R Eisma and others, 'Early User Involvement in the Development of Information Technology-Related Products for Older People' (2004) 3 Universal Access in the Information Society 131.

the elderly.[31] Research then has started to provide the techniques for a more inclusive approach to design, but they have not become mainstream.

Product Managers: The role of product managers in software development is not well covered by academic study.[32] However, they play a key role in deciding what is built, and are often responsible for making the feature and resource trade-offs. Insisting on accessibility as ship / no ship criterion would be a significant step forward. Software is sometimes shipped without being accessible in its early release, with a plan to catch it up later. Larger software companies are becoming more disciplined in enforcing build standards,[33] but this clashes with the start-up culture model of ship it, then fix it.[34] (This was echoed in the survey results). Product managers can also position accessibility as part of their product and brand marketing, for instance see Microsoft, discussed below.

Automating: Fixing the alt-text problem with artificial intelligence?

While earlier studies[35] have found Facebook to have significant accessibility problems itself, researchers at Facebook have suggested a solution that would help remedy the alt-text problem, at least in the context of images. Wu et al[36] designed a system that applies computer vision technology to

[31] Niels Hendriks, Frederik Truyen and Erik Duval, 'Designing with Dementia: Guidelines for Participatory Design Together with Persons with Dementia', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Springer, Berlin, Heidelberg 2013); Karine Lan Hing Ting and Myriam Lewkowicz, 'From Prototype Testing to Field Trials: The Implication of Senior Users in the Evaluation of a Social Application' (2015) 67 Procedia Computer Science 273.

[32] See also conclusion and GDPR chapter for further discussion.

[33] Again, Microsoft publishes its internal build standards. *https://msdn.microsoft.com/en-us/library/windows/desktop/bb231566(v=vs.85).aspx*

[34] See for example *https://twitter.com/reidhoffman/status/847142924240379904?lang=en*

[35] Maria Claudia Buzzi and others, 'Is Facebook Really "open" to All?', *2010 IEEE International Symposium on Technology and Society* (IEEE 2010).

[36] Shaomei Wu and others, 'Automatic Alt-text: Computer-Generated Image Descriptions for Blind Users on a Social Network Service'.

identify faces, objects, and themes from photos to generate photo alt-text for screen reader users on Facebook.

There are many examples of promising accessibility research.[37] One of the major challenges though is not innovative ideas, but how to "mainstream" those prototypes and edge solutions into mainstream usage. This will require collaborative action between users, research labs, industry, and also government.

8.3.1 Accessibility by design and default

Enterprise and commercial software developing tools may have accessibility enhancing capabilities, but typically these features are buried in obscure menu items. We have seen how code can nudge behaviour. For instance, if, on saving, a blog tool was to comment, "I've noticed the photo you have posted doesn't have a caption, would you like to add one, as it will mean that people with disabilities will be able to enjoy your blog?" that would likely lead to a higher level of accessible blogs. Similarly, development IDEs could be more assertive in driving accessible first development. A positive example is the new accessibility checker in Microsoft Word. When Microsoft placed it more prominently on the toolbar ribbon, usage increased dramatically.[38]

[37] Alexy Bhowmick and Shyamanta M Hazarika, 'An Insight into Assistive Technology for the Visually Impaired and Blind People: State-of-the-Art and Future Trends' 149. This paper summarizes decades of AT research.

[38] *https://twitter.com/MSFTEnable/status/982288582294433792* and *https://blogs.msdn.microsoft.com/accessibility/2018/03/19/microsoft-accessibility-journey-march-2018/*

8.3.2 Educating designers, product managers and developers

The developer survey noted the lack of formal training for developers in accessibility. Shinohara[39] et al confirm this in a broader study, and provide suggestions on how to develop a broader teaching cadre for accessibility. Exposing software developers and designers to their legal and ethical obligations to people with disabilities during their education is essential. Inaccessible code creates an externality, and the sooner that software developers and designers become aware of that responsibility, the better. Accessibility training should be made part of the compulsory computer science curriculum. It should not just cover the technical standards, but it should embed awareness and be competent in universal design. Ludi notes the impact of involving people with disabilities directly in the classroom.[40] Youngblood makes a similar point with training novice developers.[41] There is also a need for more specialist programmes to develop more accessibility experts.[42]

Anne Tynan noted in the interview "I would have thought that it would be increasingly important for software developers and others in IT and those people to understand the legal context of what they do."[43]

[39] Kristen Shinohara and others, 'Who Teaches Accessibility?', *Proceedings of the 49th ACM Technical Symposium on Computer Science Education – SIGCSE '18* (ACM Press 2018).

[40] Stephanie Ludi and others, 'Teaching Inclusive Thinking to Undergraduate Students in Computing Programs', *Proceedings of the 49th ACM Technical Symposium on Computer Science Education - SIGCSE '18* (ACM Press 2018).

[41] Susan A Youngblood, 'Communicating Web Accessibility to the Novice Developer: From User Experience to Application' (2013) 27 Journal of Business and Technical Communication 209.

[42] Paul Ryan Bohman, 'Teaching Accessibility and Design-for-All in the Information and Communication Technology Curriculum: Three Case Studies of Universities in the United States, England, and Austria' (2012). This dissertation provides a detailed analysis of various university accessibility teaching programmes.

[43] See Appendix A.

Collaboration between software faculties, built architecture faculties and medical faculties should be encouraged[44] And, while Rudolph notes that there is significant room for improvement in architect accessibility education in Germany,[45] this author argues that software is far worse.

8.3.3 Continuing education and development

While tertiary education is key, ongoing education and awareness is important too. While some software companies have ongoing accessibility education, this is not widespread, as the survey illustrated. Bieber et al[46] propose a Europe-wide accessibility professional certification as part of the European Skills ECQA, the European Certification and Qualification Association. The development of a detailed, standard curriculum and relevant training is to be welcomed, but driving adoption will be the next challenge. A positive, practical example, Atos in the UK launched an apprentice scheme to train and develop accessibility experts. It is an 18-month programme, covering programming, universal design, AT and standards such as WCAG, ISO 9241-171 and ISO 13066-1.[47]

8.3.4 Learning from best practice examples

It has been stressed that accessibility is not just about standards. There are organizations that are doing excellent accessibility developments.

[44] Valerie Watchorn and others, ‘Strategies and Effectiveness of Teaching Universal Design in a Cross-Faculty Setting’ (2013) 18 Teaching in Higher Education 477. This paper explores collaboration between medical and architecture schools; the author argues a similar approach is needed for software.

[45] Albusays and Ludi.

[46] Ronald Bieber, Klaus Höckner and Gabriele Sauberer, ‘Accessible Information and Accessibility through ICT: A Mega Trend Creates the Need for Quality Certificates for Web Accessibility Professionals in Europe and Beyond’, *Communications in Computer and Information Science* (Springer, Cham 2017).

[47] Details at: *https://atos.net/en/blog/accessibility-inclusion-future-hands*

Barclays Bank in the UK has been vocal in its support for greater accessibility and inclusion, recently making significant investment in physical branch accessibility, ATM accessibility, web and mobile accessibility. Barclays has also been active in accessibility awareness and sponsoring. The bank has an impressive inclusive design focus and has developed diverse persona for its application design. Its public commitment and focus on accessibility is prominent on its website, including a commitment to train its software developers in inclusive design.[48]

In 2014, Barclays Bank in the UK launched a new mobile personal banking application. The designers and product team worked with Persons with Disabilities early in the design process. They also partnered with AbilityNet, a UK charity with accessibility expertise. The lead product manager noted[49]

> *At one time we may have seen accessibility as something bolted on the end of a project but we're now seeing how much more we can achieve when we bring into the heart of the design process. In this project it started with testing at early design phase - in fact we tested the wireframes.*
>
> *"The disabled user testing at that point provided real insight into some of the usability issues which were relevant to every user - and I think the team saw then just how valuable this process would be."*

The application passed the WCAG AA tests, but this was not the primary design target. The project followed an agile methodology, but with accessibility testing in every build, rather than just at the end. This example shows it is possible to build mobile applications that are compelling and

[48] *https://www.barclayscorporate.com/insight-and-research/managing-your-business/making-your-business-accessible/inclusive-design.html*

[49] *https://www.abilitynet.org.uk/accessibility/case-study/accrediting-barclays-personal-banking-app*

universal. Barclays has also won awards for inclusive developments such as its pin sentry tool and ATM accessibility.

Over the past 5 years or so, Microsoft has significantly increased its focus on accessibility in its developer tools,[50] end user products and long-term R&D. Microsoft has been active in broader accessibility research. For instance, it has released a solution called Soundscape. This is a collaboration between Microsoft and the UK Guide Dog Association. It combines object recognition, voice technologies and mapping to provide an augmented assistance for blind users. In discussions with accessibility advocate Neil Milliken, he noted that Microsoft has stepped up on accessibility since the new CEO, Satya Nadella, took over. He has been more vocal on accessibility than other CEOs in technology.[51] Microsoft's disability desk[52] indicates a stronger focus on accessibility than other enterprise vendors show. Accessibility capabilities feature more prominently in recent product announcements.[53] As we have seen, there are many examples of accessibility failure. However, there are also pockets of success. These successes require amplification.

8.3.5 Encouraging people with disabilities to work in the software industry

As noted earlier, it has been well documented that the software industry has a diversity problem. This is normally formulated in the context of race, age and gender diversity, but it ought to consider people with disabilities too. The recent focus on neurodiversity is a welcome start, but there is much more that can be done. Given the right tools and environ-

[50] For instance AccScope, which enables early accessibility testing in the dev cycle. *https://msdn.microsoft.com/library/windows/desktop/Dn433239*

[51] See for instance *https://blogs.msdn.microsoft.com/accessibility/2017/09/29/hitting-refresh-on-accessibility/*

[52] See *https://support.microsoft.com/en-us/accessibility/disability-answer-desk*

[53] *http://mashable.com/2017/08/02/microsoft-windows-10-eye-tracking-accessibility/#B.ps03LENqqz*

ments, people with disabilities can be highly effective members of the workforce. For instance, governments could focus more on the software industry and related jobs for its people with disabilities employment efforts. Developers who see accessibility as a compliance burden are likely to shift attitude when they meet colleagues with disabilities.

8.3.6 More assertive action from activists, NGOs and industry champions

As we saw in the accessibility law chapter, a significant driver in accessibility progress in the built environment was the role of activists and committed supporters. NGOs can help to pressure organizations to change behaviour, as shown in the Tesco example in the UK. In Germany, works councils can help drive better accessibility through co-determination. NGOs can help drive the shift in social norms, but their collective role as litigator or negotiator can force recalcitrant employers to be more accessible. This is turn will lead to pressure on software vendors. The NGOs should engage directly with vendors too.

8.3.7 The law

The UNCRPD is a remarkable step forward, but it will require continued diligence and pressure to bring about change at a national level. EU law is gradually become more consistent, and the EU Accessibility Act will increase the legal pressure for private sector improvements. Guidelines from the DOJ would significantly reduce the confusion in the US. The global coalescence on the WCAG standards is to be welcomed. While there are considerable issues with the law, the larger problem is the lack of consistent and assertive enforcement.

8.3.8 Standards

The critique of WCAG 2.0 was noted earlier. At the time of writing, WCAG 2.1 is close to release. It includes new success criteria, as the techniques for displaying and entering information have advanced since WCAG 2.0 was published in 2008. Examples include pointer gestures and hover content. Since their inception, the WCAG standards have moved from being guidelines to being the standard that many laws around the world rely on to measure accessibility compliance. WCAG needs to evolve to cover a broader reach of disability conditions and at the same increase the objective testability of the standard. In order to strengthen its legitimacy, the more inclusive it can become, the better. Future enhancements must include cognitive disabilities, for instance.

The standards will continue to evolve and improve, but the biggest challenge remains designer and developer awareness, and competence in deploying them.

8.4 Summary: Fixing accessibility

Again, the Lessig modalities provide a useful mechanism. Table 8.1 summarizes the accessibility fixes. The most effective and important shift will be to move the mindset of software developers, designers and product managers from the medical to the human rights model. The social norm, rather than the technology itself, is the largest barrier.

Table 8.1: Improving accessibility in enterprise software

Modality	As-is	Required change	Example in practice
Law	Lack of awareness amongst developers and designers	Training methods and training University and ongoing education Collaboration with other design related departments	Game design school in the US Austrian certification
Social norm	Medical model	Shift to human rights Collaboration with other design departments Expose more engineers and designers to PWD Long-term change and education programmes Highlight inclusive technology	Deliberately hire PWD, i.e. SAP Autism initiative PWD meet developers and designers Bionics as fashion
Technology/ architecture	Edge innovations No consistent development or design method	Accessibility by design default Mainstreaming Encourage/fund more universal and AT innovation research Revise Agile and other methodologies Apply and design new technologies with PWD in mind	Barclays example Improved tooling for accessibility in Eclipse and Microsoft tools New test tool entrants Use cases for voice technologies such as Alexa, Cortana, etc. Google maps for wheelchair users Augmented reality for blind navigation Automated voice recognition to create captions Augmented alt text
Market	PWD buying centre not heard	Vendors to demand accessibility from the product supply chain Tighter procurement from public and private sector Market inclusion as a brand value	Browser testing features US public sector / new EU rules Barclays Bank, and increasingly Microsoft

9 Payroll software: Where enterprise software began

9.1 Chapter purpose: Payroll as code is law

The primary goal of this chapter is to examine the research question, "How has the development of payroll software supported compliance and influenced tax and social insurance regulations?"

It will examine the relationship between one of modern society's most significant compliance frameworks, payroll related taxes, and the software code that supports their calculation and collection. It will show how the payroll industry has emerged, and how over time it has developed an effective business and technical model for building solutions to cope with high levels of compliance complexity and change. Payroll is the original code is law in that payroll was the first business application built on a computer. Software code has fundamentally changed how taxation is calculated, collected and complied with.

There is a synergistic relationship between the tax collection authorities and software vendors that has developed over decades. This relationship has received little obvious academic attention, nither in the software engineering community, nor by those researching income tax compliance theory, nor by the growing information technology law field. The history of payroll computerization over the last 70 years is worth briefly exploring, even if merely to highlight the neglected significance of payroll in information technology and taxation theory.

The national differences in payroll practice and regulation are also enlightening. For instance, there are innovative practices in the UK and Germany that could be adopted more broadly, beyond payroll compliance.

The co-operation levels between vendors and governments are not consistent across countries.

The requirements gathering and specification strategies of payroll vendors may serve as a model for other compliance intensive developments. The architecture and approach to software maintenance and quality have significant relevance beyond payroll development, and there is an untapped opportunity to apply these. The experiences of payroll development can teach both software developers and the regulators more about building compliance software than is typically understood.

The chapter also makes the plea for broader multi-disciplinary research into the role of software code in taxation collection effectiveness and ultimately legitimacy.

9.2 Early software industry history, and the role of payroll

Much commercial business software exists to help organizations comply with laws and regulations. Whether it is calculating tax obligations, reporting on financial results, tracking health safety regulations, travel allowances, fraud identification and prevention, customs excise management, banking regulations, affirmative action reporting, absence tracking, software and software vendors play a key role in making compliance work. Software has even enabled new forms of taxation to be developed, for instance sophisticated toll systems, such as the London Congestion Zone.

A vast software and services industry exists to help organizations manage compliance and regulations using software. The market for enterprise software applications is estimated to be 355 billion US$ in 2018,[1] and a

[1] Gartner, ‘Gartner Says Global IT Spending to Reach $3.7 Trillion in 2018’ <https://www.gartner.com/newsroom/id/3845563> accessed 28 February 2018.

significant portion of that relates directly to compliance centric applications such as general ledgers and payroll. This industry has grown dramatically ever since the 1950s and continues to grow dynamically today.

While making and breaking codes drove the first computers and software,[2] the first real commercial usage of a computer was to calculate the payroll and inventory of the Lyons Tea Room company in the UK in the early 1950s.[3] It is worth briefly noting this history, as it sets the foundation for modern compliance enabling computing.[4]

9.2.1 LEO and Lyons Tea Room

The Lyons Tea Room company was one of the UK's most successful businesses in the middle of the 20th century. In the late 1940s, Lyons began to investigate the possibilities of electronic automation to improve business processes. At the time, Lyons was very advanced in terms of management and business process thinking. To quote from the 1947 report:

> *Our first concern is, of course, the advantages that Lyons may gain from the commercial development of electronic machines, but there is a wider aspect which cannot be overlooked. This machine may well be a prime factor in relieving the present economic distress of the country. In this latter respect we cannot help but feel that Lyons occupies a key*

[2] The computer industry developed from the work done to break codes in WWII.

[3] There is a well documented history, with good primary and secondary research. See for example David C Mowery, '50 Years of Business Computing: LEO to Linux' (2003) 12 The Journal of Strategic Information Systems 295; Peter Bird, 'LEO, the Pride of Lyons' (1992) 14 IEEE Annals of the History of Computing 55; David Tresman Caminer, 'LEO and the Computer Revolution' (2002) 13 Computing and Control Engineering Journal 273; Martin Campbell-Kelly, 'Development and Structure of the International Software Industry, 1950-1990' (1995) 24.

[4] However, computer history is not taught to computer science students to any great extent.

> *position; no one else here, as far as we can learn, has realised the far-reaching possibilities of electronic machines.*
>
> *We assume that Lyons will want to take full advantage of these machines for their own offices. It is possible for us to play a passive role by merely keeping in touch with developments, and in due course buying machines as they become available, probably from American sources. But such a role would not enable us to have any influence on the kind of machines built, and without commercial influence they may well be built in a form more suitable to handling mathematical and census calculations owing to the influence of the large governmental concerns.*[5]

In 1949, the Lyons team worked with Wilkes[6] at Cambridge University to fund and develop the EDSAC[7], and then build their own machines[8], called LEO.[9] The machine was operable by 1951. The original systems engineer, David Caminer, noted:

> *It had been intended from the outset that the first full-scale integrated application would be payroll. The payroll system that emerged led the world for many years.*[10]

[5] Nick Pelling, 'The Case For The First Business Computer – Nick Pelling' (2002) <http://www.nickpelling.com/Leo1.html#Part3> accessed 15 September 2017.

[6] M V Wilkes and W Renwick, 'The EDSAC (Electronic Delay Storage Automatic Calculator)' (1950) 4 Mathematical Tables and Other Aids to Computation 61.

[7] Electronic delay storage automatic calculator (EDSAC). This was the second digital computer in the world to go into regular service.

[8] M V Wilkes, 'John Pinkerton and Lyons Electronic Office' (2001) 10 Engineering Science and Education Journal 183.

[9] Lyons Electronic Office.

[10] Caminer, 'LEO and the Computer Revolution'.

> *The business case for the automated payroll showed a reduction in cost from 12.7 pence to 8.07 pence.[11] The payroll processing was very sophisticated:*
>
> *In the calculating phase, everything down to updating the state of the employee's loan account was included. PAYE was deducted with special provision for holidays. If the extent of deductions meant that the take-home pay would have sunk below a set level, then only statutory deductions would be taken. To reduce the time for making up pay packets, net pay was rounded off to half crowns and the positive or negative balances carried forward to next week.[12]*

The payroll went into production for 10,000 Lyons workers in 1953[13], with a remarkable processing time of 1.5 seconds per worker.[14] The previous manual, calculator-based process took roughly 8 minutes per payee; with the computer, it was 31900% faster.

Shortly after that successful payroll deployment, the LEO computer was used for the first computerized payroll outsourcing deal in 1955; Ford UK's payroll was processed by a LEO computer. It paid thousands of

[11] The Pelling website has the complete business case. It makes for fascinating reading. While much will seem quaint, the content will seem very similar to any modern business case. It should be taught as an example of the challenges of internal innovation. *http://www.nickpelling.com/Leo1.html#AppendixC*

[12] ibid.

[13] Georgina Ferry, *A Computer Called Leo* (2nd edn, Harper Perennial 2004) 149.

[14] David Tresman Caminer, 'Behind the Curtain at LEO: A Personal Reminiscence' (2003) 25 Annals of the History of Computing, IEEE 3.

workers at the Dagenham plant by 1956.[15] This marked the start of the UK payroll computer bureau industry. In 1954, Lyons had created LEO Computers Limited as a separate organization, which they later sold off in 1963.[16]

In the 1950s, British computing design was significantly ahead of its US counterparts, but the marketing and sales were amateurish, and government support funding or procurement was not forthcoming. Although the British computer industry faded relatively quickly into insignificance, LEO laid the initial foundation for business computing globally. It was not so much that the British lacked entrepreneurial spirit; they were simply overwhelmed by the vast investment that the US government made into defence computing, and the positive externalities this created in business computing. The US government played the role of a venture capitalist and first customer for the US computer industry, as evidenced by the early history of Engineering Research Associates, Inc. (ERA), Eckert-Mauchly Computer Company and Remington Rand.[17] The US government aggressively invested in computing and computer services, for instance, the SAGE project earned IBM revenues of 500 million US$ in the 1950s.[18] Caminer noted that in Britain, such little help as was given went toward scientific computing. Murray Laver, the senior civil servant responsible for guiding government computerization, commented candidly, “In Britain

[15] Caminer noted: Using LEO, the first stage of business outsourcing occurred with the provision of a service for the payroll of the Ford Motor Company in 1955. LEO analysts produced a job specification that was approved by the local management. The LEO staff then produced the programs, training Ford staff to be able to make changes when these became necessary. After trials, the programs were put into effect. The clock card data were brought by courier across London at a due time and the LEO organization returned the completed pay data in the same way.

[16] This became part of ICL, eventually.

[17] Arthur Lawrence Norberg, *Computers and Commerce: A Study of Technology and Management at Eckert-Mauchly Computer Company, Engineering Research Associates, and Remington Rand, 1946-1957* (MIT Press 2005).

[18] Campbell-Kelly, *From Airline Reservations to Sonic the Hedgehog : A History of the Software Industry* 38.

generally we were slow to realize that the computer market for commercial work would outgrow and greatly exceed the market for science and engineering."[19]

LEO was a squandered first mover opportunity, but many of the ideas and innovations that it started remain fundamental to modern computing and business. The relevance of this work is that it showed the power of computing to transform an essential compliance process, payroll.

9.3 Payroll and taxation. Give unto Caesar: software's role

Taxation lies at the heart of the citizen / state relationship, and as Murphy notes "in a democracy tax can be seen to be one of the cleverest human inventions."[20] Analzsing taxation and its role in society has occupied the minds of swathes of academics across several disciplines since antiquity. It is not within the scope of this work to discuss or analzse the legitimacy or appropriateness of specific forms of taxation or their levels, it is however a rich field of academic and activist discourse, and will remain so as long as taxes are levied and paid.[21]

There are models in economics and law that explore and explain tax compliance, evasion and avoidance, see for instance theoretical tax compliance,[22]and further, as a psychological contract, [23] as neuroeconomics, [24] as

[19] Caminer, 'LEO and the Computer Revolution' 14.

[20] Richard Murphy, *The Joy of Tax* (Random House 2015) 51. Provides an engaging examination of tax history and the role of tax in a democratic society.

[21] Some examples: Joel Slemrod, 'Optimal Taxation and Optimal Tax Systems. Three Cornerstones of the Theory of Optimal Taxation' (1990) 4 Journal of Economic Perspectives 157; Monica Bhandari, *Philosophical Foundations of Tax Law* (2017); ERA Seligman, *The Income Tax: A Study of the History, Theory, and Practice of Income Taxation at Home and Abroad* (The Lawbook Exchange Ltd 1914).

[22] Michael G Allingham and Agnar Sandmo, 'Income Tax Evasion: A Theoretical Analysis' (1972) 1 Journal of Public Economics 323.

behavioural dynamics,[25] as a social norm,[26] on penalty structures,[27] or using prospect theory.[28] Other researchers explore the differences between developed and developing countries taxation compliance. Tax compliance costs are also extensively researched.[29]

Recent research into the efficiency of tax collection mechanisms notes that, in all advanced economies, most taxes are collected through third-party institutions such as employers, banks, investment funds and pension funds.[30] The literature also notes that these third party collection / reporting methods are generally effective: For instance, in the US a 2012 tax compliance study by the Internal Revenue Service shows that the evasion rate for personal income is 56% when there is 'little or no' information

[23] Lars P Feld and Bruno S Frey, 'Tax Compliance as the Result of a Psychological Tax Contract: The Role of Incentives and Responsive Regulation' (2007) 29 Law and Policy 102.

[24] B Larissa-Margareta and N Ramona-Anca, 'A Neuroeconomic Approach of Tax Behavior.' (2012) 1 Annals of Faculty of Economics 649. This is a fascinating field of research in that it challenges the traditional neo-classical economic "rational man" assumption. See also the work of the Nobel prize winner, Kahneman.

[25] Michael Pickhardt and Aloys Prinz, 'Behavioral Dynamics of Tax Evasion – A Survey' 1.

[26] Eric A Posner, 'Law and Social Norms: The Case of Tax Compliance' (2000) 86 Virginia Law Review 1781; Diana Onu and Lynne Oats, '"Paying Tax Is Part of Life": Social Norms and Social Influence in Tax Communications' (2016) 124 Journal of Economic Behavior and Organization 29.

[27] Rainald Borck, 'Income Tax Evasion and the Penalty Structure' (2004) 8 Economics Bulletin.

[28] Ping Chen, Xian Deng and Fang Liu, 'A New Explanation of Tax Evasion Behavior Based on Prospect Theory' [2007] Proceedings of 2007 International Conference on Public Administration (3rd), Vol II 944.

[29] Michael Godwin, 'Compliance Costs – The Cost of Paying Tax' (1978) 6 Omega 389; Cedric T Sandford, 'International Comparisons of Administrative and Compliance Costs of Taxation' (1994) 11 Australian Tax Forum; Laurence Mathieu and others, 'The Distribution of UK Personal Income Tax Compliance Costs' (2010) 42 Applied Economics 351; Francis Chittenden, Saleema Kauser and Panikkos Poutziouris, 'PAYE-NIC Compliance Costs: Empirical Evidence from the UK SME Economy' 635.

[30] Henrik Jacobsen Kleven, Claus Thustrup Kreiner and Emmanuel Saez, 'Why Can Modern Governments Tax So Much? An Agency Model of Firms as Fiscal Intermediaries' (2016) 83 Economica 219.

reporting, while it is less than 5% when there is substantial information reporting.[31] Kumler et al examined how a change in social insurance reporting rules in Mexico reduced under-reporting of income tax.[32] For the purposes of this work, this highlights two important findings: Namely, governments largely rely on third parties to collect income tax, and the reporting process is a key driver in reducing evasion.

In turn, those third parties largely rely on software developers and software vendors to provide the tools to do the collection. The software, rather than the third party itself, determines the parameters of the collection. The tax code is codified into the software. It is the software developer and the software companies that employ them that enable modern tax collection.

Information technology and code play a critical role in the practicality and effectiveness of taxation collection. In the case of some taxation methods, such as the London congestion toll (and other models in cities such as Hong Kong), the role of technology is obvious. Without the cameras, number plate recognition software and invoicing technology, the scheme would have been impossible. Congestion charging and tolling is both an attempt to address the externality of the overcrowding of roads, and a fundraising mechanism for cities or the state, looking either to finance the road network or for other purposes.[33] The technology developer plays a critical role in determining how and what taxes can be collected. In essence, software code enables the tax code.

Enhancements in technology lead directly to new forms of taxation. When examining the economic and political literature, the role of code in setting and shifting the boundaries of what is feasible as a tax collection

[31] ibid.

[32] Todd Kumler and others, 'Enlisting Employees in Improving Payroll-Tax Compliance: Evidence from Mexico' (2013).

[33] Santos and others; Georgina Santos, 'Road Fuel Taxes in Europe: Do They Internalize Road Transport Externalities?' (2017) 53 Transport Policy 120.

technique has not received adequate academic attention. Today, it is software code that plays the role of the Sherriff of Nottingham.[34] While there has been work that looks at the productivity of tax collection authorities, for instance,[35] and the impact of ICT on tax collection in developing economies is receiving some attention, the literature search for this work did not find any legal or economic research that looked at the specific role of payroll software in enabling the income tax collection process, with the exception of a recent paper exploring the related topic of time and attendance software.[36] Modern income tax collection is inconceivable without payroll software. So, its relative neglect as a topic of academic study is puzzling.

This brings us back to Lessig's 4th modality of regulation, that of architecture. Code alters the properties of what is feasible in terms of tax collection technique. The close collaboration between software vendor and government makes possible new forms of taxation, and dramatically lowers the cost of collection. It is worthwhile exploring the relationship between PAYE / tax withholding and payroll software, as it highlights the dependence of government on payroll software as a collection mechanism.

[34] For those not familiar with the story of Robin Hood, the Sheriff of Nottingham was the tax collector.

[35] Leandro Carrera, Patrick Dunleavy and Simon Bastow, 'Understanding Productivity Trends in UK Tax Collection 1 LSE Public Policy Group Working Paper July 2009' 1.

[36] Elizabeth Tippett and others, 'When Timekeeping Software Undermines Compliance' (2017) 19 Yale Journal of Law & Technology.

9.4 PAYE and withholding income tax – historical context

Paying[37] for the vast military expenditure and servicing its debt during World War II encouraged the British government to seek a broader tax base, and a more efficient collection mechanism. Tax withholding, or pay as you earn (PAYE), is an ingenious mechanism to collect relatively small amounts of tax from a large number of people at a relatively low cost to the state. It was piloted in 1941-2, and then deployed permanently in 1944. Initially, it was a simple calculation. In the US, payroll withholding taxation was also introduced in the 1940s.[38] Milton Friedman, the well-known economist, was part of the team that devised the scheme that became the basis for the Current Tax Payment Act of 1943.[39] By making tax deductible at the time of earning (i.e. monthly or weekly), it makes the tax burden seem less onerous to the tax payer. As the US Treasury itself noted:[40]

> *This greatly eased the collection of the tax for both the taxpayer and the Bureau of Internal Revenue. However, it also greatly reduced the taxpayer's awareness of the amount of tax being collected, i.e. it reduced the transparency of the tax, which made it easier to raise taxes in the future.* [41]

[37] While PAYE is well understood by tax experts, most readers of this dissertation are not tax experts. So, it is appropriate to provide a brief history and definition of withholding tax and PAYE.

[38] Withholding tax was first mooted in the US civil war, but not deployed widely.

[39] Later, Friedman showed some regret for his involvement. Friedman is well known for his views on limiting state intervention in business.

[40] This quote was spotted by an enterprising journalist, Goldberg. It was promptly deleted from the treasury website.

[41] Goldberg, 'Automatic Tax Withholding' (*Washington Post*, 2013) <http://www.aei.org/publication/automatic-tax-withholding/> accessed 14 September 2017.

It also shifted the tax collection burden onto the employer. This meant that the tax authorities could more effectively police compliance, as they engage with the employer on a variety of other tax related matters. Most countries today have some form of PAYE or withholding tax collected by the employer via the payroll.

9.4.1 The payroll vendor landscape in the US, UK and Germany, briefly

This section briefly describes the payroll market development and vendor landscape in the US, UK and Germany. Payroll software design has largely been software vendor driven, rather than developed in-house. The changing demands of payroll compliance for employers mean that payroll software is a competitive and vibrant market, despite its maturity.

US payroll vendor landscape

In North America, ADP, the payroll company, was formed in 1949, and in the late 1950s began to work with IBM and others on the computerization of the North American payroll. ADP and other payroll providers emerged to take on the administrative burden that tax withholding had shifted to the employer.[42] In 1957, ADP moved from manual processing to punch card based systems. By the 1960s, ADP was making use of a mainframe to calculate payroll. It leased its first mainframe in 1961.[43] By 1970, it was processing the payrolls of 7,000 companies, totalling

[42] ADP grew into one of America's most successful companies. It went public in 1961. Today, it has a market capitalization of approximately 50 billion USD. ADP is said to pay one in six Americans, and it has significant market share on a global basis, with a top 3 market share of payroll in France, Germany and the UK, and a strong presence in most major economies.

[43] Martin Campbell-Kelly, 'Historical Reflections: The Rise, Fall, and Resurrection of Software as a Service.' (2009) 52 Communications of the ACM 28.

5 billion USD in wages.[44] Today, ADP claims it pays 1 in 6 Americans, and it has payroll operations in many countries. While there are only a handful of competitors at a global scale, there is a robust, competitive market of payroll software and service providers at a national level. Competitors include Ultimate Software, Workday, Trinet, Ceridian, Oracle, SAP and Paychex. There are also start-ups targeting payroll processing. Examples include Zenefits and Gusto. The US census bureau estimates the US payroll services market to be 39 billion USD in 2016.[45]

UK payroll vendor landscape

In 1963, in Peterborough, UK, Peterborough Software was founded by Ian Evans Gordon. It used spare processing capacity from his then employer, Perkins Engines. By 1990, 20% of the UK population were paid by a Peterborough solution. Peterborough Software was acquired, and eventually became part of Northgate Arinso (NGA), a major ADP competitor. ADP is also present in the UK, and other competitors to NGA include Midland Software, Agresso UNIT4, Oracle, SAP and Sage. The UK payroll market is very competitive, with a mix of international and local vendors competing. There is also a robust payroll outsourcing market in the UK, with Capita, ADP, NGA, etc.

Germany payroll vendor landscape

In Germany, in 1966, DATEV (*Datenverarbeitung und Dienstleistung für den steuerberatenden Beruf*) was founded as a registered cooperative to process tax and payroll. Over the last 50 years, it has grown into a € billion business, producing payroll and tax processing (such as VAT). It is a market leader in the German *Mittelstand*, paying roughly 11 million

[44] Campbell-Kelly, *From Airline Reservations to Sonic the Hedgehog : A History of the Software Industry* 62.

[45] https://www.statista.com/forecasts/409746/united-states-payroll-services-revenue-forecast-naics-541214

people.[46] ADP is a significant player in the German market, and SAP holds a strong position in the large enterprise market. SAP's payroll developments began in the 1980s for the German market, and it then expanded, today covering over 50 countries. SAP's payroll is used both in-house and by payroll service providers. The trade magazine *Personalwirtschaft* [47] tracks the HR technology vendor landscape, and listed over 50 providers in its 2015 market survey. These include GDI, P&I Loga, HS Personalwesen, Lessor, VEDA, Bau Software, and Sage. Start ups include HeavenHR.

Standard software dominates

Organizations today rarely build their own payroll and, if they do, it is typically a legacy system that has grown so complex that reverse engineering the rules is a major undertaking. They either buy standard software and process the payroll themselves, or they outsource the payroll process to a payroll services provider. The market for HR payroll software is roughly 6 billion US$ annually and the market for payroll processing is several times larger than that.[48] Despite its maturity, it is a dynamic market. It is competitive, with large vendors providing multi-country solutions competing with smaller national players. Vendors tend also to differentiate by customer size and sometimes industry. The public sector often has an extra level of complexity, either addressed by specialist vendors or by additional features in the larger vendor offerings. Payroll rules and regulations have reached a level of complexity such that it requires specialized expertise to interpret these rules. Calculating payroll

[46] DATEV, 'Chronologischer Überblick 1966 Bis 1975' <https://www.datev.de/web/de/m/ueber-datev/das-unternehmen/geschichte/chronologischer-ueberblick-1966-bis-1975/> accessed 15 September 2017.

[47] Personalwirtschaft, 'Software Für Payroll' [2015] *Personalwirtschaft*.

[48] See Pang, https://www.appsruntheworld.com/top-10-core-hr-applications-vendors-market-forecast-and-customer-wins/

tax serves little competitive advantage. So, many employers seek to standardize and outsource payroll processing and responsibility.

It is clear from these examples that the software industry continues to see payroll as a significant market for investment. Meeting government driven compliance can be a significant source of revenue and technology innovation for software vendors.

While tax research shows that governments have shifted the tax collection burden onto the employer, this work argues that it is the software industry that really enables the tax collection process to function as effectively as it does. It is also useful to note that software also enables tax minimization, and better tax planning by tax payers.[49]

9.5 Enabling and refining tax and other collections complexity

While payroll software initially mimicked the manual work that was done by the payroll clerk, once established, it enabled new forms of taxation collection to be deployed. Modern rules such as taxation of company car usage based on CO_2 emissions output (UK)[50] or US cross-state taxation rules,[51] or complex leave accrual rules (New Zealand[52]) would be almost impossible to calculate manually. Improvements in technology are often mirrored by increased sophistication in tax collection. For instance,

[49] JL Guyton and others, ‘The Effects of Tax Software and Paid Preparers on Compliance Costs’ (2005) 58 National Tax Journal 439.

[50] See *http://cccfcalculator.hmrc.gov.uk/CCF0.aspx*

[51] Particularly complex in the US is the taxation of employees such as pilots and truck drivers, who cross multiple states.

[52] See the NZ Holidays Act (2003) In discussion with payroll product managers, New Zealand’s leave calculation under the Holidays Act is particularly complex. For instance, Section 9 sets out a requirement to calculate actual daily pay for the purposes of leave accrual. Also, if some public holidays fall on a weekend they are treated differently for leave accrual purposes. Section 45A(1).

improvements in file transfer technology has enabled tighter integration between the payroll and the various receiving parties, such as tax authorities, and private and public social insurance. Today, payroll does not only collect income tax, but other contributions, such as social insurance payments, public and private healthcare contributions, and court instructed deductions such as garnishments (for example, child support or unpaid student loans). For instance, Brazil has a payroll lending provision, enabling loans to be directly collected from the employee via the payroll, and paid to the bank. This has resulted in a reduction in loan interest rates.[53]

An example of payroll complexity

Multiple or concurrent employments are also very complex. For instance, a doctor in a hospital may have two or more jobs. S/he could be head of a research department and paid for that work at a given rate, either calculated via a timesheet or by a default number of hours per month. S/he has another job as a surgeon, where she is paid a different rate with different terms and conditions of employment, for instance her/his holiday and pension, health benefits, unemployment insurance and other entitlements also accrue at different rates. This must all be calculated and then consolidated into a single monthly or bi-weekly payslip. It would be hard to imagine doing this manually. Payroll deductions and entitlements run to many pages of rules today. The complexity is such that specialist vendors have focused on tax table maintenance, tax calendars and tax jurisdiction assessment.[54] Payroll vendors have large teams of compliance experts.

[53] Christiano A Coelho, João MP De Mello and Bruno Funchal, 'The Brazilian Payroll Lending Experiment' (2012) 94 Review of Economics and Statistics 925.

[54] For example, BSI. See *https://www.bsi.com*

In the interview with the head of payroll compliance at Ultimate Software, she noted:

> *It would be almost impossible to calculate a payroll manually in certain states in the US and after a certain threshold of employees. I think a dozen employees and you're in Florida, where they have no state income tax withholding, you could probably do it. It'd be timely, but anything over about 25 employees I think it'd be virtually impossible. We have a new piece of code, for example, that came through effective August 1st and to manually calc a single employee it takes even me, I'm fast, I'm fast at calculating. I'm not good at a lot of things but I can calculate really fast, and it takes me, using tools like Excel, it takes me about 45 minutes per employee to calculate a paycheck.*
>
> *In many, many states like California, Connecticut, New York, the states that have a lot more people in them and therefore a lot more employment, or the states that lean to be a little bit more liberal, it would be impossible to even do a 12-man payroll.*[55]

9.5.1 PAYE, collections and software

PAYE has become the default tax collection mechanism for income tax, in essence, enabled by payroll automation. Modern payroll does not only facilitate tax collection from the employee, it enables sophisticated employer contribution calculation and imbursement. Cumulative PAYE means that even quite complex variable pay tax scenarios are calculated

[55] See Appendix C.

correctly over the year.[56] In the UK, most tax payers do not need to submit a year-end income tax return. So, it is likely that many citizens underestimate the levels of tax that they pay. 86% of income tax is collected by PAYE in the UK.[57]

Similarly, rules for time and attendance have developed a level of complexity that would make calculation without significant software practically impossible. Time and Attendance software today is able to use complex algorithms to help organizations optimize for compliance, organization requirements and employee preference. The complexity of rules, be they works council driven, union or directly from government, require software to calculate the shift and overtime inputs into payroll. The EU Working Time Directive and its derivative legislation at national level creates a significant compliance burden that would be hard to comply with without the help of software for calculating and reporting.

9.6 Government, user and vendor collaboration

Over the last 60 years, most governments, employers and payroll vendors have developed effective mechanisms for working together. Software vendors have built significant expertise and, while they compete with

[56] Most income tax is deducted at source: by employers through the Pay-As-You-Earn (PAYE) system, or by banks, etc. for any interest payments. The PAYE system is cumulative: when calculating tax due each week or month, the employer considers income not simply for the period in question but for the whole of the tax year to date. Tax due on total cumulative income is calculated and tax paid thus far is deducted, giving a figure for tax due this week or month. For those with stable incomes, this system will be little different from a non-cumulative system (in which only income in the current period is considered). For those with volatile incomes, however, the cumulative system means that, at the end of the tax year, the correct amount of tax should have been deducted, whereas under a non-cumulative system, an end-of-year adjustment might be necessary.

[57] Vanessa Houlder, ‘Payroll Reforms Help UK to Close Tax Gap’ *Financial Times* (2016).

each other, they often work together with governments and user groups to understand and sometimes influence payroll regulations. Many countries have a payroll authors group, which meets regularly with the relevant regulators to discuss possible law changes and their technical viability. Payroll related laws change often, and payroll vendors have developed effective mechanisms to understand legal changes, and adopt the products accordingly. In some markets, payroll vendors are certified offering a compliant solution, or process, but in many they are not. Governments today look to payroll vendors to drive new forms of collection efficiency and effectiveness. Witness the UK RTI or Brazilian eSocial, and in Germany, DEÜV. It is not unusual for a country to make significant changes to the payroll rules and reporting multiple times in a year. SAP tracks roughly 1500 compliance changes a year in its globalization unit.

In 1982, the American Payroll Association was formed with the goals of educating payroll experts, and providing a voice to government. The UK has a similar institution, the Chartered Institute of Payroll Professionals. Its predecessor was formed in 1980. These institutes have become highly professional, offering sophisticated training, examinations and certifications of payroll experts. They also lobby governments and vendors. The payroll vendor also plays an important role in educating the payroll departments in how to cope with regulations. The ecosystems to support payroll are sophisticated, with specialized consultants and vendors. Specialized vendors and consultants also handle complex edge cases, such as ex-pat global assignment payrolls, or complex executive stock and deferred compensation provisions.

The example of euro transition: the vendor reaction to significant legal change.

The adoption of the euro in 1999-2002 required a major enhancement to payroll and financial solutions. For the transitional period, the payslip had to be displayed in both the old currency and the euro, and the accounting backend had to track both currencies. Requirements included:

- Date driven multi-currency fields
- Allowing more than one currency per currency field
- Retroactive calculations capable of working across multiple countries
- Multi-currency interfaces
- Reports in multi currency
- Pay slips in multi currency
- Conversion routines for tables such as wage agreements
- Conversion testing and audit routines[58]

Software and payroll service vendors used these requirements to target competitors, and to encourage /coerce customers to move from older versions onto newer solutions. For the transitional period, the move to the Euro helped drive significant software and consulting sales.[59] Compliance changes often provide the impetus for software sales cycles. So, while legal changes can be costly for the vendor to develop, they can create the opportunity for new sales, or upselling. For instance, more recently, during the recent Euro crisis, when it seemed that Greece might leave the Euro, SAP prototyped what capabilities would be required, and then estimated that a new currency capability would be available within weeks of a currency shift. This reinforces the position that software vendors can move quickly to deliver significant compliance features when the market incentives seem likely to demand it.

[58] Thomas Otter, ‘Western Europe: The Impact of the EMU on HR and Payroll Systems.’ (1999) III HRIM Journal 85.

[59] For example, the SAP 1999 annual report (Form 20-F page 39) states the growth in product revenue was also attributable to strong demand during the first half of 1998 for software that complies with year 2000 requirements. The growth in product revenue was further attributable to demand for software that complies with the EMU's conversion to the euro, including business processing during the dual-currency phase.

9.6.1 UK tax collection and pension collection reforms. RTI and Auto-enrolment

A theme in this chapter is that new forms of technology lead to new forms of payroll tax collection. Improvements in integration technology have enabled the UK government to implement a major reform of its payroll tax (PAYE) reporting and pension enrolment rules, called Real Time Integration (RTI).[60] This makes a useful illustration of the vital role the software vendor plays in compliance enforcement, and the importance of government vendor collaboration. It highlights the effective use of technology enhancements to drive more effective and efficient tax collection.

Real Time Information (RTI) was described by Her Majesty's Revenue and Customs (HMRC) and various commentators as the biggest reform of PAYE since its introduction in the 1940s. Instead of reporting annually via a form (P35), employers must report PAYE and national insurance deductions at the time of or prior to the payroll run. The idea is very simple in principle, but relies on good, well-thought-through processes and robust software and interfaces. Instead of the HMRC finding out who was employed by whom and what they were paid only at the end of every tax year, RTI means that the HMRC will know this information in real time every time an employee or worker is paid. While the HMRC provides a tool for very small employers (fewer than 10 employees), this regulation makes electronic submission via an approved payroll solution or provider obligatory. Basically, having code is law. By having the data earlier, the government is able to make more accurate provisions, and also better manage social benefits and other tax credits that are dependent on pay information. The government also sees RTI as a mechanism to reduce tax avoidance by part-time workers and those who hold multiple jobs.

[60] HMRC, 'Real Time Information (RTI): Improving the Operation of Pay As You Earn' (2014).

A discussion paper was published July 2010, and the HMRC gathered feedback from employers and software vendors. A second consultation stage followed in December 2010, and the responses were published in September 2011.[61] The HMRC worked with vendors on a pilot scheme, making sure that the interface and accompanying documentation were robust and complete. Vendor solutions were then certified by the HMRC as compliant with the interface. There was a major project on the part of the HMRC to make sure that the PAYE processing receiving systems would be able to cope with the incoming data. HMRC used external consultants from CAP Gemini to help with the project. There was also a large-scale education campaign, with the HMRC, vendors and the CIPP[62] working together to update the 1.8 million employers in the UK about the new process. The HMRC has an extensive website with interface examples, test routines and a help desk for vendors to get advice on the specifics of the interface and its inner workings.

As is the case with many government IT projects, some of the UK press was sceptical that the project would work.[63] Nevertheless, it seems that RTI has worked according to plan. An extensive online search was unable to find any significant negative reporting on the RTI post go live.

HMRC reported[64] that the proportion of small and medium-sized employers failing to correctly operate PAYE schemes dropped from 41 per cent in 2005-06 to 24 per cent in 2014-15, and the gap for PAYE tax collection fell from £4bn to £2.8bn in the year 2014-15. The HMRC also performed a survey to access customer satisfaction.[65] The report was generally very

[61] ibid.

[62] Chartered Institute of Payroll Professionals.

[63] Real-time PAYE threatens new wave of tax code blunders. http://www.telegraph.co.uk/finance/personalfinance/tax/10356800/Real-time-PAYE-threatens-new-wave-of-tax-code-blunders.html

[64] HMRC, 'Overview of Making Tax Digital - GOV.UK' (2017) <https://www.gov.uk/government/publications/making-tax-digital/overview-of-making-tax-digital> accessed 14 September 2017.

[65] The use of the term customer to describe a taxpayer takes a little getting used to.

positive on the RTI feedback.[66] The RTI fits in with the broader initiative to digitize all revenue collection in the UK. The next stage of the project involves real-time tax code adjustment, and tighter integration with other departments and initiatives, such as the Department for Work and Pensions and the Universal Credit Scheme.[67] VAT and other tax collection mechanisms are 'going digital':

> *Making Tax Digital is a key part of the government's plans to make it easier for individuals and businesses to get their tax right and keep on top of their affairs - meaning the end of the annual tax return for millions.*

It is clear that the UK government sees the partnership with technology vendors as key to achieving its taxation agenda. The consultation process with vendors was key to the success of the initiative, as was the extensive marketing and communication of the initiative. The UK government provides extensive guidance and advisory support for software developers. This is not limited to payroll, but covers other compliance related areas such as excise control, corporation tax, etc. For instance, the website notes:

> *Making Tax Digital (MTD) will help give businesses a modern, streamlined system to keep their tax records and give information to HMRC. Millions of businesses already*

[66] Under RTI, the perceived burden of EOY has decreased or stayed the same for most employers: 75% of employers rated the burden at EOY as minimal (1 or 2 out of 5), compared to 54% under the previous system. 80% of employers perceived the burden to have decreased or remained the same under RTI as the previous system. 80% of employers felt that EOY under RTI took the same amount or less time to complete, compared with the previous system. Half (49%) of employers reported that EOY under RTI had taken them 1 or 2 hours to complete, compared with 29% under the previous system. There has not been a large increase in financial cost to businesses at EOY under RTI: Two thirds (64%) felt that there had been no change in the costs of running payroll at EOY under RTI. Three quarters (73%) expect the costs of running payroll at the next EOY to be about the same as this year.

[67] The Universal Credit Scheme is currently facing significant headwinds.

> *bank, pay their bills and interact online. Digital record keeping is the next step and is one that many businesses have already taken.*
>
> *HMRC has been developing a close and collaborative joint working partnership with commercial software developers. By sharing its application programme interfaces (APIs), HMRC will enable developers to build digital tools that will interact directly with HMRC's own systems and provide a joined-up customer experience.*[68]

In the case of RTI, the government provides highly detailed technical specifications, for instance, on the middleware protocols.[69] These are maintained regularly. In discussion with several payroll developers[70] who have worked on several countries, the UK has the leading edge in terms of how it communicates with payroll developers. Some other countries are seen to have a more distant relationship with the vendors, and this means that the government may not be aware of what is technically feasible. Also, it takes the vendors longer to figure out the rules without good guidelines; this creates costs for the employer, and lost collections for the government in question.

9.6.2 Code as Nudge: Pension savings

At the same time as the RTI initiative, the Department for Work and Pensions in the UK deployed a new model for pension enrolment. Rather than having employees opt in to the employer pension, as in the past, the new provisions introduced a default enrolment. Employers are now obliged to

[68] https://www.gov.uk/government/publications/making-tax-digital-software-suppliers-terms-of-collaboration/terms-of-collaboration-between-hm-revenue-and-customs-and-software-developers

[69] For example see https://www.gov.uk/government/publications/transaction-engine-document-submission-protocol

[70] Telephone interviews with senior globalization expert at SAP, October 2017.

enrol employees into a workplace pension. Again, while there was significant press fearmongering prior to deployment, results are positive.

As the National Audit Office Report[71] notes, workers can then choose to opt out, but automatic enrolment builds on evidence of inertia in people's savings decisions to encourage more people to save for retirement.[72] The report goes on to note that employer compliance is higher than expected, and workers newly contributing to a pension increased more than was expected. It initially expected 7 million people to be newly saving or saving more in workplace pensions as a result of automatic enrolment. It has now increased its estimate to 9 million. The programme also came in under budget.

The initial findings of the National Audit Office would seem to further validate Thaler's now famous nudge theory applied to pension savings. Thaler et al[73] argued that by making pension contribution and a gradual increase in contributions a default, rather than an opt-in, contributions and therefore pension savings would increase significantly.

Now that auto-enrolment is well established, the UK government has established an automatic contribution escalation mechanism. The employee contributions will rise over three 3 years from 1% to 5% by 2019.[74] This is in essence a large-scale implementation: the "Save more Tomorrow" program.[75]Again, in order to achieve this smoothly, it required the government to work closely with software vendors and pension providers to enable the capability in the software, and to help inform the HR

[71] NAO, 'Automatic Enrolment to Workplace Pensions' (2015).

[72] Tippett and others 60.

[73] Richard H Thaler and Shlomo Benartzi, 'Save More Tomorrow^{TM}: Using Behavioral Economics to Increase Employee Saving' (2004) 112 Journal of Political Economy S164; Richard H Thaler and Cass R Sunstein, *Nudge* (Penguin 2008).

[74] See *https://www.workplacepensions.gov.uk/employee/*

[75] Thaler and Benartzi.

departments of employers and employees about the change and what to expect. Code as Nudge.[76]

Both the RTI and the Auto Enrolment initiative illustrate how software solutions can underpin large-scale compliance initiatives and agendas. Neither RTI nor auto enrolment could have been achieved without significant government and software vendor collaboration.

9.6.3 German payroll: The case of social insurance collaboration

German social insurance and tax is complicated, and the payroll that helps support it is considered to be one of the most complicated in the world by payroll vendors. The complexity is partly in the calculation of the tax and insurances, but a bigger challenge is the reporting and communicating to the authorities. In order to make this complexity manageable, the German authorities in collaboration with the insurer representatives business associations and payroll vendors have developed functional and technical standards and a certification model. This has the advantage of insulating the software developer from attempting to directly interpret statute, provides the buyer of the solution with assurance that the solution is compliant, and enables the integration to leverage up-to-date technology enhancements coherently. The standard also drives consistency across vendors and government departments, likely lowering the overall cost.

By way of example, herewith a relatively brief look at the health and social insurance model. SGB IV Section 95 "*Gemeinsame Gundsätze Technik*" demands the definition of technical and functional standards for data transfer, but does not define the standards itself.

[76] Thaler and Sunstein discuss and advocate the use of this technique in both private and goverment pension models. They note the example of the KiwiSaver plan in New Zealand, and the US Pension Protection Act. Stuart Adam and Glen Loutzenhiser, 'Integrating Income Tax and National Insurance: An Interim Report' (2007).

The author's abbreviated translation of Section 95 of SGB IV follows:

> *The representatives of the health insurers, the pension insurers, the department for work, and government accident insurance body are to agree the collective standards for the electronic transfer of data, the technology for transfer, and the interface design. Should this require electronic signature or encryption, it should rely on the technical standards that the security in information technology departments provide. The final approval is from the ministry of work and social affairs, after consultation with the health ministry and the association of employers.*

A more detailed definition of the standards themselves are then documented in the "Verordnung über die Erfassung und Übermittlung von Daten für die Träger der Socialversicherung Datenerfassungs und Übermittlungsverordnung - DEÜV" provides the precise rules for the definition, testing and validation of the data transfer interfaces (especially Sections 17-22). The technical management of the integration services is done by the ITSG (Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung GmbH), which is a service company established by the GKV Spitzenverband. It manages the technical infrastructure and provides advice to vendors, insurers and employers, not just on behalf of health insurance, but also for pension and other social insurers, in essence, a shared service. The ITSG also develops software, for instance DAKOTA,[77] a secure protocol for the transfer of personal data, which is then in turn used by payroll vendors.

The functional standards and integration payload are reassessed annually. There are specific provisions for payroll developers. Defined in the "*Pflichtenheft*", these are produced by ITSG. This is an extensive guide, running to over 300 pages. It defines data dictionary layout, security

[77] *http://www.itsg.de/oeffentliche-services/dakota-ag/technische-vorgaben/*

rules, rollback procedures and so on. There is also an extensive set of test scenarios, against which vendors must test their applications. The basis for this provision of testing data and procedures is Section 22a of the DEÜV. Vendor solutions are also certified on the basis of these tests, see Sections 20 and 21.

The technical XML standard is called eXTRa. It is described as an XML-based transport mechanism for the electronic data transfer between business and administrative government.[78] This open-source standard was developed through collaboration between various participants, pension, health, ITSG and business representative bodies. The editorial control is with the *Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.* This body has the goal of reducing the bureaucratic effort between state and employer, and it has existed in some form since the 1920s. The standard is used, not just for health insurance data transfer, but for a variety of other employer to government transfers, including pension data transfers. The solution is technically advanced, applying modern interface design practices, such as an enterprise service bus. The standard is also very well documented, with extensive design guidelines and other critical documentation elements. There is also a planned roadmap.[79]

The German social insurance system demands detailed, extensive and up-to-date information from employers. Without payroll software, this collection would likely be impossible. While at first glance the German model seems highly bureaucratic, the clear differentiation between the statute, the regulations, the functional and technical standards, and the enforcement mechanisms makes for an effective process. This could be considered as a strong example of co-regulation.

[78] ist ein einheitliches XML-basiertes Transportverfahren für die elektronische Datenübermittlung zwischen Wirtschaft und Verwaltung. http://www.extra-standard.de/ueber-extra/was-ist-extra/index.html

[79] See *http://www.extra-standard.de/ueber-extra/was-gbt-039s-neues-kopie/index.html*

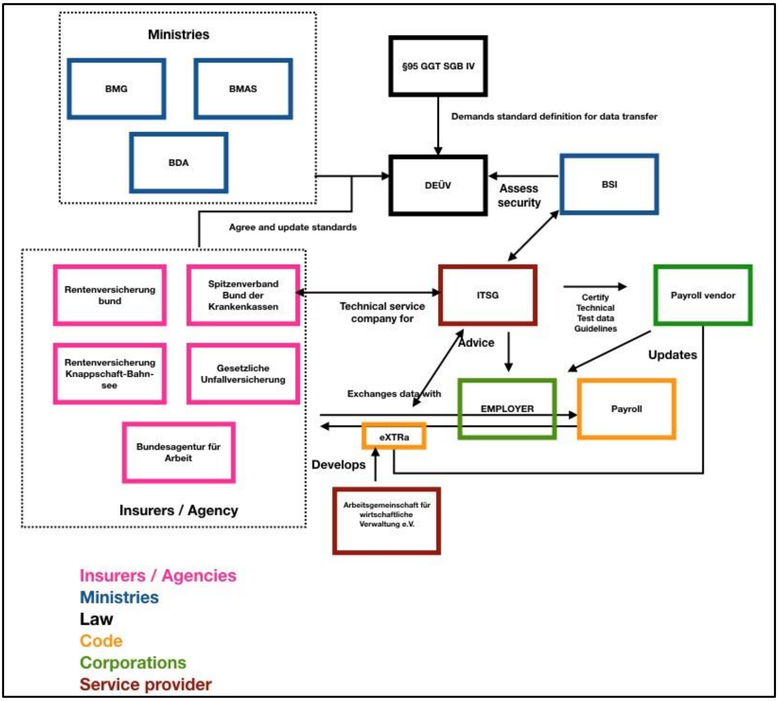

Ministries
BMG
BMAS
BDA
§95 GGT SGB IV
Demands standard definition for data transfer
DEÜV
Assess security
BSI
Agree and update standards
Rentenversicherung bund
Spitzenverband Bund der Krankenkassen
Technical service company for
ITSG
Certify Technical Test data Guidelines
Payroll vendor
Rentenversicherung Knappschaft-Bahn-see
Gesetzliche Unfallversicherung
Advice
Updates
Exchanges data with
EMPLOYER
Payroll
eXTRa
Bundesagentur für Arbeit
Develops
Insurers / Agency
Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.
Insurers / Agencies
Ministries
Law
Code
Corporations
Service provider

Figure 9.1: German social insurance process illustration

9.6.4 A study of time and attendance software in the US

Just as HR software can be designed to facilitate compliance and embed regulation into the applications, it can also undermine compliance if it enables behaviours that run counter to the regulations, or if the regulations are poorly defined. In a recent study,[80] Tipett et al examined a number of US timekeeping software solutions used to track time for the purposes of compliance with the Fair Labor Standards Act (FLSA) and other

[80] Tippett and others.

Department of Labor legislation. The study raised several concerns about features or lack of features in the software, for instance, with supervisor edit features, rounding rules, exception identification and automated meal breaks. One of the strong marketing threads in time and attendance software is its promise to reduce employee fraud, but the authors argue that supervisor fraud requires attention too, and that some software features actually make supervisor fraud easier than in manual systems. Vendors have ignored building controls against supervisor fraud, in the main, because neither the employers nor the regulators were demanding that capability.

The authors also note that the rules for rounding and several other elements of the FLSA regulations have not been revised for more than 30 years, and they comment that the regulations mention storing records on microfilm, an out-dated practice. Some elements of the regulation date back to 1938, with the last major revision in the 1980s. They make some suggestions to the Department of Labor, which controls the FLSA regulation, to revise their guidelines, summarized below:

- Provide workers with hourly access to their timesheets, including supervisor / employer edits
- Require employers to document edit reasons
- Provide reports documenting automated rules
- Provide transparency in rules through reporting tools
- More clarity in output files
- Improved process control and oversight
- Removal of rounding rules

The pithy conclusion states:

> *If the Department of Labor draws on behavioral compliance insights and places more stringent requirements on employers, they will demand – and software makers will produce – better software.*[81]

It would also be sensible for the Department of Labor to engage directly with leading software vendors in order to understand the art of the possible in the technology, and influence vendor strategy directly, as per the German and UK model discussed above. Time and attendance regulations that have not undergone significant revision since the 1980s cannot be effective for the employer, the employee, the software vendor or the regulator.

This type of regulation could be well suited to a standards based approach, as per the DEÜV example. There are standards for systems auditability that could easily be applied here, and the transparency of calculation suggestion is reasonable. The pace of technology change in Time and Attendance means that specific technology feature demands of regulators are problematic, especially if the regulations are only attended to every few decades, for instance mobile device based time capture or use of GPS data.

While Tippett does not specifically state it, software vendors typically react to the direct demands of their customers rather than to any sense of intrinsic fairness or legal conformity. In the absence of clear requirements from the regulator, vendors build what they think customers want to buy, not necessarily what would be the most accurate and robust interpretation of the legislation or regulation. This is no different from the automotive industry, as the brief discussion of automotive safety above aptly illustrates.

[81] ibid 61.

9.7 What can payroll teach other compliance related software development functions?

While payroll received attention from IT academic research in the early part of business computing development, today it receives scant attention. This is unfortunate.

At the risk of nostalgia, payroll requirements have helped drive innovations in hardware and software for decades. For a time, ADP was the largest data processor outside of government. In the 1990s, electronic payslip distribution was key to launching employee self service, which was the first use of the browser for transactions in enterprises. Today though, payroll vendors can largely leverage the performance and scale innovations that have developed elsewhere in the software industry. Today, new advances in software technology typically create new opportunities for payroll developers, rather than the other way around.

The growth of the internet and object-oriented programming played a major role in the shift of programming styles from procedural to test driven models, and eventually Agile. In the 1990s, some large complex multinational companies developed and maintained their own in-house payrolls, as they felt that packaged software did not have the flexibility to cope with their complexity. It was on a payroll project at Chrysler that Kent Beck first introduced Extreme Programming.

9.7.1 Optimizing for maintenance and change control

Payroll software is continually changing because of the constant flow of legal changes. Successful payroll architectures enable most of the legal changes to be handled at a table or configuration level, rather than through code modification. This predates today’s low code endeavours by

40 years or so. Ease of maintenance is the single most important design factor for long term solution stability and profitability. Successful payroll architecture enables very granular change control. A change to the rule in Bulgarian payroll should not impact French payroll, for instance.

9.7.2 Legal change / fix communication and distribution

Payroll vendors have developed sophisticated and reliable channels to communicate information about legal changes and techniques to deploy them effectively in test and product environments. Not all changes are a response to a legal change; some changes are because of bugs or product issues.

Liz Buck noted in the interview:

> *After each release of the software, which, sometimes tax legislation can be put in a release and sometimes it has to go out immediately because of timing, we do webinars that focus on just what's in there. There's a whole section on compliance and payroll. Obviously, the Canadian and the US audiences get separate webinars to detail what we've delivered for their market in that release.*
>
> *Especially things like healthcare reform, which is a multi-year Act passed in the US What we're trying to do is get way ahead of that so that we can have focused webinars. When that law came through, we did just a Healthcare and HIRE Act webinar for our clients.*
>
> *We also have a blog that I post on regularly. I would say, almost daily. On the blog we try to educate our customers not only on employment legislation that they'll need to use our product to support, but also employment legislation that they'll have to change their processes to support. So*

> *that, we're more holistic. Then, anything that's urgent, so let's say we get a flurry of retroactive laws that are being passed.., where they pass a law on August 1st and its effective January 1st of the current year so you have to go back.*
>
> *If we have legislation like that that we have to build really quickly for we'll publish what's called a news wire that actually goes to people's email boxes and says hey there's a change that's coming up immediately. It's going to be applied tonight. Here's the impact and here's how we're helping you.*
>
> *Multiple ways of communicating depending on the urgency and what the client needs to do to prepare for it.*[82]

And on deployment:

> *SaaS makes it easier. For one, software service you have less customization. You have a lot of what I call configuration or customer specific design work but not a lot of customization so it's very easy when I have those late*-breaking *laws, as I like to call them, to go and just update my whole SaaS farm and then I know the client is current. I'm not asking them to do something that maybe they've got because they have it on premise they've customized or they have developers that are going to have to work with it. They can pretty quickly adapt in a SaaS model to getting that through.*[83]

[82] Lightly edited for clarity and brevity, see Appendix C.

[83] Lightly edited for clarity and brevity, see Appendix C.

9.7.3 Data protection law and testing

From the perspective of payroll accuracy, payroll should be tested with live data. However, given the sensitive nature of payroll data from a privacy and security perspective, this is problematic. Payroll vendors, or their partners, have developed tools that effectively obscure and mask the data, while enabling effective testing, as noted in the interview with Nigel James:

> *Nigel: Yeah. We generally use tools. And there's a couple of tools, particularly for SAP HR systems, because it's such a big issue that there's software that will copy back from a production system. They give you tools to say "Make it John Doe one, two, three, four" kind of thing, instead of "CEO" or whoever.*[84]

In the context of increased attention on privacy and testing, the experiences of payroll developers in managing the line between creating effective test data and not compromising live data require closer examination by researchers interested in GDPR testing for instance.

9.7.4 The local product manager

Experts who actually understand the regulations and can take the regulation and turn it into a software specification are critical for payroll success. The interviews with Ultimate, ADP and SAP highlighted this key role. These resources take time to train. This is a hybrid role. Often, these experts come from having worked in payroll departments or have a background in the compliance rules themselves. Wu used the metaphor of

[84] See Appendix D.

"coder as tax lawyer"[85] and, in the case of payroll product management, this is indeed the case.

In the interview with Liz, she commented:

> *I have five people in my compliance research group, and they each own a portion. They're in charge of staying ahead of the legislation in those areas through these services but also through their own individual contacts at the state and individual research. Part of their day, every day, is spent just looking at what's coming.*
>
> *All of our tax research analysts--or most of tax research analysts, and our product analyst in the compliance area have a certification that's call a CPP. It's given by the American Payroll Association--so it's an association certification. It stands for Certified Payroll Professional. Basically it means they've been through a course, and then taken a test that tests their knowledge of the payroll area. That includes a pretty heavy section on compliance. Additionally, we have a CPA on staff that's a certified professional accountant that helps with that in an advisory role for all of Ultimate Software at the product world. He works in development. He's not like someone who works in corporate. We have a CPA in corporate too, certainly, that does our finance stuff but this is someone who works in development that all he does is helps makes sure the accounting law we're abiding by, especially since we've added our tax filing services*[86]

These product managers develop relationships with the broader payroll community, such as key customers, other vendors, payroll organizations

[85] Wu, 'When Code Isn't Law'.

[86] See appendix D.

and the government departments. They may also serve on influencing bodies and councils.

Again, from the interview with Liz:

> *Thomas: How does the process go from, you find out about a rule, and then you end up having to build that rule into the system? How does that process work?*
>
> *Liz: There are tax research analysts, one of those team of five who keeps up with the laws, probably when it was coming down the pipe if we had enough notification, if not, once it passed but hopefully before it was effective, would get all those requirements together. They typically come in the form of an IRS code change or a California code change. They typically print out all the legalese around it, and they work with what we call a product analyst. The product analysts are actually the people who are going to convert that legalese into requirements for our developer to code from and for a quality assurance tester to create test cases from. They're what I would call the middleman between jurisdictional tax research analysts and the developers.*
>
> *They would take that requirement and, in working with the tax research analysts, they would convert it into what we need to do in products. We need to add a data field to support the eco-friendly car, and then we need to reduce taxes.*
>
> *If you're in the State of California and you're paying this, you reduce it however the law reads, like this. That product analyst would take it and convert it into what the developer needed to do, and obviously the tester would write test cases to support that.*

> *The product analyst would also prepare customer-facing documentation to help the customers understand, if you want to have this tax reduction, you will need to go in for everybody with a company car and mark this eco-friendly box, and perhaps answer the five questions California wants you to answer. You know, date of purchase, manufacturer, model number; whatever you need to track to get that tax credit.*[87]

The developer survey highlighted the chasm between software developers and law. Product management, when done well, can help bridge that. The role of product managers has also received scant academic attention; yet given their critical role in successful product development, this is a glaring omission.

9.7.5 What can legislators and regulators learn from payroll?

Tax law generally does an effective job in separating law from the specifics of the underlying regulation. This enables rapid alteration of tax rates, and provides transparency to payroll vendors and employers. The examples of the UK and Germany show that well-structured communication helps vendors build compliant solutions and enable change, and drive down the cost of compliance for employers and the cost of collection for government. Governments that have a more antagonistic or shallow relationship with payroll vendors would do well to reassess that approach in the light of the UK and German approach.

Payroll vendors today are beginning to apply artificial intelligence capabilities to analyze payroll rules. As governments look to how they process tax, they should seek out more collaboration with payroll technology experts.

[87] Appendix C.

9.8 Payroll summary: Half a century of law is coded

For more than 60 years, governments and software vendors have collaborated to develop ever more sophisticated solutions for income tax collection and calculation. When moved to do so, software vendors can quickly and effectively respond to relatively complex compliance requirements.[88] Governments can effectively leverage technology vendors to suit their own purpose. This chapter has addressed the research question of how the development of payroll software has supported and influenced tax and social insurance regulations.

[88] This is not to suggest that all government / vendor IT initiatives are successful. The failure rate of government IT projects is high and there are a number of high profile payroll project failures.

10 Sarbanes Oxley: Accidental instigator of a new software market

10.1 Chapter purpose: How Section 404 created a software market

When in its interests, the software industry can respond remarkably rapidly to a compliance requirement. The Sarbanes-Oxley Act (SOX) heralded a boom in compliance software. It would not be overstating it to say that SOX, and more specifically, Section 404, created a new market category for enterprise software. The software industry responded adroitly and, within months of the passage of the Act, SOX-related software became the most rapidly growing sector in enterprise software.

This chapter will briefly trace the history and context of SOX, provide an overview of the Act, examine the role of the PCACOB, assess the various frameworks, the standards that developed or were reinvigorated, and the response of the software industry to create a market category where none existed.

10.2 Business and political context

To understand the significance of SOX, it is important to look at the political and business environment preceding its passage.

The exposure of massive corruption at Enron, Global Crossing,[1] Tyco,[2] Worldcom,[3] ,Adelphia[4] and many others, and the dismal failure of the existing corporate governance and audit processes (including the eventual collapse of Arthur Andersen, the audit firm) threatened to destroy the trust in financial markets. Without trust, financial markets cannot function effectively.[5] The Chief Accountant of the Securities and Exchange Commission noted in a radio interview:

> *I think the scandals have touched many Americans. There are 90 million Americans who have put their money in the capital markets and have invested there through their*

[1] Global Crossing, like WorldCom, was a telco. There were massive accounting irregularities and excessive executive pay: *http://www.nytimes.com/2002/02/11/business/how-executives-prospered-as-global-crossing-collapsed.html?mcubz=1*

[2] Christian H Kemmerer and Tara J Shawver, 'Tyco: A Top-Down Approach to Ethical Failure' [2007] SSRN Electronic Journal. While the Enron case is better known, the behaviour of the Tyco CEO is dramatically illustrative of just how out of control things were prior to SOX. Kozlowski, as well as Mark Swartz, CFO; and Mark Belnick, chief legal officer, were accused of acting with "egregious, self-serving, and clandestine misconduct" accusing these men of effectively looting the company by obtaining over $170 million in loans for themselves with no formal approval or knowledge to shareholders. In addition, Kozlowski and Swartz engaged in profitable related party transactions and awarded themselves lavish perks

[3] On 25 June 2002, WorldCom, a major long distance telecommunications company, announced that it had overstated earnings in 2001 and 2002 by more than $3.8 billion.

[4] The Adelphia scandal involved massive fraud by the Rigas family, who funded an extravagant lifestyle through loans from the company. They hid the loans for years, but eventually they were exposed. They were eventually given substantial prision sentences. The audit firm Deloittes paid what was then the largest fine to the SEC, without admitting wrongdoing.

[5] Hans J Blommestein, 'How to Restore Trust in Financial Markets?' in Paul H Dembinski and others (eds), *Enron and World Finance: A Case Study in Ethics* (Palgrave Macmillan UK 2006).

> *401(k)s or IRA accounts. So the frauds and the loss in market value of some $9 trillion certainly affected everyone.*[6]

Brookings Institute Research examined the impact of the Enron and WorldCom bankruptcies:

> *Both bankruptcies resulted from accounting malpractice, and symbolize the broader crisis in corporate governance – a crisis which involves top blue chip companies, has reached political leaders at the highest levels of government, and has resulted in high levels of volatility in U.S. stock markets* [7]

This quote illustrates the massive impact Enron had on accounting and business academia:

> *The Enron case plays on many different dimensions, but its prominence is not merely part of popular culture's obsession with scandal du jour. Rather, the Enron situation challenges some of the core beliefs and practices that have underpinned the academic analysis of corporate law and governance, including mergers and acquisitions, since the 1980s.*

[6] NPR interview, 'Has Accounting World Changed Since Enron? : NPR' (2005) <http://www.npr.org/templates/story/story.php?storyId=4673933> accessed 20 September 2017.

[7] Carol Graham, Robert Litan and Sandip Sukhtankar, 'The Bigger They Are, The Harder They Fall: An Estimate of the Costs of the Crisis in Corporate Governance' (2002) 2.

> *These amount to an interlocking set of institutions that constitute "shareholder capitalism," American-style, 2001, that we have been aggressively promoting throughout the world.*[8]

Enron and the other scandals initiated an ethical soul searching that had been largely absent in business academia, the MBA accreditation bodies,[9] accounting bodies and business itself.[10] The failure of business education to teach and instil an ethical component was raised by leading business academics, and debated in the business media[11] and academic journals.[12]

[8] Jeffrey N Gordon, 'What Enron Means for the Management and Control of the Modern Business Corporation: Some Initial Reflections.' (2002) 69 The University of Chicago Law Review 1223.

[9] For instance, see the interview with Trapnell, "Clearly, without question, the scandals of Enron, WorldCom, and others have raised the awareness of business schools about the importance of business ethics. As a result of these scandals, business schools have been the recipients of verbal attacks and complaints. In my opinion business schools have acted positively to enhance, build, add, and grow ethics education programming in a variety of ways and in many cases very creatively."

[10] In the period after the introduction of SOX, large global corporations significantly increased their corporate social responsibility efforts.

[11] See for instance the Economist: *http://www.economist.com/node/3667863*

[12] Sara L Rynes, 'Editor's Foreword Carrying Sumantra Ghoshal's Torch: Creating More Positive, Relevant, and Ecologically Valid Research' (2007) 50 *Academy of Management Journal* 745; Jeffrey Pfeffer, 'Why Do Bad Management Theories Persist? A Comment on Ghoshal' (2005) 4 Academy of Management Learning and Education 96; Julian Birkinshaw, 'Introduction to "beyond Self-Interest Revisited" by Hector Rocha and Sumantra Ghoshal' (2006) 43 *Journal of Management Studies* 583; Henry Mintzberg, 'How Inspiring. How Sad. Comment on Sumantra Ghoshal's Paper' 108; Daniel J Slater and Heather R Dixon-Fowler, 'The Future of the Planet in the Hands of MBAs: An Examination of CEO MBA Education and Corporate Environmental Performance' (2010) 9 Academy of Management Learning and Education 429; Sumantra Ghoshal, 'Bad Management Theories Are Destroying Good Management Practices' (2005) 33 IEEE Engineering Management Review 79; John Gapper, 'Comment on Sumantra Ghoshal's "Bad Management Theories Are Destroying Good Management Practices"' (2005) 4 Academy of Management Learning and Education 101.

10.2.1 Quit custodiet ipsos custodes?

The press headlines highlighted the Caligula-like excesses of the CEOs,[13] but the fraud on this scale was not just the result of a batch of bad CEOs and CFOs. It was a more fundamental failure. The auditors, rather than detecting the issues, were, at best, missing them and, at worst, colluding with those committing the fraud.

Owen noted:

> *The imbalance between management and auditors was further heightened by the economics of the audit industry itself. The by then 'Big Five' accountancy firms viewed their audit businesses as loss leaders for cross-selling higher margin consultancy services (including the very tax and corporate finance advisory services which allowed client firms to 'enhance' earnings).*[14]

Owen also notes that client firms typically spent three times more on consulting services than they did on audit services. Coffee[15] noted that the Big Five learned during the mid-1990s how to cross sell consulting, and treat the audit function as a port of entry into a lucrative client. He goes on to note that the failure of gatekeepers (i.e. auditors) was key to understanding the massive wave of fraud in the late 1990s. He argues that they 'acquiesced in managerial fraud', and that Arthur Andersen were

[13] For instance, Tyco CEO's $6,000 shower curtain, the $2,200 wastebasket.

[14] Tom Kirchmaier Owen, Geoffrey and Grant, Jeremy, 'Corporate Governance in the US and Europe: Where Are We Now?' (2005) 9.

[15] John C Coffee, 'Gatekeeper Failure and Reform: The Challenge of Fashioning Relevant Reforms' (2004) 160 Virginia Law Review 717.

"unlucky" rather than being the one bad apple.[16] From the mid-1990s, there was a significant spike in accounting irregularities.[17]

10.3 Sarbanes Oxley's passage

In the wake of the scandals, market collapse and the looming mid-term elections, two bills were passed: one in the house[18] (April 2002) and one in the senate (June 2002). The bills had been proposed by Senator Paul Sarbanes and Congressman Michael Oxley. The WorldCom scandal broke in early June 2002, adding a further sense of urgency to the proceedings, and strengthened the position of the more stringent proponents for reform, as well as increased pressure from President Bush. A conference committee was formed to reconcile the two bills, and gave the combined bill the name Sarbanes-Oxley Act of 2002. It passed without change, and with a massive majority of 423-3 in the house, and 99 to 0 in the senate.[19] The bill passed remarkably quickly, and the rule making that followed was also very rapid.

In order for SOX to be implemented, it required budget, a restructuring of part of the SEC, the establishment of the PCAOB (Public Company Accounting Oversight Board), to name a few. SOX itself established principles, leaving the rules and enforcement actions to be set by the SEC (Securities and Exchange Commission). The SEC commenced rulemaking in August 2002, and this continued through 2003 and into 2004. The

[16] ibid.

[17] The Waste Management Inc case was a major example of such a fraud. In 2002, the SEC filed suit against the former management, alleging that the company misstated earnings in the period 1992-7, resulting in a restatement.

[18] Corporate and Auditing Accountability, Responsibility, and Transparency Act. HR 3763.

[19] Ivy Xiying Zhang, 'Economic Consequences of the Sarbanes-Oxley Act of 2002' (2007) 44 Journal of Accounting and Economics 74. This provides a useful timeline of the Act.

major rule-making activities were complete by June 2004.[20] Contrast this with the ADA rule-making time-frame.

10.4 What does SOX do?

The Act mandated reforms to enhance executive corporate responsibility, financial disclosure, and stronger oversight of the audit and accounting professions. This work will not analyze the Act in detail, but nevertheless it is worth providing a brief overview before examining the reaction of the software industry to the specific elements of the Act, and the regulations they created.

Table 10.1: SOX outline

SOX outline	
Title I	Establishes the PCAOB (Public Company Accounting Oversight Board. This is to provide independent oversight of the audit profession. It also creates a central oversight board for defining and enforcing the audit processes for SOX compliance.
Title II	Establishes standards for external auditor independence. Restricts auditors from providing consulting services to their clients, and enforces audit partner rotation.
Title III	Mandates that senior executives take individual responsibility for the accuracy and completeness of financial reports. Sec. 302 instructs the SEC to promulgate requirements that the principal executive officer and principal financial officer certify the following in periodic financial reports: (1) the report does not contain untrue statements or material omissions; (2) the financial statements fairly present, in all material respects, the financial condition and results of operations; and (3) such officers are responsible for internal controls designed to ensure that they receive material information regarding the issuer and consolidated subsidiaries.

[20] Yael V. Hochberg, Paola Sapienza and Annette Vissing-Jorgensen, ‘A Lobbying Approach to Evaluating the Sarbanes-Oxley Act of 2002’ (2009) 47 Journal of Accounting Research 519.

Title IV	Describes the enhanced reporting requirements for financial transactions, for instance of executive stock transactions,or off-balance sheet activities. It also requires internal controls for the accuracy of the financial statements and requires timely reporting of material changes in financial condition. Sec. 404 directs the SEC to require by rule that annual reports include an internal control report which: (1) asserts management responsibility for maintaining adequate internal control mechanisms for financial reporting; and (2) evaluates the efficacy of such mechanisms. Requires the public accounting firm responsible for the audit report to attest to and report on the assessment made by the issuer.
Title V	Focuses on disclosing conflicts of interest in security analysts, and establishes a code of conduct for security analysts.
Title VI	Defines SEC authority to censure or bar securities professionals from practice.
Title VII	Requires the SEC and the Comptroller General to perform various studies and report their findings. (i.e. audit firm consolidation, credit agency behavior).
Title VIII	Describes specific criminal penalties for manipulation, destruction etc. of financial records, and provides certain whistle blowers protections (sec 806). This Title is also known as the Corporate and Criminal Fraud Accountability Act of 2002.
Title IX	Increases penalties for white collar crimes and conspiracies, also known as White Collar Crime Penalty Enhancement Act of 2002.
Title X	States that the CEO must sign the tax return.
Title XI	It identifies corporate fraud and record tampering as criminal offenses, and sets and strengthens specific penalties.

The key points can be summarized as follows:

- The creation of the PCAOB to oversee the audit profession
- Various mandates to ensure that companies adopt stronger internal controls to ensure the reliability of the financial statements
- Requirement that the CEO and CFO certify the financial statements
- Auditor independence
- Audit committee with stronger independent directors
- Tighter rules on loans to executives and their stock trading

- Changes to disclosure rules that set how companies disclose information to the public to increase the speed and transparency of information flow
- Whistle blower protections
- New criminal and civil penalties for corporate misconduct

10.4.1 The path from Section 404 to internal controls and software investment

Section 404 itself does not mention software. It is important to explain how SEC regulation, external guidelines, frameworks and standards have created the demand for IT investment. Other sections of SOX are important for internal controls, for instance Section 302. However, this research will focus on Section 404.

Section 404 directs the SEC to require by rule that annual reports include an internal control report which: (1) asserts management responsibility for maintaining adequate internal control mechanisms for financial reporting; and (2) evaluates the efficacy of such mechanisms. It requires the public accounting firm responsible for the audit report to attest to and report on the assessment made by the issuer.

The SEC in turn defined internal control as

> *a process designed by, or under the supervision of, the registrant's principal executive and principal financial officers, or persons performing similar functions, and effected by the registrant's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that*

- pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the registrant;
- provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and receipts and expenditures of the registrant are being made only in accordance with authorizations of management and directors of the registrant, and
- provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements.[21]

Internal controls are the processes the company uses to ensure that the financial statements comply with the Generally Accepted Accounting Principles and are free from material omissions and misrepresentations.[22]

The SEC notes there are 4 components of the Section 404 compliance process: [23]

1. Management should note the principal risks to accurate financial disclosure and the controls designed to address those risks. The SEC guidance establishes a risk-based approach to internal controls. Essentially management should explain what it sees are the major risks, and what controls are in place to reduce the risk of material misstatement.
2. Once management has identified the key controls that need to be assessed, management should analyze whether the controls are actually effective in preventing or detecting financial reporting fraud or errors.

[21] *https://www.sec.gov/news/press/2003-66.htm*

[22] There are other accounting standards that are also concerned with internal controls, but they are not relevant for this analysis. See for example the INTOSAI GOV 9100.

[23] Stephen M Bainbridge, *The Complete Guide to Sarbanes-Oxley: Understanding How Sarbanes-Oxley Affects Your Business* (Adams Media 2007) 203–4.

3. Management should then determine whether there are any deficiencies in its internal controls.
4. Management must document the processes by which the report was prepared.

Bainbridge noted that most companies rely on the “the emerging suites of Section 404 compliance software tools” to provide this documentation. The link between regulation and these software tools is the central theme of this chapter.

The SEC rules also stated that the companies should base their assessment on a suitable recognized control framework. The SEC approved framework in the first final rule was the Internal Control Integrated Framework (ICIF), which in turn had been defined by the Committee of Sponsoring Organizations of the Treadway Commission, known as COSO, in 1992.[24] This is a broad framework, establishing principles for the internal controls. In 2004, this framework was extended to include Enterprise Risk Management. It is useful to briefly describe the COSO Framework as it provides one of the links between the high level provisions of Section 404 and the practical implementation of those provisions into code. COSO plays a similar role to SOX as the W3C does to accessibility.

Exploring the link between the law and the scope of the software investment requires a brief exploration of that framework, see also Ramos.[25]

[24] What is COSO? This initiative was set up in 1985 as an independent private sector initiative, sponsored by the 5 major accounting professional associations. The goal of COSO is to provide thought leadership on COSO’s vision to be a recognized thought leader in the global marketplace on the development of guidance in the areas of risk and control which enable good organizational governance and reduction of fraud. See *https://www.coso.org/Pages/aboutus.aspx*

[25] Michael Ramos, ‘Just How Effective Is Your Internal Control?’ (2004) 15 Journal of Corporate Accounting & Finance 29.

Table 10.2: COSO simplified

Component	Description
Control Environment	Senior management sets the "tone at the top" that influences behaviour and attitude.
Risk Assessment	The organization must be aware of and deal with the risks it faces. It must set objectives, identify risks to those objectives, and analyze and develop ways to manage them.
Control Activities	Policies and procedures must be established and executed to help ensure that the actions identified by management to address risks are carried out.
Information and Communications	Surrounding the control activities are the information and communication systems, incl. the accounting system. These systems enable the organization to capture and exchange the information needed to conduct, manage and control operations.
Monitoring	The entire control process must be monitored, and modified if necessary.

Of particular interest here is the specific guidance for information technology systems. Ramos notes that COSO describes two types of controls:

1. General controls: Data centre operations, access security, maintenance controls, system development controls.
2. Application controls: These are controls for transaction processing, authorization, data validity and application integration.

COSO provides a common framework and language with which the company management can discuss, communicate and evaluate business risk and high level controls with employees, investors, regulators and, importantly from a SOX perspective, the auditors. COSO has undergone revisions. In 2013, the Internal Control Integrated Framework was updated and, in 2017, the Enterprise Risk Management Integrated Framework was also updated.

However, almost all businesses today are highly dependent on information technology to run their operations and financial data. COSO is not the tool to describe the information technology controls in detail. In order to understand the risks and controls inherent to IT, an IT specific framework is required, such as COBIT.

10.4.2 COBIT

Organizations require a more IT focused framework or standard to more objectively describe, measure and improve IT controls. COBIT, the control objectives for information and related technology, is such a framework. This framework was first published in 1993 by the Information Systems Audit and Control Association[26], and has had various updates since then, the latest version being COBIT 5. The popularity of COBIT over the last 15 years can be partly but directly attributed to the demands that SOX placed on IT organizations. ISACA contributed feedback to the SEC on a number of occasions during the SOX consultation period. It quickly became the predominant IT controls framework for IT controls.[27] COBIT has received considerable academic attention too.[28]

The current version covers 5 domains and 37 processes.

[26] The Information Systems Audit and Control Association, known as ISACA, was founded in 1965. It provides certifications such as CISA, the Certified Information Systems Auditor. Today, it has 135,000 members. ISACA also acquired the CMMI Institute from Carnegie Mellon University.

[27] The CEB 2014 IT Audit Benchmark survey noted that COBIT was used by 60% of responding organizations.

[28] G Ridley, J Young and P Carroll, 'COBIT and Its Utilization: A Framework from the Literature', *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the* (IEEE 2004); David S Kerr and Uday S Murthy, 'The Importance of the COBIT Framework IT Processes for Effective Internal Control over Financial Reporting in Organizations: An International Survey' (2013) 50 Information and Management 590; Brad Tuttle and Scott D Vandervelde, 'An Empirical Examination of CobiT as an Internal Control Framework for Information Technology' (2007) 8 International Journal of Accounting Information Systems 240.

Table 10.3: COBIT 5 domains

COBIT 5 domains	
EDM	Evaluate, Direct and Monitor
APO	Align, Plan and Organize
BAI	Build, Acquire and Implement
DSS	Deliver, Service and Support
MEA	Monitor, Evaluate and Assess

Each domain breaks down into processes, for example:

Table 10.4: Deliver, Service and Support processes

COBIT 5 Deliver Service and Support	
DSS1	Manage Operations
DSS2	Manage Service Requests and Incidents
DSS3	Manage Problems
DSS4	Manage Continuity
DSS5	Manage Security Services
DSS6	Manage Business Process Controls

Each process in turn has attributes and controls, as well as an RACI matrix. (Responsible, Accountable, Consulted, Informed).

The more granular controls in COBIT map to higher level principles and controls defined in COSO. The link between the two is well defined and documented. COBIT overlaps in part with other standards and frameworks, such as ITIL, and ISO 17799, now ISO 27002. In many instances, it is complementary to those standards. For an examination of the combined use of COBIT and ISO17799, see Von Solms.[29] For COBIT, ITIL and ISO standards alignment details, see also Hardy.[30]

COBIT 5 now includes ITIL[31] principles, and there is detailed mapping available to help organizations determine which framework to use for which purpose[32]. Since the passage of SOX, the frameworks have become richer as has the ecosystem of consultant that advise organizations on these frameworks.

The framework is also mapped to other laws and regulations, for instance the Payment Card Industry Data Security Standard, PCI DSS.[33]

10.5 The role of the PCACOB, briefly

The PCAOB was established by SOX Title I to provide independent oversight of the audit and accounting professions, and it is also responsible for setting audit standards. Prior to SOX, the audit profession in the US was self regulated. This was a major change. The SEC has oversight of the PCAOB. According to the SEC, the PCAOB responsibilities are:

[29] Basie Von Solms, ‘Information Security Governance: COBIT or ISO 17799 or Both?’ (2005) 24 Computers and Security 99.

[30] Gary Hardy, ‘Guidance on Aligning COBIT, ITIL and ISO 17799’ (2006) 1 Information Systems Control Journal 32; Shamsul Sahibudin, Mohammad Sharifi and Masarat Ayat, ‘Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations’, *Proceedings - 2nd Asia International Conference on Modelling and Simulation, AMS 2008* (IEEE 2008).

[31] ITIL developed from the UK government guidelines.

[32] *https://www.isaca.org/Knowledge-Center/COBIT/Pages/COBIT-Mapping-Documents.aspx*

[33] *https://www.isaca.org/Knowledge-Center/cobit/Documents/CF-Vol-1-2014-Supporting-PCI-DSS-3-0-Compliance-With-COBIT-5_nlt_Eng_0114.pdf*

- registering public accounting firms;
- establishing auditing, quality control, ethics, independence, and other standards relating to public company audits;
- conducting inspections, investigations, and disciplinary proceedings of registered accounting firms; and
- enforcing compliance with Sarbanes-Oxley.

The PCACOB is important for this research in so far as it sets the standards for enforcing compliance with SOX. This work will not discuss broader roles of the PCAOB, nor will it examine the debates relating to self-regulation of the audit profession, other than the brief mention earlier.

In June 2004, the SEC approved the PCACOB's Auditing Standard no. 2, which set out "the standards by which Auditors should conduct an audit of internal control over financial reporting performed in conjunction with an Audit of Financial statements". The standard was to apply for audits of the fiscal year beginning 2006.

Prior to this standard, auditors merely had to 'consider' the internal audit. With this standard, it demanded that the auditors actually audit the internal controls over financial reporting. This meant evaluating the processes used to assess the internal controls, evaluating the effectiveness of the design and operation of the controls, and forming an opinion about whether the control over the financial reporting is adequate. The standard also imposed specific responsibilities on the company management. These provide detail to the higher level provisions outlined in SOX:

- Accept responsibility for the effectiveness of the company's internal control over financial reporting
- Evaluate the effectiveness of internal control over financial reporting, using suitable control criteria such as the COSO framework or an alternative recognized framework developed by a body of experts following due process

- Support the evaluation with sufficient documented evidence
- Present a written assessment about the effectiveness of the company's internal control as of the end of the most recent fiscal year.

The requirement for organizations to evaluate internal controls was driven in part by the SEC requirement, but mainly by the demands of the PCAOB standard.

The PCAOB standard no 2, despite being over 200 pages, makes scant direct mention of IT. The only direct reference to IT in PCAOB Standard 2. An Audit of Intemal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements, is that financial auditors should perform a 'walkthrough' of the information system to be satisfied with the design and operation of the applicable[34] controls.

However, the standard does recommend COSO and the tight alignment between COSO and COBIT provided a framework to assess the IT controls.

10.5.1 PCAOB Audit Standard no 2 and its immediate impact

Given the rather hectic passage of SOX itself, the speed at which the regulations were produced, its aftermath, and the general market sentiment, it is not surprising that this first standard and its subsequent implementation had flaws, and, as is often the case with complex legislation and regulation, unintended consequences:

[34] Joseph B O'Donnell and Yigal Rechtman, 'Navigating the Standards for Information Technology Controls' (2005) 75 The CPA Journal 64.

- Confusion reigned.[35]
- Cost of audit went up dramatically in the period immediately after the introduction of the Audit Standard. Various studies have documented the massive increase in audit costs in the first few years after the passage of AS2. One such study noted a mean increase in audit fees of over 80%.[36] Other studies reported increases in audit fees of over 65% [37] and a large increase in internal compliance costs.
- Auditors were given increased power to demand information from organizations, yet many organizations did not have good process documentation or the tools to automate process documentation and monitor process controls. For instance, many organizations did not have up-to-date system based organization charts. So, significant time and money was spent building organization charts in tools such as Powerpoint and Visio.
- The standard itself lacked precision. So, this gave the auditors a rather more powerful remit than was originally envisaged.
- Audit firms, forced to divest of their consulting divisions, were able to use the PCAOB standards to drive new audit revenue. For instance, fee discounting dropped significantly post SOX.[38]
- The aggressive (if you were an audit client) and prudent (if you were an auditor) approach of the audit firms meant that many CEOs and CFOs made SOX compliance the number one priority.
- Organizations that relied on third party service providers in turn placed compliance demands on them, in part because auditors demanded that third party providers prove that they too had adequate controls in

[35] Parveen P Gupta and Tim Leech, 'Making Sarbanes-Oxley 404 Work: Reducing Cost, Increasing Effectiveness' (2006) 3 International Journal of Disclosure and Governance 27.

[36] K Raghunandan and Dasaratha V. Rama, 'SOX Section 404 Material Weakness Disclosures and Audit Fees' (2006) 25 AUDITING: A Journal of Practice & Theory 99.

[37] Susan W Eldridge and Burch T Kealey, 'SOX Costs: Auditor Attestation under Section 404'.

[38] Hua Wei Huang, K Raghunandan and Dasaratha Rama, 'Audit Fees for Initial Audit Engagements before and after Sox' (2009) 28 Auditing 171.

place. This massively increased the focus on the SAS70[39] audit, which has similar control attestation requirements.[40]

- Internal audit and the technology to support it shifted dramatically from being a low impact, commodity-like process to being a strategic area of investment. The market for internal auditors boomed[41] and the skillset expectations for internal auditors also increased.[42]
- Consulting advisory services for SOX mushroomed.
- It created a massive opportunity for new software companies to emerge, for existing vendors to create new products, and also for vendors to re-package existing technologies for the new challenges of SOX.
- While it has been shown that overall IT spend increased, IT topics that could be linked directly (or sometimes tenuously) to SOX crowded out other IT spend.

The accounting standards have since been updated (PCAOB Auditing Standard no. 5 was approved in 2007), and some of the teething issues of the earlier standard were addressed. The PCAOB described it as being less prescriptive, more scalable, eliminates unnecessary procedures, and a

[39] Statement on Auditing Standards (SAS) No. 70, Service Organizations, was a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A service auditor's examination performed in accordance with SAS No. 70 (also commonly referred to as a "SAS 70 Audit") represents that a service organization has been through an in-depth examination of their control objectives and control activities, which often include controls over information technology and related processes. Via http://sas70.com/sas70_overview.html

[40] Lineke Sneller and Henk Langendijk, ‘Sarbanes Oxley Section 404 Costs of Compliance: A Case Study’ (2007) 15 Corporate Governance 101.

[41] Tom Oxner and Karen Oxner, ‘Boom Time for Internal Audit Professionals: Thanks to the Profession’s Growing Stature, Internal Auditors Are Enjoying Higher Salaries and Greater Career Opportunities, The IIA’s Latest Job Market Survey Reports’ (2006) 63 Internal Auditor 50.

[42] Glenn E Sumners and Jared S Soileau, ‘Addressing Internal Audit Staffing Challenges’ (2008) 37 EDPACS 1; Jeffrey W Merhout and Sarah E Buchman, ‘Requisite Skills and Knowledge for Entry-Level IT Auditors’ (2007) 18 Journal of Information Systems Education 469.

principled approach to determine when auditors can rely on the work of others. Research has shown a decrease in audit costs with AS5.[43]

10.6 SOX and accidental software market

10.6.1 The case of separation of duties: From feature to market

Separation of duties (SoD) is a control mechanism to help organizations reduce incidents of fraud and error. It has been a fundamental part of accounting and business practice for literally hundreds of years. Obvious examples of SoD include someone that signs cheques should not be able to create creditors. Prior to SOX, while internal auditors and others concerned with fraud control paid attention to SoD checks in business processes, and accounting and payroll software typically had some SoD controls built into the applications (for instance, most payrolls enable organizations to have a four-eyes principle for expense or payroll changes), SoD was not a significant driver for IT or process spend in most organizations.

Prior to SOX, in part because there was limited adoption of IT governance frameworks such as COBIT, the deployment of SoD concepts in the development, operation and maintenance of the IT systems themselves was relatively inconsistent at best.

Frameworks such as ITIL and COBIT insist on SoD for IT processes, for instance in systems user provisioning, or access to production system code or back-up storage security.

[43] Jagan Krishnan, Jayanthi Krishnan and Hakjoon Song, ‘The Effect of Auditing Standard No. 5 on Audit Fees’ (2011) 30 AUDITING: A Journal of Practice & Theory 1.

With the arrival of SOX, two major factors changed for separation of duties, turning it into a major business and IT concern. Because of the increased audit power conferred by the PCAOB standard, auditors demanded stronger implementation and assessment of the traditional business process SoD checks. For instance, they would require detailed documentation listing the persons approving invoices and their position on their organizational chart, and, for cases where it was not possible to separate the duties, the risk mitigation had to be clearly documented.

Secondly, it was not enough just to have SoD at the business process level. Because IT systems run those business processes, and a failure or weakness in those systems is itself a material weakness, SoD in IT suddenly became a significant obligation. So, SoD drove a massive focus on application and IT security management.

In the space of less than 18 months, SoD went from being a minor feature to being a CFO level demand. This created an almost instant market for tools that could track and manage SoD. Managing super-users became big business.

Initially, small, nimble vendors developed solutions to solve specific compliance requirements, such as SoD. An example of such a vendor was Virsa Systems. Virsa was founded in 1996 as an audit technology consultancy. With SOX, it focused on taking that expertise and building tools for SoD management and control, based in part on software solutions developed with PWC. These tools sat on top of various ERP systems, such as SAP, Oracle or PeopleSoft. Their 2004 press release described their toolset as follows:[44]

> *The Enterprise Control Manager consists of several seamlessly integrated management and analysis modules, which provide a powerful array of customizable features that*

[44] *https://www.businesswire.com/news/home/20040120005662/en/Virsa-Unveils-Enterprise-Control-Manager-Accelerate-Sarbanes-Oxley*

address an organizations specific business requirement around security & controls. These modules include Virsa's Risk Assessment Module, Role Management Module, Firefighting Analysis Module, and Enterprise Controls Module.

Virsa's Risk Assessment Module provides comprehensive SOD and risk management capabilities that completely automate the analysis and resolution of SOD and SOX related issues. Its preventative controls feature includes, the monitoring of conflicting transactions, the ability to define rules that fits your specific enterprise applications environment and unlimited "drill-down", reporting capabilities. This module facilitates 24x7 audits and SOD compliance, thus fulfilling the key Sarbanes-Oxley requirements.

The Role Management Module is a powerful and intuitive way to manage role definitions and change management. This not only enforces best practice but also automates many time-consuming and painful tasks like creation of master & derived roles.

The Firefighting Administration Module is an innovative solution to automate the firefighting process including administration, monitoring and logging of firefighting activities. This enables the handling of production system emergencies in an organized and systematic manner.

The Enterprise Controls Module automates the most time consuming tasks related to regulatory compliance. It has multi-level reporting capabilities to meet the needs of all key players such as CEO's, CFO's and auditors. The Enterprise Controls Module dashboard performs the reporting, rating and tracking of material weaknesses, significant deficiencies and deficiencies. This module can also be

> *customized to report, track and document remediation from a process and assertion perspective.*

For the year 2005, Virsa reported 245% growth, closing deals with America Online, Coleman, General Electric, Johnson & Johnson, Kohler, Lockheed Martin, Merck, PricewaterhouseCoopers and Sony Electronics. In Europe, the company closed deals with GlaxoSmithKline, Siemens, Sanofi-Aventis, Unilever, Diageo, Vodafone UK, Velux, Holcim, Premier Foods, BOC Group and Elan. Elsewhere, Virsa added new customers including Pioneer Foods in South Africa, Tata Motors in India, ABB in China, WEG in Brazil, and Nexen, BreconRidge and Precision Drilling in Canada.[45] It is useful to note that SOX drove global demand for compliance tools, not just in the US.

Another vendor that emerged as a competitor to Virsa was Approva. It was founded in 2002, and it offered a solution called BizRights. An excerpt from a 2004 press release noted:

> *The newest version of BizRights(TM) expands its functionality to include simulation analysis for proactive risk management, pre-defined approval templates and documentation of changes to internal controls. These enhancements enable BizRights users to continuously identify, document, test, manage and monitor internal controls throughout their organizations. As a result, BizRights helps customers achieve ongoing Sarbanes-Oxley compliance, smoother ERP upgrades, rollouts and consolidations and greater business process efficiency.*[46]

[45] *https://www.businesswire.com/news/home/20060221005523/en/Virsa-Closes-2005-300-Customers-Record-Results*

[46] *https://www.businesswire.com/news/home/20040406005398/en/Approva-Introduces-BizRights-2.0-Software-Facilitate-Secure*

Approva's customers included Air Products, Campbell Soup Company, Colgate-Palmolive, DirecTV, Discovery Communications, McCormick & Company, Pratt & Whitney, Siemens and Wyndham Hotels & Resorts. In 2006, Approva closed a deal with Procter and Gamble. The wording of the P&G press release is illustrative of the market sentiment at the time for internal controls:

> *P&G will use the software to design, test, monitor and audit application controls across its global SAP deployment including managing sensitive access and segregation of duties (SOD), supporting a compliant provisioning process for new user requests, and monitoring sensitive transactions within SAP.*[47]

The fact that P&G issued a press release about buying SoD software illustrates how concerned large multinationals were about telling the market that they were on top of SOX compliance. Usually, it is the software vendor who issues the press release. This could be described as virtue signalling.

Solutions such as Virsa and Approva were fast movers in the market. Virsa developed a strong partnership with SAP, and was acquired by SAP in 2006. The terms of the acquisition were not publically disclosed. SAP then expanded the Virsa offering and combinied it with other solutions into a broader offering.

At the time of the acquisition, Gartner described the acquisition as follows:

> *"SAP customers should see this planned acquisition as positive. It fills a gap in SAP's compliance capabilities and signals a commitment to the vision SAP articulated at the end of 2005 – to put compliance at the center of its strategy...*

[47] *http://news.pg.com/press-release/pg-corporate-announcements/approva-corp-licenses-its-bizrightsr-platform-and-enterpris*

> *SAP plans to form a fifth business unit to focus on governance, risk and compliance in a way that complements other mySAP components, and will continue Virsa's strategy to build out a product line that provides end-to-end compliance tools and process-specific solutions. SAP plans to consolidate all its compliance-related efforts into this new business unit."*[48]

Other vendors in the controls market included ACL Services, FoxT, CSI Tools, LogicalApps, Greenlight Technologies Infogix Oracle, Open Pages, Oversight Systems Security Weaver and SymSure.

Approva was acquired by Infor (Lawson) in 2011. In 2007, Oracle acquired LogicalApps. In 2010, IBM acquired Open Pages.

10.6.2 The extended market for SOX related solutions

SoD was one example of a pressing SOX-related compliance requirement, but the scope of solutions marketed to "help solve SOX" was far broader. Many enterprise software vendors attempted to link solutions to SOX, even if they were only tangentially relevant.

Vendors quickly grasped the power of the word SOX to release capital and operating budget. Hamerman, a Forester analyst, noted in an article in 2006[49] that "SOX is becoming a catalyst or driver to make overdue improvements in ERP and IT infrastructure." Hagerty from AMR commented that [SOX] is a rallying cry for lots of disparate vendors in many categories. The trend for all sorts of vendors to use SOX as a marketing lever was succinctly described by Morgan, from Open Pages, "There isn't

[48] Gartner, 'SAP Fills Its Compliance Gap With Virsa Acquisition Deal' (2006).

[49] *http://searchdatamanagement.techtarget.com/news/1159557/Find-the-right-SOX-tool*

a software company out there that isn't trying to put the perfume of SOX on whatever pig they own."

10.6.3 Placing GRC and controls software in an academic research context

A search found relatively little academic research focusing on the packaged software market for SOX-related solutions, either in accounting or IT journals. However, there are two welcome exceptions that require perusal.

Firstly, Asprion and Knolmayer[50] provide a robust model for the assimilation (adoption) of access control software. They note:

> *The Sarbanes-Oxley Act (SOX) was a milestone in terms of externally initiated "Corporate Compliance" requirements and took a pioneering role towards professionalization of Internal Controls System (ICS). Enterprise-wide ICS typically consist of hundreds of internal controls which are used for monitoring and supervising potential risk areas and fraud. This results in the need to automate internal controls; software vendors offer so called "Compliance Software", which is often also marketed as GRC (Governance, Risk Management and Compliance) software.*[51]

[50] Petra M Asprion and Gerhard F Knolmayer, 'Assimilation of Compliance Software in Highly Regulated Industries: An Empirical Multitheoretical Investigation', *Proceedings of the Annual Hawaii International Conference on System Sciences* (IEEE 2013).

[51] ibid 4405.

Their analysis noted that three pressures have led to increased assimilation of control systems:

- Coercive pressures: Obligatory external requirements drive assimilation.
- Mimetic pressures: Vendor marketing of best practices, often supported by arguments from audit firms.
- Normative pressures. Influential organizations such as ISACA and the Big4 accounting and audit firms refer, in particular in connection with the SOX, to risks caused by inadequate access controls. In this context, special focus is given to access and SoD controls; automation of these controls is highly recommended.

Secondly, the term GRC did not emerge from IT or accounting research; it was vendor and IT analyst driven. In a detailed study, Racz et al[52] trace the development of the term. They noted:

- There is basically no scientific research on GRC as an integrated concept.
- Software vendors, analysts and consultancies are the main GRC publishers.
- Software technology is the prevailing primary topic. Regulatory compliance is the main driver of GRC, challenged by risk management.
- ERM is an important methodology within GRC (ERM being enterprise risk management).

GRC then began as a marketing term. It enabled software vendors, and the consultancies that support them, to define a new market segment. Vendors were able to assemble various solutions under this broad term, and attract the attention of CFOs and CIOs. The starting point for this

[52] Nicolas Racz, Edgar Weippl and Andreas Seufert, 'A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC)', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Springer, Berlin, Heidelberg 2010).

endeavour was SOX, and, arguably within that, the internal controls related to separation of duties. Today, GRC is a broad umbrella term for a variety of governance, risk compliance technology solutions and services. IDC estimated the 2017 market for GRC software to be 11.8 billion USD.[53]

10.6.4 The impact of SOX more broadly

SOX generally drove a significant increase in earnings corrections and restatements, and the gloomy predictions of some commentators that it would destroy the public offering market were largely unfounded. In the wake of the Act, the passage of the regulations and its enforcement regime, trust in the market returned. SOX had massive impact on accounting and audit regulations around the world, as many countries introduced similar regulations, and the inevitable impact that US compliance rules bring to global organizations wishing to do business with American customers and organizations.

In the specific context of internal controls, SOX made many organizations take those controls more seriously. Organizations today have better process documentation, roles management and separation of duties. IT departments are further along the ITIL and/or COBIT maturity models than 15 years ago.

This work is not focused on passing judgement on the macro-level success of SOX. Accounting academics and commentators are still divided on whether it was worth the cost. Significant questions remain about the effectiveness of the audit industry reform, for instance. It remains controversial today, with significant lobbying efforts to water it down from various lobby groups, especially since the shift in the White House.

[53] https://www.businesswire.com/news/home/20170726005133/en/Strong-Demand-Expected-Drive-Worldwide-Governance-Risk

10.7 Summary: Rapidly building a market out of compliance

Returning to the initial observation: This research will show how the enterprise software industry was able to exploit the law to drive favourable business outcomes for itself, while providing solutions to aid compliance.

Table 10.5: A convergence of opportunities. The market for SOX tools.

Opportunity / driver	**Sarbanes Oxley**
Creditable threat of significant fines and public opprobrium for senior executives.	SOX created a creditable threat of jail time, loss of job, etc. for senior executives.
Compelling event that creates a sense of urgency – the high cost of doing nothing.	The annual audit meant that organizations had to make quick purchase decisions.
Legal concepts that are transposable into standards or frameworks that can be understood by software developers and implemented.	PCAOB AS2 and A5, COSO and COBIT provided a coherent set of requirements that software developers could work with to build solutions.
Expertise available.	Former auditors or finance software developers.
Effective policing of compliance.	SOX empowered an army of auditors to police compliance.
Manageable solution scope.	The first SoD tools did not require massive R&D investment. This enabled new vendors to emerge quickly. The requirements were complex enough that end customers did not want to build something themselves.
Enabling ecosystem.	Consultants, analysts and auditors helped both to sell the solutions and deploy them.
Revenue Model.	Vendors were able to price solutions and quickly develop revenue streams.

SOX, especially Section 404, accidently created a multi-billion dollar market for GRC software and services. The research question asked: What drove the investment into software to support Sarbanes-Oxley compliance? This table summarizes why the software industry moved so aggressively to build SOX related solutions. Finally, Lessig's modality model is useful to summarize the impact of SOX.

Table 10.6: Lessig modalities applied to SOX

Modality	**Impact**
Law	Massive, newsworthy fraud drove rapid adoption of SOX and created new institution PCAOB. Vagueness in standards created confusion, and auditor overreach.
Market	Virtue signaling: Rapid shift to be seen to invest in controls... Growth in demand for audit expertise.
Social norm	Increased ethics focus in MBA type programmes and corporate social responsibility. Shift in attitude in IT departments towards standards such as ITIL and COBIT.
Architecture / technology	New technologies developed to aid compliance (i.e. SoD control).

The GDPR chapter examines the similarities between SOX and GPDR, and the conclusion will suggest that regulators need to learn from the SOX experience

11 GDPR in the enterprise software context

11.1 Chapter purpose: Examining GPDR

This chapter will briefly compare the EU Data Protection Directive with the GDPR, and examine some of the criticisms of the GDPR. It will then examine how various Enterprise Software vendors are approaching the GDPR. The Lessig modality framework provides a useful lens to offer suggestions for how the aims of the GDPR, in particular Privacy By Design, can be more effectively achieved. SOX, Payroll and Accessibility all provide mechanisms and lessons learned that can be applied to data protection.

11.2 Data Protection: A brief history and a definition

Privacy and data protection have blossomed into a field of extensive academic research across multiple disciplines.[1] There is growing collaboration between technology researchers, economists, sociologists and legal theorists, see for instance the work of the Oxford Internet Institute, ZAR or the Berkman Institute. Privacy is complex[2], and a difficult concept to

[1] Brown and Marsden 47.

[2] Hielke Hijmans and Alfonso Scirocco, 'Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty Be Expected to Help?' (2009) 46 Common Market Law Review 1485; Daniel J Solove, 'Understanding Privacy' (2008) 420; Judith Olson and Jonathan Grudin, 'Toward Understanding Preferences for Sharing and Privacy'; Lilian Edwards, 'The Internet and Security: Do We Need a Man with a Red Flag Walking in Front of Every Computer' (2007) 4 SCRIPTed: A Journal of Law, Technology and Society.

precisely define:[3] on the one hand, it can be defined as a property,[4] something that can be traded; on the other hand, it can be seen as a fundamental human right. The impact of technology on privacy presents one of the most significant regulatory challenges of the last 50 years.[5]Data protection law is in essence informational privacy (as opposed to spatial or physical privacy).[6] At the risk of oversimplification, the US tends to see privacy as property, Europe as a right. The fundamental differences in EU v US positions on privacy have been thoroughly examined,[7] but need not concern us here.

Lloyd's definition remains very useful: "The purpose of data protection may be considered that of imposing obligations upon those who process

[3] Daniel J Solove, 'A Taxonomy of Privacy' 447; Hazel Grant, 'Data Protection 1998-2008' (2009) 25 Computer Law and Security Review 44, 44; Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2009).

[4] Lawrence Lessig, *The Architecture of Privacy*, vol 1 (1998).

[5] Brown and Marsden 47.

[6] Lee A Bygrave, 'Privacy and Data Protection: An International Perspective' [2010] Scandinavian studies in law. While the precise definitions of data protection and privacy have occupied the minds of several eminent legal scholars, it is not within the realms of this work to revisit those.

[7] Joel R Reidenberg, 'E-Commerce and Trans-Atlantic Privacy' (2001) 38 Houston Law Review; Holly Kathleen Hall, 'Restoring Dignity and Harmony to United States-European Union Data Protection Regulation' (2018) 23 Communication Law and Policy 125; William J Long and Marc Pang Quek, 'Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise' (2002) 9 Journal of European Public Policy 325; Joanna Kulesza, 'Transboundary Data Protection and International Business Compliance' (2014) 4 International Data Privacy Law 298; P Blume, 'Trans-border Data Flow: Is There a Solution in Sight?' (2000) 8 65; Peter P Swire, 'Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in Privacy and Self-Regulation in the Information Age by the U.S. Department of Commerce.' [1997] SSRN Electronic Journal; Andrew Charlesworth, 'Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures.' (2003) 54 Hastings LJ 931.

personal data, and conferring rights upon those whose details constitute its subject matter."[8]

Data protection law began in Germany, in the state of Hesse, in the 1970s, largely as a response to the increasing power of state and government surveillance, especially given the role of the Stasi in the GDR and, before that, NAZI rule. By the 1990s, various countries across Europe had implemented varying levels of data protection law. The mixed nature of these laws caused confusion and threatened the free flow of information across the Union, hence the need for the EU Data Protection Directive.

11.3 The EU Data Protection Directive, briefly

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereafter EUDPD) was an attempt to create a consistent standard for data protection across Europe, and therefore improve data flows within Europe. It was adopted in 1995 and took effect in 1998. It was in part modelled on the OECD recommendations and principles for the protection of personal data (Notice, Purpose, Consent, Security, Disclosure, Access, Accountability).

11.3.1 Criticisms of the EUDPD

The EUDPD was drafted in the era of the mainframe, before the internet, and largely before the rapid growth of the PC into almost every home, and it is now showing its age. Many businesses have expressed frustration with the EUDPD[9] and it has been unable to cope with the enormous growth of privacy adverse technologies, both in terms of state and

[8] Ian Lloyd, *Information Technology Law* (2014) xli.

[9] Grant 46.

corporate surveillance. Zuboff's term 'surveillance capitalism' is particularly apt.[10] Swire criticized the EUDPD for failing to cope with small, nimble organizations. Having been written when computing was controlled by large multinationals, the EUDPD failed to take account of the potential power of small companies to infringe on privacy.[11]

The Directive also failed to drive the hoped-for levels of consistency across Europe. Different countries have applied the Directive quite differently, and have differing approaches to enforcement. As Poullet noted, this is neither good for data subjects, nor businesses.[12] The Directive has failed to achieve its primary goal to "create a uniform market at the European level for personal data ensuring a high level of protection for data subjects." Poullet also noted other failures of implementation including the lack of public awareness of their rights and the excessive legalism of Data Protection Authorities. Hon et al have noted the Directive's failure to grasp the complex relationship between controller and processor, especially in cloud computing.[13] On similar lines, the Directive has been criticized for not imposing direct statutory obligations on the processor.[14] This author's main criticism[15] of the EUDPD was that it placed no direct

[10] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 Journal of Information Technology 75.

[11] Swire, 'Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in Privacy and Self-Regulation in the Information Age by the U.S. Department of Commerce.' While Swire's metaphor of elephants and mice is useful, the mice of yesterday are now the 100 billion dollar elephants of today.

[12] Yves Poullet, 'EU Data Protection Policy. The Directive 95/46/EC: Ten Years after' (2006) 22 Computer Law and Security Report 206.

[13] W Kuan Hon, Christopher Millard and Ian Walden, 'Who Is Responsible for "Personal Data" in Cloud Computing? The Cloud of Unknowing, Part 2' (2012) 2 International Data Privacy Law 3, 7.

[14] Jenna Lindqvist, 'New Challenges to Personal Data Processing Agreements: Is the GDPR Fit to Deal with Contract, Accountability and Liability in a World of the Internet of Things?' (2017) 26 International Journal of Law and Information Technology 45.

[15] Thomas Otter, 'Data Protection Law: The Cinderella of the Software Industry?' (2007) 23 Computer Law & Security Report 67.

burden on the software manufacturer, only on the data controller, and the controller had limited interest or leverage over the software manufacturer.

The inherent tension between the US and European privacy regimes is manifested in the challenge of cross-border data flows, especially the failure of the Safe Harbour agreement, and the rather awkward scramble recently to replace it with the privacy shield.[16]

In 2009, the UK ICO commissioned a report on the Directive. In the report foreword, the ICO head, Richard Thomas, noted the following about the Directive:[17]

- It is outdated, in terms of technology and regulatory approach.
- It has unclear objectives and insufficient focus on detriment, risk and practical enforcement.
- It is seen as bureaucratic, burdensome and too prescriptive. It focuses on "how" organizations should do things, rather than on "what" they should be achieving.
- It is not clear how much choice and control individuals should have, with regulators sometimes applying the law in a paternalistic way.
- Prescriptive criteria for processing personal data have become a rigid control mechanism. Much effort is devoted to the artificial justification of otherwise unobjectionable processing.
- Its scope is becoming increasingly unclear, for example in on-line and surveillance contexts.
- Its international transfer rules are unrealistic against a backdrop of high-volume, globalized data flows.

[16] David Bender, 'Having Mishandled Safe Harbor, Will the CJEU Do Better with Privacy Shield? A US Perspective' (2016) 6 International Data Privacy Law 117; Tobias Bräutigam, 'The Land of Confusion: International Data Transfers between Schrems and the GDPR'.

[17] RAND Europe, 'Review of EU Data Protection Directive' (2009) 1.

Nevertheless, despite these issues, the Directive has been seen as the gold standard to which many other regulators aspire.[18] Greenleaf has described and analyzed the growth of the global data privacy law for several decades. His latest study notes that 120 countries now have national laws.[19] Many of these bear more than a passing resemblance to the EUDPD.

The Directive (and its national implementations) have provided some privacy protection to European data subjects, but since the early part of this century it became increasingly clear that the Directive required a significant overhaul. Several surveys showed that EU citizens were growing increasingly concerned about privacy.

11.3.2 Replacing the EUDPD

In 2010, the EU[20] announced its intent to rethink data protection and privacy by

- Addressing the impact of new technologies
- Enhancing the internal market dimension of data protection
- Addressing globalization and improving international data transfers
- Improving the coherence of the data protection legal framework

The drafting of the General Data Protection Regulation[21] (GDPR) was subject to intense lobbying, and several delays.[22] It was originally planned

[18] Brown and Marsden 64.

[19] Graham Greenleaf, ‘Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey’.

[20] A comprehensive approach on personal data protection in the European Union *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52010DC0609*

[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

for early 2014, but it was only passed into law 2 years later, with a 2-year transition period to enable countries to alter local legislation and for organizations to get prepared.

11.3.3 GDPR: Revolution or evolutionary tweak?

When reading the words of the German MEP Jan Albrecht, the "GDPR will change the world."[23] He foresees a massive shift in data protection regulation and enforcement that fundamentally alters the global privacy landscape. However, when one reads the website of the UK ICO, the aspirations seem more modest: "What must be recognized is that GDPR is an evolution in data protection, not a total revolution." There are many similarities between the GDPR and the EUDPD, and several significant differences. For organizations that were in reasonable shape for the EUDPD, it will still be a significant step up. For organizations that have ignored the EUDPD, or where they were not obliged to comply, the GDPR will have a massive impact. For many enterprise software vendors, GDPR will mean significant changes in how software is built, sold and deployed.

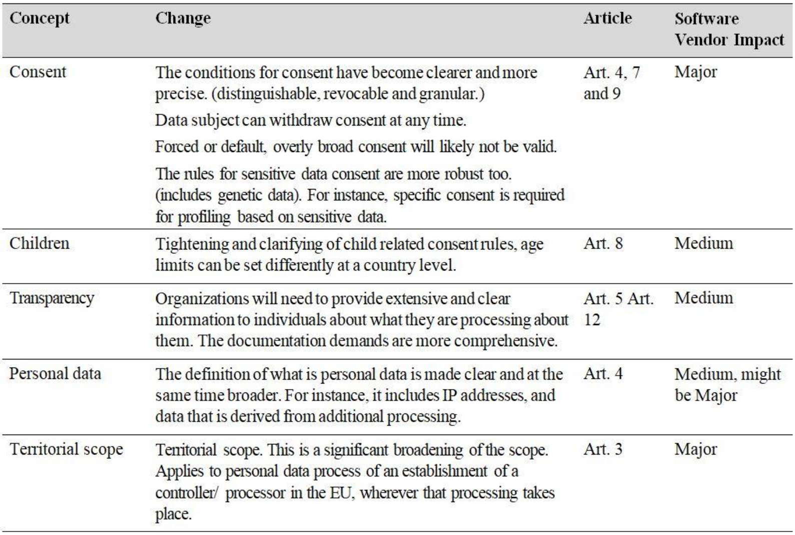
[22] Edwards notes in a forthcoming book that over 4000 amendments were tabled by industry lobbyists. Several MEPs cut and pasted texts from eBay and others into their proposals. *https://lobbyplag.eu/map*

[23] Jan Philipp Albrecht, 'How the GDPR Will Change the World' (2016) 2 European Data Protection Law Review 287. Albrecht throws down a rather aggressive gauntlet here.

11.3.4 What are the main differences between the EUDPD and the GDPR?

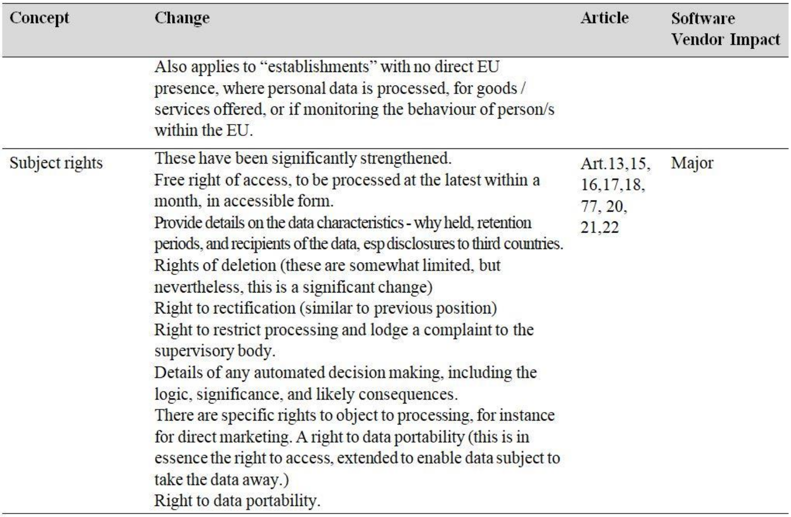
Rather than attempt a detailed assessment of the changes, the table below provides an overview of the major changes, and notes their likely impact on enterprise software vendors.[24]

Table 11.1: GDPR delta and impact

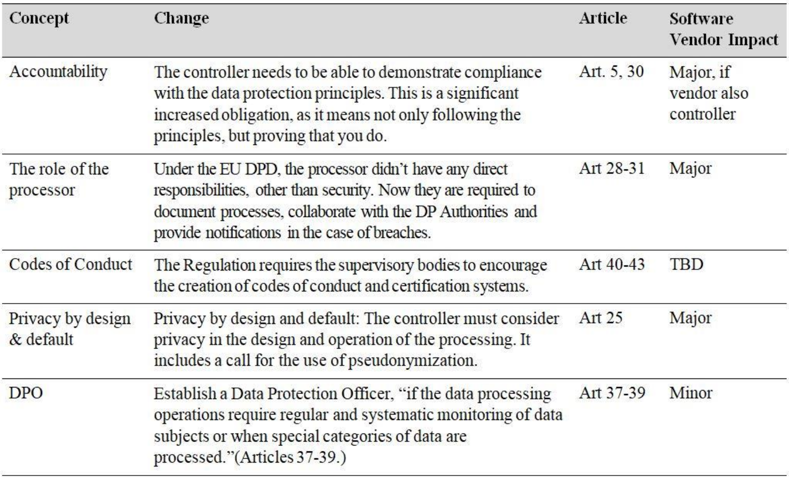


Concept	Change	Article	Software Vendor Impact
Consent	The conditions for consent have become clearer and more precise. (distinguishable, revocable and granular.) Data subject can withdraw consent at any time. Forced or default, overly broad consent will likely not be valid. The rules for sensitive data consent are more robust too. (includes genetic data). For instance, specific consent is required for profiling based on sensitive data.	Art. 4, 7 and 9	Major
Children	Tightening and clarifying of child related consent rules, age limits can be set differently at a country level.	Art. 8	Medium
Transparency	Organizations will need to provide extensive and clear information to individuals about what they are processing about them. The documentation demands are more comprehensive.	Art. 5 Art. 12	Medium
Personal data	The definition of what is personal data is made clear and at the same time broader. For instance, it includes IP addresses, and data that is derived from additional processing.	Art. 4	Medium, might be Major
Territorial scope	Territorial scope. This is a significant broadening of the scope. Applies to personal data process of an establishment of a controller/ processor in the EU, wherever that processing takes place.	Art. 3	Major

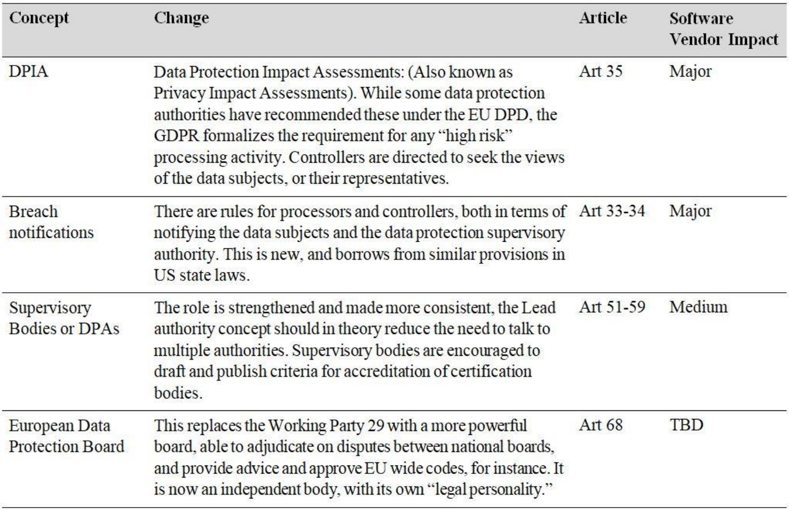
[24] Ruth Boardman and Ariane Mole, 'Guide to the General Data Protection Regulation' (2016). This work was very helpful in providing a clear summary of the changes. The points below largely follow that summary.



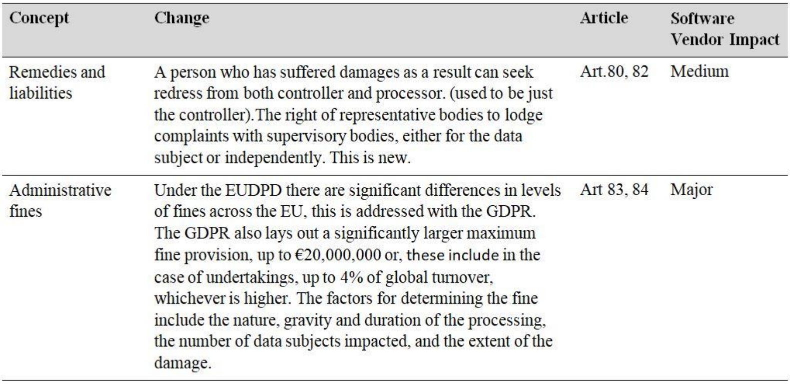
Concept	Change	Article	Software Vendor Impact
	Also applies to "establishments" with no direct EU presence, where personal data is processed, for goods / services offered, or if monitoring the behaviour of person/s within the EU.		
Subject rights	These have been significantly strengthened. Free right of access, to be processed at the latest within a month, in accessible form. Provide details on the data characteristics - why held, retention periods, and recipients of the data, esp disclosures to third countries. Rights of deletion (these are somewhat limited, but nevertheless, this is a significant change) Right to rectification (similar to previous position) Right to restrict processing and lodge a complaint to the supervisory body. Details of any automated decision making, including the logic, significance, and likely consequences. There are specific rights to object to processing, for instance for direct marketing. A right to data portability (this is in essence the right to access, extended to enable data subject to take the data away.) Right to data portability.	Art.13,15, 16,17,18, 77, 20, 21,22	Major



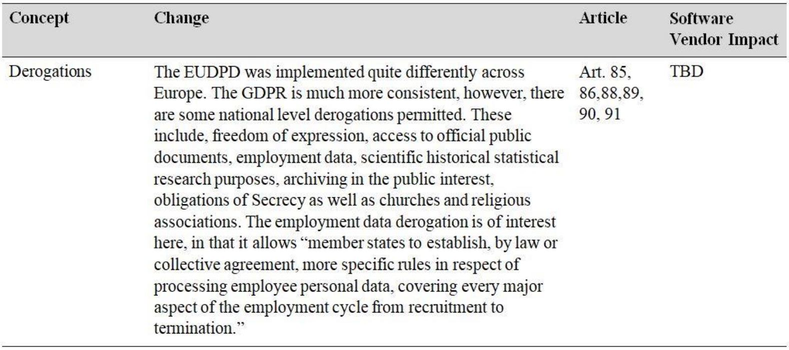
Concept	Change	Article	Software Vendor Impact
Accountability	The controller needs to be able to demonstrate compliance with the data protection principles. This is a significant increased obligation, as it means not only following the principles, but proving that you do.	Art. 5, 30	Major, if vendor also controller
The role of the processor	Under the EU DPD, the processor didn't have any direct responsibilities, other than security. Now they are required to document processes, collaborate with the DP Authorities and provide notifications in the case of breaches.	Art 28-31	Major
Codes of Conduct	The Regulation requires the supervisory bodies to encourage the creation of codes of conduct and certification systems.	Art 40-43	TBD
Privacy by design & default	Privacy by design and default: The controller must consider privacy in the design and operation of the processing. It includes a call for the use of pseudonymization.	Art 25	Major
DPO	Establish a Data Protection Officer, "if the data processing operations require regular and systematic monitoring of data subjects or when special categories of data are processed."(Articles 37-39.)	Art 37-39	Minor



Concept	Change	Article	Software Vendor Impact
DPIA	Data Protection Impact Assessments: (Also known as Privacy Impact Assessments). While some data protection authorities have recommended these under the EU DPD, the GDPR formalizes the requirement for any "high risk" processing activity. Controllers are directed to seek the views of the data subjects, or their representatives.	Art 35	Major
Breach notifications	There are rules for processors and controllers, both in terms of notifying the data subjects and the data protection supervisory authority. This is new, and borrows from similar provisions in US state laws.	Art 33-34	Major
Supervisory Bodies or DPAs	The role is strengthened and made more consistent, the Lead authority concept should in theory reduce the need to talk to multiple authorities. Supervisory bodies are encouraged to draft and publish criteria for accreditation of certification bodies.	Art 51-59	Medium
European Data Protection Board	This replaces the Working Party 29 with a more powerful board, able to adjudicate on disputes between national boards, and provide advice and approve EU wide codes, for instance. It is now an independent body, with its own "legal personality."	Art 68	TBD



Concept	Change	Article	Software Vendor Impact
Remedies and liabilities	A person who has suffered damages as a result can seek redress from both controller and processor. (used to be just the controller).The right of representative bodies to lodge complaints with supervisory bodies, either for the data subject or independently. This is new.	Art.80, 82	Medium
Administrative fines	Under the EUDPD there are significant differences in levels of fines across the EU, this is addressed with the GDPR. The GDPR also lays out a significantly larger maximum fine provision, up to €20,000,000 or, these include in the case of undertakings, up to 4% of global turnover, whichever is higher. The factors for determining the fine include the nature, gravity and duration of the processing, the number of data subjects impacted, and the extent of the damage.	Art 83, 84	Major



Concept	Change	Article	Software Vendor Impact
Derogations	The EUDPD was implemented quite differently across Europe. The GDPR is much more consistent, however, there are some national level derogations permitted. These include, freedom of expression, access to official public documents, employment data, scientific historical statistical research purposes, archiving in the public interest, obligations of Secrecy as well as churches and religious associations. The employment data derogation is of interest here, in that it allows "member states to establish, by law or collective agreement, more specific rules in respect of processing employee personal data, covering every major aspect of the employment cycle from recruitment to termination."	Art. 85, 86,88,89, 90, 91	TBD

11.4 Academic responses to the GDPR

The GDPR has generated significant academic commentary, not just from legal scholars, but also from other disciplines such as computer science. Several authors have raised doubts about the GDPR's ability to cope with new technologies, and other concerns about the GDPR. These are worth briefly noting, but this is by no means a complete overview of the criticism of GPDR .

11.4.1 A question of risk

The GDPR makes several references to risk (in PbD and DPIA, for instance), but it currently fails to provide clarity about how to assess privacy risk effectively. As Raabe notes[25], computer science and industry have extensive standards for security risk, but applying these to privacy is problematic. Without a coherent model of privacy risk that can be effectively mapped to software design, software developers run the "risk" of ignoring risk, or being paralyzed by it. With the GDPR, the legislator has shifted the responsibility of deciding what is "data protection compliant"

[25] Oliver Raabe, 'Beiträge Zu Einer Systemtheorie Sicherheit' (2018) Forthcoming Acatech.

to the data controller (and indirectly the software developer) without giving them the mechanisms to judge and mitigate risk. He argues that neither the BSI privacy impact assessment guidelines, nor the German Standard-Datenschutz model provide an adequate assessment of risk. He proposes a more robust and quantitative modelling process and calls for more collaborative research between computer science, risk management experts and legal researchers on applying more robust risk modelling techniques to privacy. Quelle notes that "Controllers have always had to implement the law, but under the Data Protection Directive, they were not required to assess whether the legal requirements are sufficient to achieve protection or, to the contrary, whether they are disproportionately burdensome."[26] The GDPR changes this dramatically. Spina comments, "In this new regulatory framework, data controllers are requested to control, in a formal and structured way, the risks to the rights and freedoms of data subjects arising from data processing operations"[27] and that there is confusion amongst experts about the role of risk and risk management in data protection.[28] While Recital 90 requires the use of an "objective method", neither the GDPR itself, nor the WP 29 provide guidance on how to actually perform the risk analysis.[29] At the time of writing, various data protection agencies were drafting or planning to publish guidelines.

11.4.2 Privacy by design and default, and the privacy impact assessment

Before noting how PbD and PIA are applied to the GDPR, it is useful to briefly describe the history of these concepts. They have been applied

[26] Claudia Quelle, 'The "Risk Revolution" in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too', vol 17 (2017) 16.

[27] Alessandro Spina, 'A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics' (2017) 8 European Journal of Risk Regulation 88, 89.

[28] ibid 90.

[29] Raphaël Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' *Computer Law and Security Review* (2018) 11.

sporadically prior to the GDPR, but the GDPR moves them to a central role. For software developers, PbD is likely to be fraught.

While the ideas of designing or engineering privacy into products has been around since the first lace curtains, it gained attention in the informational privacy context through the work and advocacy of Cavoukian,[30] the Canadian DPO. The concept is alluring. The privacy implications should be considered at design time, not merely during system operations. She noted 7 principles:

1. Proactive not reactive; preventative not remedial action.
2. Privacy as the default setting.
3. Privacy embedded into design.
4. Positive-sum, not zero-sum, outcomes
   (i.e. no trade-off between different interests).
5. End-to-end security – ensuring full life-cycle protection.
6. A commitment to visibility and transparency.
7. Respect for user privacy – all developments need to remain
   user centered.

The German data protection commissioner at the time, Schaar,[31] while in favour of PbD, suggested that the positive-sum was not workable, emphasizing the need to more assertively protect the rights of data subjects above commercial interests. The UK ICO sought a more hands off, business friendly approach.[32]

Some computer scientists, while intrigued, expressed considerable frustration with the rather nebulous concepts and lack of 'codeable' definitions.

[30] Ann Cavoukian, 'Privacy by Design – The 7 Foundational Principles – Implementation and Mapping of Fair Information Practices' [2009] Information and Privacy Commissioner of Ontario, Canada 5.

[31] Peter Schaar, 'Privacy by Design' (2010) 3 Identity in the Information Society 267.

[32] Inga Kroener and David Wright, 'A Strategy for Operationalizing Privacy by Design' (2014) 30 Information Society 355, 357. This paper provides an excellent summary of PbD and its challenges.

As recently as 2014, privacy by design was described as vague, noting that (existing) legislation makes many references to PbD, without specifying what it means.[33] Colesky et al note that "However, PbD in itself lacks concrete tools to help software developers design and implement privacy friendly systems. It also lacks clear guidelines on how to map specific legal data protection requirements into system requirements."[34] In defence of PbD, there have been several papers on modelling PbD into code.

Clarke provides a detailed history of the PIA[35] and provides a useful definition, "A PIA is a systematic process, which identifies and evaluates from the perspectives of all stakeholders the potential effects on privacy of a project, initiative or proposed system or scheme and which includes a search for ways to avoid or mitigate negative privacy impacts."[36] Wright notes that the UK introduced the first PIA in Europe in 2007.[37]

11.4.3 PbD and PIA in the context of the GDPR

Edwards encapsulates Article 25 as follows, "it provides that controllers shall apply software design principles as well as organisational measures

[33] Dag Wiese Schartum, 'Making Privacy by Design Operative' (2016) 24 International Journal of Law and Information Technology 151; DK Mulligan and Jennifer King, 'Bridging the Gap between Privacy and Design' (2011) 14 Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems 989; Kroener and Wright; Demetrius Klitou, 'A Solution, But Not a Panacea for Defending Privacy: The Challenges, Criticism and Limitations of Privacy by Design' (2014). See also the heated, by academic standards, discussion between Narayanan and Cavoukian on the limits of pseudonymization.

[34] Michael Colesky, Jaap-Henk Hoepman and Christiaan Hillen, 'A Critical Analysis of Privacy Design Strategies', *2016 IEEE Security and Privacy Workshops (SPW)* (IEEE 2016).

[35] Roger Clarke, 'Privacy Impact Assessment: Its Origins and Development' (2009) 25 Computer Law and Security Review 123.

[36] Roger Clarke, 'An Evaluation of Privacy Impact Assessment Guidance Documents' (2011) 1 International Data Privacy Law 111.

[37] David Wright, 'Making Privacy Impact Assessment More Effective' [2013] The Information Society.

to ‘engineer in’ privacy protection throughout the development, as well as the data capture, processes.”[38] She also notes that Article 25 is advisory in nature in that PbD is restricted by the state of the art, costs of implementation and the nature of the processing in question. Tsormpatzoudi et al note that mixing by design and by default creates more grounds for confusion.[39] For the short term, PbD is likely to cause confusion and frustration in software development circles. So, it is vital that the industry moves from isolated use cases to a set of coherent and practical tools to aid software developers and designers. As Kroener and Wright note, “While these measures can be seen as a step forward in terms of privacy regulation, simply proposing principles is not enough.”[40]

The DPIA (Article 35) and the template tools from the ICO[41] and CNIL have also come under criticism from computer scientists, for instance, by Ahmadian et al, who state “they generally are not suitable to be a process reference model. They describe a set of generic and abstract steps toward PIAs, and most importantly, they do not consider the concrete design of a system to identify specific design flaws and threats”[42] Clarke argues that the “EU notion of a DPIA falls so far short of a PIA as to raise doubts about whether it has any value as a privacy-protective mechanism.”[43]

[38] Lilian Edwards, *Law, Policy and the Internet* (Hart).

[39] Pagona Tsormpatzoudi, Bettina Berendt and Fanny Coudert, ‘Privacy by Design: From Research and Policy to Practice – the Challenge of Multi-Disciplinarity’ (Springer, Cham 2016) 204.

[40] Kroener and Wright 362.

[41] The ICO published a detailed DPIA / PIA guide on the 22nd March 2018. It was not assessed for this work.

[42] Amir Shayan Ahmadian and others, ‘Supporting Privacy Impact Assessment by Model-Based Privacy Analysis’ (2018) 8.

[43] Roger Clarke, ‘Roger Clarke’s “PIA vs. DPIA”’ (2017).

Even putting aside the criticisms of the DPIA, given that one of the goals of GDPR is to drive consistency, it seems counterproductive for several national level data protection authorities to develop and push their own DPIA tools.[44]

The biggest failing of privacy by design in the GDPR in the context of enterprise software is that is does not clearly define the role and obligations of the software developer/ vendor. The assumption that the controller always builds the software, or has complete control over the development process, is naïve. Most controllers buy software, rather than building it from scratch. While recital 78 does note, "producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products," this is thin. In the context of cloud computing, the processor may well have more power in determining whether PdD is embedded in the solution than the controller does.

11.4.4 The limits of anonymization and pseudonymization, and GDPR

Applying the computer science research of Sweeney[45], the legal scholar, Ohm challenges one of the fundamental assumptions of data protection law, that of strong anonymization. "Data can either be useful or perfectly anonymous, but never both."[46] Sweeney found that 87% (216 million of 248 million) of the population in the United States had reported characteristics that likely made them unique based only on 5-digit ZIP, gender and date of birth. Computer scientist Narayanan argued that the privacy

[44] The author is aware of 4 (UK, FR, DE and one from ENISA), but suspects there may be more.

[45] Latanya Sweeney, 'Simple Demographics Often Identify People Uniquely' (2000) 671 Health (San Francisco) 1.

[46] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1701, 1704.

regulators overplay the power of de-identification.[47] There is a lively debate with Cavoukian.[48]

Anderson, in his commentary on the draft UK ICO Anonymization Code of Practice, was also scathing, stating, "It is disgraceful that the draft Code ignores the relevant science."[49] [50] Narayanan's and Anderson's concerns are particularly challenging to the GDPR, as the GDPR makes significant reference to both pseudonymization[51] and anonymization. As Leverett et al note, "The fair-processing rule of thumb of 'consent or anonymise', namely that firms making secondary use of personal data should either get the subjects' consent or redact the data to the extent that it is no longer personal, is coming under strain from Web 2.0, as both consent and anonymization are rapidly getting less tractable in a world of big data."[52]

11.4.5 Algorithms, big data, machine learning in the GDPR

The question of whether the GDPR provides a right to an explanation of the algorithm remains vexing.[53] Edwards and Veale note that the GDPR is "restrictive, unclear, or even paradoxical concerning when any explanation-related right can be triggered." They argue that the route to algorithm

[47] Arvind Narayanan and Vitaly Shmatikov, 'Robust de-Anonymization of Large Sparse Datasets', *Proceedings - IEEE Symposium on Security and Privacy* (IEEE 2008).

[48] Ann Cavoukian and Daniel Castro, 'Big Data and Innovation, Setting the Record Straight: De-Identification Does Work' [2014] Information and Privacy Commissioner 18.

[49] Response from R Anderson draft ICO Code, at *http://www.cl.cam.ac.uk/~rja14/Papers/fipr-ico-anoncop-2012.pdf*

[50] Edwards, *Law, Policy and the Internet*. Forthcoming book by Edwards provides a robust analysis of the various weaknesses (and strengths of the GDPR).

[51] Pseudonymization is the separation of data from direct identifiers so that linkage to an identity is not possible without additional information that is held separately.

[52] Eireann Leverett, Richard Clayton and Ross Anderson, 'Standardisation and Certification of the Internet of Things' [2017] Proceedings of WEIS 1, 11.

[53] Edwards, *Law, Policy and the Internet*.

fairness is more likely to come through privacy by design, privacy impact assessments or certification. When most users do not have the time or interest to interpret website terms and conditions, it is unlikely that they would dig into the innards of algorithm structures. When the algorithm itself is beyond human comprehension, as is sometimes the case in deep learning, the difficulty becomes insurmountable.

11.4.6 Internet of Things and the GDPR

After making the valid caveat that it is problematic to analyze legislation that has not yet been applied, Lindqvist questions how GDPR will cope with the challenges of the Internet of Things (IoT), especially given the dynamic of the processor and controller relationship. She makes the valid point that the GDPR assumes the controller is the more powerful party in the controller / processor relationship, but in a complex technology supply chain, such as the IoT, the processor is offering the service, and determining the “rules”.[54] She makes the plea for clear guidance from the yet to be formed Data Protection Board. More generally, the IoT is a fertile area of legal and computer science research collaboration.

11.4.7 Blockchain and the GDPR

Finck[55] examines the tension between blockchain (distributed ledger technology) and the GDPR. She argues that the GDPR is in part outdated, even before it enters into force, as it assumes a centralized controller, which is inimical to the design of distributed ledger technology. She also notes that DLTs, when deployed correctly, can be a strong privacy enhancing technology.

[54] Lindqvist 63.

[55] Michèle Finck, ‘Blockchains and Data Protection in the European Union’ (2018) 18 Max Planck Institute for Innovation & Competition Research 1.

11.4.8 Certification

Lachaud argues that the GDPR has not created the correct framework for the certification process to be successful, as it is overly complex, with the potential for overlap and competition. It fails to learn from other certification initiatives, and it does not create effective incentives.[56]

11.4.9 Is the GDPR doomed?

Koops[57] thinks so, arguing that the GDPR is founded on 3 fallacies (too much focus on informational self-determination, too much faith in controller actions and regulating everything in one law). While this is one of the more negative assessments of the GDPR, it would be reasonable to note that many commentators have noted faults with the GPDR; some issues are significant, others minor. At the risk of judging the law before it is deployed, the GDPR is like any complex law that is crafted by committee: It is a montage of compromise. It is, however, a significant improvement on its predecessor. Its success will be determined by how it changes the behaviour of those building, controlling and processing data.

It is beyond the scope of this work to explore the impact of the GDPR on the behaviour of social media providers, such as Facebook[58] and Twitter. However, the next section will examine how the enterprise software industry has responded to GDPR to date.

[56] Eric Lachaud, ‘Why the Certification Process Defined in the General Data Protection Regulation Cannot Be Successful’ (2016) 32 Computer Law & Security Review 814.

[57] BJ Koops, ‘The Trouble with European Data Protection Law’ (2014) 4 International Data Privacy Law 250.

[58] At the time of writing, the Cambridge Analytica story was front page news.

11.5 GDPR is working in the context of enterprise software

The GDPR is already working. The threat of the large fine has moved data protection law from the corner of the library into the corner office.[59] Organizations are scrambling to hire data protection skills, databases are being inventoried, cleaned, pruned and audited, security processes tightened, standards scrutinized, consent statements are being rewritten into clearer language, processes documented, employees trained, sub-processor contracts reviewed, and software vendors are being challenged to show how their solutions are compliant. Vendors are building solutions to aid with compliance. Privacy engineering research is likely to receive more funding and interest from academic and commercial computer science.

Returning to the developer survey, it showed that most software developers had not received formal training in the EU DPD, despite being responsible for building systems that process personal or even sensitive data. Their perceptions of how their employers build privacy into product were at best mixed.

Revisiting Lessing's modalities for a moment, the longer term success of the GDPR in the enterprise software context will depend on whether it is able to catalyze shifts across all 4 modalities.

[59] The FT interviewed several large software companies. https://www.ft.com/content/5365c1fa-8369-11e7-94e2-c5b903247afd

Table 11.2: GDPR mapped to modalities

Modality	Actor	Shift
Market	Corporate end customer	Positioning GDPR compliance as a part of corporate social responsibility. GDPR compliance as a purchase. Virtue signalling.
	Software vendor	GDPR as marketing tool, vendor virtue signalling.
		Start ups focusing on GDPR relevant tools.
Social Norm	Educators	PbD taught in comp sci.
	Software vendor / regulator	Early collaboration on new technologies.
Architecture / technology	Software developer	Mainstreaming of privacy engineering and privacy impact assessments in dev process.
	Software vendor	Privacy in product supply chain. Using AI to protect privacy.
Laws	Legislators	Sectorial laws, international mimicry. Surveillance v privacy.
	Regulators	Stronger guidance and enforcement.

We will now explore this in the context of enterprise software.

11.6 Enterprise software vendor reaction to the GDPR

11.6.1 As processors

Many enterprise software vendors are processors under GDPR (for some services, they may be controllers too). They are required to comply with the obligations in the same way as any other processor. For instance, a vendor who provides payroll via cloud computing would be a processor. A scan of vendor websites[60] shows that many payroll service providers are currently revising sub-processor contracts and contracts with controllers, tightening IT security audits, updating integration techniques, adjusting internal code of conduct / employment contracts, defining breach policies and procedures, revising data retention / deletion[61] policies and procedures, training staff, defining subject access request procedures, agreeing binding corporate rules[62] and establishing PbD / PIA assessment processes.

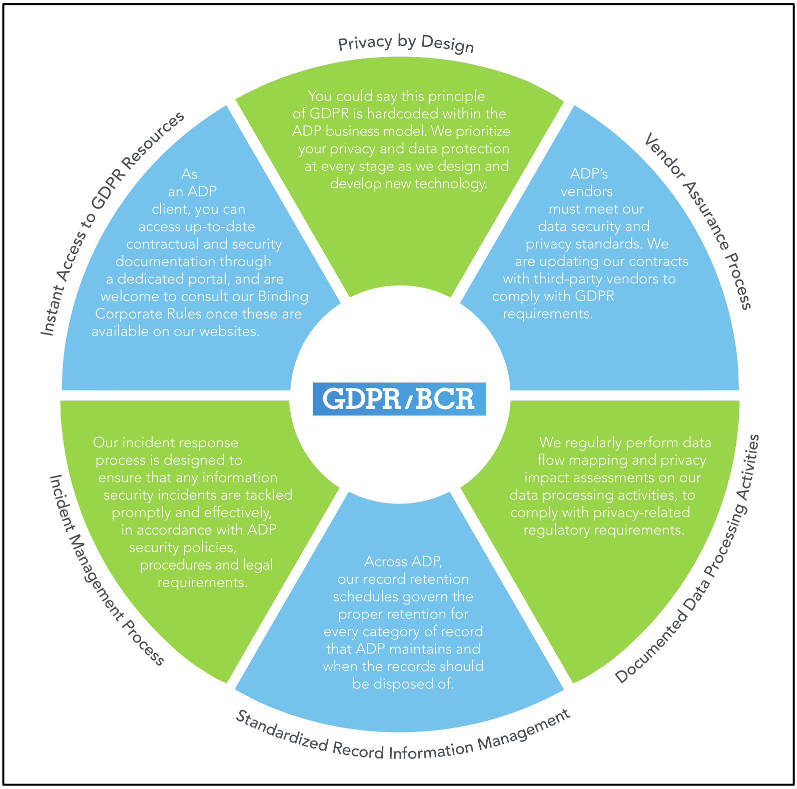
11.6.2 As vendors

As with SOX, GDPR has quickly become a marketing and sales lever. Many vendors have white papers, videos and webinars highlighting how their solutions purport to support their customers in becoming GDPR compliant. Vendors and consultants dominate web search results for GDPR. Larger vendors position both their own internal compliance efforts and their products and services. See example below from ADP.

[60] See *https://www.brightpay.co.uk/docs/17-18/gdpr/gdpr-and-the-payroll-bureau/* and *https://www.sdworx.com/en-us/prepare-your-hr-payroll-department-for-gdpr/sd-worx-statement* as examples.

[61] Payroll is an interesting example of the limitations of the right to deletion, as payroll data is often required to be held for tax and audit purposes.

[62] For instance, in early 2018, ADP agreed binding corporate rules from all 28 EU countries, both as processor and controller: *https://www.adppayroll.com.au/insights-and-resources/media-centre/enm/51040/457/1349251/adp-ranks-among-elite-handful-of-companies-worldwide-with-approved-binding-corporate-rules-for-global-data-protection*


Privacy by Design
Vendor Assurance Process
Documented Data Processing Activities
Standardized Record Information Management
Incident Management Process
Instant Access to GDPR Resources
GDPR/BCR

You could say this principle of GDPR is hardcoded within the ADP business model. We prioritize your privacy and data protection at every stage as we design and develop new technology.

ADP's vendors must meet our data security and privacy standards. We are updating our contracts with third-party vendors to comply with GDPR requirements.

We regularly perform data flow mapping and privacy impact assessments on our data processing activities, to comply with privacy-related regulatory requirements.

Across ADP, our record retention schedules govern the proper retention for every category of record that ADP maintains and when the records should be disposed of.

Our incident response process is designed to ensure that any information security incidents are tackled promptly and effectively, in accordance with ADP security policies, procedures and legal requirements.

As an ADP client, you can access up-to-date contractual and security documentation through a dedicated portal, and are welcome to consult our Binding Corporate Rules once these are available on our websites.

Figure 11.1: ADP positioning of GDPR and binding rules

The marketing machines of software vendors have been far more effective and vocal at communicating that the GDPR is coming and what it is about than the efforts of the data protection authorities. This is at the likely cost of hype, for instance in August 2017 the UK ICO noted, “Here at the ICO, we took the view that it was time to sort the fact from the fiction before the new law comes into effect on 25 May 2018, given some of the misinformation and outright scaremongering out there – some of which, it must be said, seems commercially driven."[63] Recently, the CIPP[64] in the UK lamented the lack of payroll focused guidance from the ICO[65] and the ICO has not updated its employment code of practice since 2011.

Some recruitment software vendors have also provided useful documentation about how to comply with the GDPR, for instance SmartRecruiters have a series of webinars, FAQs[66] and white papers,[67] clearly outlining how to recruit in line with the provisions of the GDPR, for example, explaining how the transparency principle is supported in the product:

> *In SmartRecruiters, for example, transparency is provided to applicants in the form of a Privacy Policy that covers acceptable access to and use of personal data. Leveraging our Compliance Interface, SmartRecruiters Customers may share with applicants their own privacy policies governing the collection and processing of an applicant's personal information as part of the job application and hiring process, enabling applicant (and data subjects) to be informed about how their data will be used.*

Moving beyond the scope of HR software, Salesforce.com for instance, has an extensive site[68] with training materials, GDPR relevant product specifications, and details of Salesforce.com's binding corporate rules agreement.

[63] See *https://iconewsblog.org.uk/2017/08/25/gdpr-is-an-evolution-in-data-protection-not-a-burdensome-revolution/*.

[64] Chartered Institute of Payroll Professionals. See payroll chapter.

[65] See *http://www.hrmagazine.co.uk/article-details/everything-you-need-to-know-about-payroll-and-gdpr*

[66] See *http://ta.smartrecruiters.com/gdpr-compliance-faq-en.html*

[67] Available via the smartrecruiters website, registration required.

[68] See *https://www.salesforce.com/gdpr/overview/*

11.6.3 Security vendors leveraging GDPR

GDPR reinforces the obligations organizations already have under other legislation and regulation to make sure data is held securely. This, like Sarbanes-Oxley did, provides a lever for security solution vendors to re-position and re-emphasize their offering. In many cases, these vendors are not building new technologies specifically for GDPR, but are using GDPR to drive a sense of urgency into the sales cycle. For instance, encrypting back-ups has been good practice for decades, but GPDR becomes the urgent driver to prioritize that investment.

The IDC notes that:

> *GDPR-related security spending presents a $2.3 billion market opportunity in 2017, and it is forecast to grow to $3.7 billion in 2019. European organizations are maturing in their GDPR readiness journey and are now ready to make investment commitments to support compliance," said Martin Whitworth, research director, IDC European Data Security and Privacy. "Many organizations are actively seeking solutions to ensure regulatory compliance as well using the regulation as a trigger to improve their organizational security stance. For vendors, simply branding products and services as GDPR-ready is unlikely to be effective. They need to help customers understand how new regulations will impact their business, showcase how their solutions can help in addressing any regulatory shortfalls, and work to improve data governance processes."*[69]

[69] See *https://www.idc.com/getdoc.jsp?containerId=EMEA42677317*

11.6.4 Start ups: The example of subject access rights

GDPR has also begun to create an opportunity for new start ups. For instance, Senzing provides a tool to help organizations discover personal information for subject access requests or other data inventory activities. Subject access rights (SAR) have existed in various forms prior to the GDPR, and Ausloos and DeWitte[70] note these have rarely been leveraged and, when applied, often face disinterest, hostility and especially incomplete responses from the controller. The GDPR creates a stronger right to access (Art. 15) and is likely to see more take up[71]. Organizations have 30 days to respond, rather than 40 under the EU DPD. Senzing suggests, based on a survey, that larger organizations expect to get an average of 246 subject access request enquiries per month, for which they will need to search an average of 43 different databases, each taking more than 7 minutes. The total time spent finding data for GDPR enquiries per month will be more than 75,500 minutes (1259 hours). This equates to nearly 60 hours of searching per working day (or 7.5 employees dedicated solely to GDPR enquiries every day).[72] The SAR then may turn out costly for organizations. Their solution uses machine learning to seek out the data subject's information, and states that is built using privacy by design principles.[73] The application of machine learning as a privacy enhancing technology is to be welcomed. The success of GDPR will not depend on stopping technology, but rather harnessing it.

[70] Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' [2018] International Data Privacy Law.

[71] A journal search could not find a firm prediction of an SAR increase in academic literature, but many law firm sites mention the likelihood of a significant SAR increase.

[72] Senzing white paper: *https://senzing.com/wp-content/uploads/2018/02/Senzing-GDPR-Report.pdf* The study is well worth reading, as it highlights a lack of preparedness by many organizations for SAR and GDPR generally.

[73] Jeff Jonas, the founder and CEO, was the co-author of the seminal PbD article, with Anne Cavoukian.

While it is too early to assess the success of GDPR, given that the law has not yet come into force, it has already shifted the focus of the enterprise software industry. It is not all doom and gloom.

11.7 Learning from SOX, payroll and accessibility

This section aims to apply the successes and failures of SOX, payroll and accessibility to GDPR, suggesting areas for intervention or focus. There are similarities that have not been adequately explored in research to date. This section also includes some tentative predictions and dispenses advice liberally.

Table 11.3: GDPR and SOX compared

Characteristic	**SOX**	**GPDR**	**Modality**
Public concern / incidents	Enron, worldcom	Snowden erc, "Creepy" social media incidents	Social norm
Increased sanction	Fines, jail time for execs	Large fines	Law
New or modified regulator	PCAOB	European Data Protection Board	Law
Software vendor marketing	Virsa, SAP, Oracle, IBM	IBM, ADP, Salesforce	Market / Architecture
Consulting / advisory marketing	Big accounting firms, systems integrators, lawyers, niche players	Big accounting firms, systems integrators, lawyers, niche players	Market
Start ups	Virsa systems, Protiviti, Approva	Senzing, Aircloak, Privitar	Market / Architecture
Confusing new standards	AS2 then AS5	WP29 automated decision making draft guidance	Law

Leverage existing standards	COBIT, COSO, ISO27001, ISO 31000, Soc 70, ITIL	ISO27001, ISO31000, BS10012:2007	Law
Cost of compliance	Under-estimated by regulators	Under-estimated by regulators	Market
Requires risk management	Mitigation of control weakness, GRC	PbD, PIA	Social norm / technology
Legislative and rule making process	Rapid	Slow	Law
Skills shortage	Internal auditors	DPOs	Market
Breach notification and communication	Section 302 and 404	Article 33 within 7 2 hours	Law
Global impact	J-SOX, German, UK and other reforms	“Gold standard”	Law, social norm
Pressure to weaken	Continuous	Likely, given lobbying history	Social norm

11.7.1 Data housekeeping, standards and risk

SOX drove organizations to document and make inventories of systems, data, processes, organizational information. At first, this was done manually, often via spreadsheets. However, over time organizations deployed tools and standards to optimize the reporting and process efforts. While secure processes alone do not ensure privacy, unsecure processes are, by definition, privacy inhibiting. Despite an extensive literature search, the author was unable to find academic research comparing SOX and GDPR. Frameworks such as COSO and COBIT, while mentioned in practitioner[74] circles, seem to be largely missing from academic or regulator discourse on privacy risk. Risk models and practices from audit and finance are mature and, while not without problems, building privacy risk tools and methods without building on the prior form would be sub-optimal.

[74] For example ISACA; see SOX chapter.

Harnessing the SOX experience would be very sensible, but simply rebranding SOX tools and processes as GDPR tools and processes will not be successful either.

11.7.2 Costs of compliance

The biggest surprise for the SEC and corporations with SOX was the cost of compliance, and it seems that GDPR will be similar. A study by EY and the International Association of Privacy Professionals in 2017 estimated that the average cost for the Fortune 500 company would be $ 16 million.[75] A PWC study across a broad number of US companies notes that 77% of organizations expect to spend over 1 million US$, with 9% of respondents saying they would spend over 10 million US$.[76] A Deloitte study noted, "Respondents repeatedly raised the challenge of interpreting the Regulation text as a key issue, and welcomed further guidance from the Article 29 Working Party (WP29).[77] The ICO's position noted above that GDPR is not burdensome and is naïve at best.

In SOX, the vagueness in the design of AS2 drove up the cost to organizations, and undermined organizations' support for SOX. It was, in part, the lack of clarity that drove up compliance cost, as organizations hired consultants, and the confusion enabled auditors to drive up fees and other audit costs. Accessibility standards creation has been slow, and only partially effective, and this has significantly impacted accessibility efforts. Driving effective standards requires funding, dedicated resources and multi-party engagement. Unless the data protection authorities move assertively to deliver practical, workable guidance that software engineers, payroll managers and marketing managers can understand and

[75] See *https://www.ft.com/content/0d47ffe4-ccb6-11e7-b781-794ce08b24dc*

[76] See *https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-gdpr-series-pulse-survey.pdf*

[77] See *https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-nwe-gdpr-benchmarking-survey-november-2017.pdf*

deploy, GDPR will quickly be seen as a bureaucratic imposition. Investment will eventually shift to avoidance and minimal compliance, rather than positive compliance.

11.7.3 The threat of big fines, and the need for a strong regulator

Both SOX and the GDPR have received intense corporate attention, largely because of the threats and sanctions that the law provides. With SOX, congress made a strong financing commitment to both the SEC[78] and the PCAOB.[79] Data protection authorities today are poorly funded, given the complex nature of data protection, and the new obligations that the GDPR places on organizations. As Swire notes pithily, cyberlaw suffers from a lack of cops.[80] To place the funding in perspective, the UK ICO spent roughly 25 million GBP in the financial year to 31 March 2017.[81] They collected roughly 20 million GBP in fees, implying a net investment by the UK government of 5 million GBP. The department is responsible not just for DP, but for 13 other laws including Freedom of Information.[82] One large company is likely to spend more on GDPR compliance than the UK Government is prepared to spend on educating and enforcing the regulation. A typical software start up receives more funding than the ICO office.

[78] The SEC has an annual budget of 1.6 billion US$

[79] The PCAOB annual budget is roughly $250 million per annum, with about 900 employees.

[80] P Swire, ‘No Cop on the Beat: Underenforcement in E-Commerce and Cybercrime’ (2009) 7 Journal on Telecommunications & High Technology Law 107.

[81] ICO website update with exact link.

[82] Given this low level of funding, the output of the ICO in terms of communications and guidance is impressive. In 2018, the budget has been increased, and the ICO has increased hiring activity.

It is a commonly held[83] view that the US has given up[84] on regulating privacy. Most software comes from US software companies so if Europe is really serious about enforcing data protection rights established in law, it will need far more enforcement and regulatory education investment than it has today.

The data protection authorities are an important element, but there is also a need for a stronger security regulator in Europe. Leverett et al also strongly argue that ENISA is significantly under-resourced. [85]

Unless the regulatory bodies at both the EU level (art 68) and national level (art 57) receive funding of an amount that will enable them to deliver on their obligations in terms of the GPDR, the success of the GDPR will be imperilled.

This work does not examine the role the GDPR plays in constraining government surveillance, but it is obvious that there is an inherent conflict between the governments' role as funder of the data protection agencies and their own surveillance initiatives, see for instance Vanberg et al, who note the challenges in reconciling the post-Brexit tensions, given the stronger surveillance regimen in the UK.[86] While the ECJ has upheld the independence of the data protection authorities, in Commission v Hungary[87], the relative investment levels in protecting citizens' privacy, as against monitoring them, is illustrative. As Barlow noted, "relying on

[83] Leverett, Clayton and Anderson 11.

[84] It is too early to tell if the recent revelations with Facebook signal a real shift.

[85] ibid 21.

[86] Aysem Diker Vanberg and Maelya Maunick, 'Data Protection in the UK Post-Brexit: The Only Certainty Is Uncertainty' (2018) 32 International Review of Law, Computers & Technology 190.

[87] C-288/12 Commission v Hungary

the government to protect your privacy is like asking a Peeping Tom to install your window blinds."[88]

11.7.4 Technical advice and guidance. Leges instituuntur cum promulgantur[89]

By moving the GDPR to a risk model, the demand for coherent technical advice from the regulator is likely to increase dramatically. The majority of guidance data coming from national authorities and the WP29 is not written with the software developer in mind. It typically targets legal experts and data controllers. In the payroll chapter, it was noted that in both the German medical insurance and UK RTI examples, the authorities provide concrete, detailed technical advice that a software developer can code to. The authorities deliver test data, and have a helpline and strong technology advisory services for software developers. In this regard, the CNIL's initiative to deliver the open source PIA tool is to be welcomed. The ICO recently published a technology strategy[90]and, while a 'technology fellowship post doc programme' will bring more technological skills, more developer centric guidance is needed.

11.7.5 Mainstreaming privacy engineering

In accessibility engineering, there is a vibrant, global community of software developers and designers creating innovative assistive technologies. There are some enlightened software companies making investments, but

[88] Dianne Murray and Karen Renaud, 'Privacy and the Citizen', *Usability in Government Systems* (Elsevier 2012). The quote is cited in many places.

[89] Concept in Roman Law, Decretum Gratiani, pt. I, c. 3, dist. VII, paraphrased as laws only come into effect once it is possible to know about them. While, as we saw earlier, ignorance of the law is no excuse, law that is not clearly explained gets a maxim too.

[90] Published in *https://ico.org.uk/media/about-the-ico/documents/2258299/ico-technology-strategy-2018-2021.pdf*

accessibility is still a niche, with most software developers and designers ignorant of the human rights of people with disabilities.

Today, privacy engineering is in a similar position.

Privacy eroding technologies are built in two ways:

Firstly, when product managers, designers and engineers deliberately design a solution to be privacy adverse, by gathering more information than the user wanted to share or deliberately confusing the user, for instance, with deliberately awkwardly phrased questions on tick boxes, or more sophisticated deceits. These are called dark patterns.[91] Designs that encourage users to share more information than they plan to are informally known as privacy Zuckering.[92]

Secondly, when product managers, designers and engineers do not consider privacy in their product design so they leave out privacy features, either through ignorance, or because of other product priorities.

Limiting or at least reducing the first scenario will require stronger regulatory intervention, greater customer awareness and vocal opprobrium. The second scenario requires, in the main, privacy aware engineers.

The challenge in the university computer science context is two-fold:

Develop and encourage leading edge research and specialized skills in privacy engineering. Privacy is technically challenging, and PET has attracted research interest since the 1990s.[93] Over the last decade, privacy

[91] See *https://darkpatterns.org/* for examples.

[92] Per darkpatterns. *https://darkpatterns.org/types-of-dark-pattern/privacy-zuckering* and orginally *https://www.eff.org/deeplinks/2010/04/facebooks-evil-interfaces*

[93] S Kenny and J Borking, ‘The Value of Privacy Engineering’, Refereed Article (2002) 1 The Journal of Information, Law and Technology (JILT) 1.

engineering research publication has grown dramatically[94] and has seen increasing research funding.[95] It is now an established research discipline. Equally promising is the high level of cross-disciplinary collaboration[96] with legal scholars and economists.[97] It is important to consider privacy engineering not only as a data model / database coding activity. Front end design will also require attention.

Provide the majority of software engineers with a basic grasp of privacy by design, and awareness. The survey showed the lack of awareness in most software developers about privacy, and it also highlighted the interest to learn. The shortage of privacy engineers has been clearly identified by industry[98] programmes such as the CMU MSIT[99] in privacy engineering. These should help meet that demand, but the more awkward challenge will be providing generalist software developers with privacy competence in the undergraduate curriculum.

One of the challenges for accessibility, still unresolved, is to build universal design into every stage of the software development cycle. PbD faces the same challenge if it is to be successful. Both require better tooling, new methods of testing and new methodologies. We need to find ways of designing and coding software that reinforces human rights, rather than undermining them.

[94] Seda Gürses and Jose M Del Alamo, ‘Privacy Engineering: Shaping an Emerging Field of Research and Practice’ (2016) 14 IEEE Security and Privacy 40, 41.

[95] See for instance *https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en*

[96] For example, the Centre for Applied Legal Studies at KIT, the OII at Oxford and COSIC at Leuven.

[97] Ross Anderson and Tyler Moore, ‘Information Security Economics – and Beyond’ in Alfred Menezes (ed), *Advances in Cryptology - CRYPTO 2007*, vol 4622 (Springer Berlin / Heidelberg 2007).

[98] Lorrie Faith Cranor and Norman Sadeh, ‘A Shortage of Privacy Engineers’ (2013) 11 IEEE Security and Privacy 77.

[99] *http://privacy.cs.cmu.edu/*

One of the frustrations with the privacy (and other laws) is translating them into a form that an engineer can code to. While there has been progress in tools that model laws, we are some distance away from an automated statute to specification capability. In the meantime, payroll provides a useful model. Critical to the success of payroll development and maintenance is the product manager. In the context of payroll, the product manager is the bridge between the lawyer or regulator and the engineer. Product managers can speak law and they can speak code, even if they do not write it.

While the product manager (PM) role is well established in software companies, it has, to date, received relatively little research or teaching attention. In most large software companies, there is a division between the product manager and the engineer. The PM creates the requirements and sets priorities, given the budget constraints, and the engineer figures out how to build it. At the risk of oversimplification, the PM says what and the engineer says how, and they argue about when.

While the GDPR talks of the controller responsibilities in Article 25, in standard software it is the product manager who needs to "Take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing". In most software companies, the person who decides what to code is not the one actually coding it.

It will be important to develop product managers who understand PbD, and are able to prioritize privacy effectively. Given the lack of formal PM teaching in universities, this will likely need to be driven at company level.

11.7.6 Start-ups and innovation

The history of the software industry is littered with examples of innovation that is directly or indirectly linked to government action. DARPA's funding of the internet is the most well known, but there are others. Regulatory behaviour can drive software investment, if not always in predictable ways. We saw in the payroll chapter how the payroll industry developed solutions for PAYE. Sarbanes-Oxley, or more precisely, the threat of sanction in SOX, created a market for new technology vendors to emerge. Compliance became "cool", and it attracted the interest of entrepreneurs and venture capitalists. The EUDPD did not drive a major wave of technology innovation, either from large tech vendors or start-ups, partly because the regulatory approach did not create a compelling sense of urgency in corporates to invest.

Venture capital funding[100] for security related start-ups has grown dramatically,[101] firms have cybersecurity practices[102] and there has been a number of privacy specific investments.[103]

[100] It is not lost on the author that VCs have funded the privacy eroding technologies too.

[101] See *https://www.csoonline.com/article/3249246/security/list-of-200-cybersecurity-startups-that-received-venture-capital-in-2017.html*

[102] For example, *https://www.bvp.com/cyber-security*

[103] For example, Senzing, Privacy Labs, *https://www.geekwire.com/2017/initialized-capital-leads-4m-round-privacy-labs-startup-helps-users-control-data/* Privitar, *https://www.privitar.com/listing/privitar-closes-16m-in-series-a-funding-as-businesses-turn-to-data-privacy-technology* Wirewheel, *https://www.prnewswire.com/news-releases/wirewheelio-secures-31-million-in-seed-round-led-by-psp-growth-and-nea-300555439.html* Protenus *http://www.healthcareitnews.com/news/cybersecurity-startup-protenus-raises-4-million-series-funding-round* MDclone *https://www.prnewswire.com/news-releases/israeli-startup-mdclone-announces-15m-funding-for-a-new-healthcare-data-paradigm-enabling-real-time-access-to-data-and-insights-with-zero-risk-to-patient-privacy-300593108.html* Integris *https://www.geekwire.com/2018/integris-raises-another-1-5m-data-privacy-intelligence-platform-gdpr-deadline-looms/* Aircloak *https://aircloak.com/* BigID. *https://bigid.com/*

Many of these start-ups are applying machine learning and other advanced techniques for privacy enhancement. There is a tendency, especially in legal research and regulator communication, to focus on the dangers of big data and other technologies, while ignoring, or downplaying, the privacy enhancing potential of those technologies. One of the positive elements of the PbD promise is that it sees technology as part of the solution. It will be important for regulators in particular to stress more of the innovation elements of PbD, rather than relegate it to a compliance checklist.

The GDPR has helped drive a wave of privacy related start-ups and shift the investment mix of the larger software companies. While responding to GDPR is a major driver, the wave of large-scale breaches, such as Equifax, mean that both the social norm and market modalities are beginning to value privacy more explicitly. The line between privacy and security is blurred, but it is reasonable to suggest that GDPR has significantly increased VC and entrepreneur interest in privacy enabling technologies. However, an online search was unable to find examples of a dedicated privacy technology fund in Europe. As part of its broader digital agenda, the EU and national governments would be well served by providing access to funding for privacy related start-ups. Larger software firms have venture arms, for instance one of the SAP venture arms, SAP.IO, invested in BigID.[104] The investment levels in privacy enabling technologies have never been as robust. As with SOX, it is likely that we will see larger software companies acquiring smaller vendors to build up GDPR relevant offerings. For instance, in 2017, SAP acquired Gigya, a customer identity management tool vendor.

[104] This solution aims to help organizations comply with the record keeping obligations of Art. 30, amongst other things.

11.7.7 Placing GDPR compliance efforts in a broader GRC context

It is stating the obvious that GDPR is not the only regulation organizations need to comply with. In the context of e-Commerce, the upcoming ePrivacy regulation is critically important, yet receives far less publicity than the GDPR is currently enjoying.[105] For GDPR compliance to become standard practice in organizations, it is likely that it will need to form part of a broader GRC framework and, as noted earlier, SOX created GRC.

Governance, briefly

The size of the potential fines makes it clear that GDPR is a board level issue. Organizations will need to treat privacy in the same way as they treat other societal impact topics, in the context of the corporate brand.[106] Organizations currently position environmental sustainability and workforce diversity in corporate sustainability annual reports. However, privacy is hereto typically missing from these models and standards.[107] More work is required to embed privacy (and GDPR) into standards such as COSO and other governance frameworks, such as the new ISO 31000. For organizations that process personal data, the investor community is likely to ask more questions about privacy compliance than has been the case until now and, in the wake of Equifax (and Facebook), about the risk that GDPR non-compliance brings. International governance instruments such as the UN Global Compact do not yet address issues relating to privacy, even though it is defined as a human right in various UN

[105] David Flint, ‘The Forgotten Regulation’ [2018] Business Law Review 27.

[106] Privacy as a brand value is not new.

[107] See *https://www.globalreporting.org*

instruments[108]. The Compact defines principles for the physical environment, but not the virtual one. Virtue signalling for privacy values will increase.[109]

Risk, briefly

While privacy risk is complex, and cannot simply be subsumed into other security risk assessments, GDPR risk cannot be viewed in a silo. The PIA for instance needs to be placed in the broader context of social risk. In examining IoT, Edwards et al[110] note the need for sustainability for design, for instance. Privacy risk must be able to be evaluated in the context of other organization risks. Economists have developed models of privacy economics[111] that have helped improve understanding of why the markets and individuals behave as they do. It is an important contribution to privacy study. To improve how privacy evaluates and understands risk, a similar outreach is required to the risk community. The PIA is a tool for assessing the risks of new forms of processing; it is not an operational compliance framework.

Compliance, briefly

As noted earlier, the significant component of GDPR compliance can be enforced by applying existing standards, tools and processes more

[108] The right to privacy is enshrined by the Universal Declaration of Human Rights, Article 12 (UN General Assembly resolution 217 A(III)), Paris, France, 10 December 1948; the International Covenant on Civil and Political Rights, Article 17 (General Assembly resolution 2200 A(XXI)), New York, 19 December 1966, UN Treaty Series, vol. 999, No. 14668, p. 171 and vol. 1057, p. 4019; the Convention on the Rights of the Child (art. 16) and others.

[109] It is no coincidence that the recent Apple operating system update featured a prominent PbD message.

[110] Lilian Edwards, Derek McAuley and Laurence Diver, 'From Privacy Impact Assessment to Social Impact Assessment,' *2016 IEEE Security and Privacy Workshops (SPW)* (IEEE 2016).

[111] Alessandro Acquisti, 'The Economics of Personal Data and the Economics of Privacy' (2010).

assertively. For instance, the GPDR tightens controls over sub-processors (Art 28). Under SOX, auditors demanded that if an organization uses a service provider to process transactions and/or host data, the organization needs to test the effectiveness of the service provider's controls. Instead of every company doing unique checks on their suppliers' controls, an audit standard is used. The modern version of this standard is called ISAE 3402[112] internationally, and SSAE 16 in the US. This in turn has 3 reports: a SOC type 1, 2 and 3. These reports provide an audit attestation of

> *Security: The system is protected against unauthorized access, use or modification;*
>
> *Availability: The system is available for operation and use as committed or agreed;*
>
> *Processing Integrity: System processing is complete, valid, accurate, timely and authorized;*
>
> *Confidentiality: Information designated as confidential is protected as committed or agreed;*
>
> *Privacy: The system's collection, use, retention, disclosure and disposal of personal information are in conformity with the commitments in the service organization's privacy notice and with criteria set forth in the Generally Accepted Privacy Principles (GAPP) issued by the AICPA and CPA Canada.*[113]

SOC 3 can create WebTrust and SysTrust reports.

This work has not examined the merits of the privacy components of SOC3, and the literature search found little mention of them in the privacy

[112] International Standard on Assurance Engagements and Standard for Statements for Attestation Engagements.

[113] https://www.ssae16professionals.com/services/soc-2/

research. Even if privacy specific elements of the controls do not exactly meet the GDPR requirements, the rest of the model will be helpful in assessing the organization's focus on secure operations.

It is likely auditors will become more interested in auditing data practices and the data inventory. Data has been seen as an asset, but unless the company can show that the data has been collected and used according to the GDPR principles, data is no longer an asset. This will be especially significant in M&A situations. Again, the techniques, processes and technologies deployed for SOX will have more than a passing relevance for GDPR compliance. Data protection authorities should seek to inform and influence audit standards. The GDPR will lead to a significant increase in audit costs for organizations with significant personal data processing activities.

It is early days for GDPR related certification and validation. There are decades of experience in IT related audits and controls that bear closer examination and assessment. GDPR compliance will be more effective if privacy values and measures are integrated into existing control processes. In computer science research, the majority of the discussion about PbD has focused on the impact of PbD on the code creation process. Equally significant, but having had less focus, is the role of PbD in operations processes. Knittl and Hommel provide a practical example of PbD in operations; [114] Rother and Schiering note issues with existing operations models for PbD.[115] There has been some analysis of how PbD may

[114] Silvia Knittl and Wolfgang Hommel, 'SERVUS@TUM: User-Centric IT Service Support and Privacy Management', *Proceedings of the 13th International Conference on European University Information Systems (EUNIS 2007), Grenoble, France, June 2007* (2007).

[115] SV Rother and Ina Schiering, *Privacy in the Life-Cycle of IT Services – an Investigation of Process Reference Models*, vol 421 (Springer, Berlin, Heidelberg 2014).

work in a DevOps environment.[116] More recently, the term SecDevOps has gained traction with vendors and in research.[117] The author was unable to find mention of privacy in a cursory scan of SecDevOps research.

The survey asked questions about the consumption of third party services via web services, and many developers under-estimated the risks involved across multiple dimensions in consuming such services. While privacy scored higher than other legal issues, only 30% saw it as a critical risk. Only 5% saw industry standards as a critical risk.

11.7.8 Practical skills shortage and developing DP as a profession / career

Figure 11.2 depicts the growth on job board postings for the terms GDPR and its French equivalent, RGPD. The search was performed using the SmartSearch tool.[118] This tool analyzes job posting data; it is based on a robust machine learning model.[119] Other searches were performed on terms such as data protection, privacy and their French equivalents. Other related terms showed significant growth, such as privacy and data protection.

[116] Michele Guerriero and others, ‘Towards DevOps for Privacy-by-Design in Data-Intensive Applications’, *Proceedings of the 8th ACM/SPEC International Conference on Performance Engineering Companion – ICPE ’17 Companion* (ACM Press 2017); Tran Quang Thanh and others, ‘Embedding Security and Privacy into the Development and Operation of Cloud Applications and Services’, *2016 17th International Telecommunications Network Strategy and Planning Symposium (Networks)* (IEEE 2016).

[117] Vaishnavi Mohan and Lotfi Ben Othmane, ‘SecDevOps: Is It a Marketing Buzzword? Mapping Research on Security in DevOps’, *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016* (IEEE 2016).

[118] SAP acquired a French software company, Multiposting, in 2015. The toolset posts jobs to thousands of job boards and other career sites. One of the multiposting tools, Smartsearch, also has the ability to search for job titles, skills and other job related data across many hundreds of thousands of job postings. As the company originally began in France, the data is mainly for France, but with a growing dataset across Europe. Details of the mechanics behind the tool can be found in the PhD thesis below.

[119] Emmanuel Malherbe, ‘Standardization of Textual Data for Comprehensive Job Market Analysis’ (Université Paris-Saclay 2016).

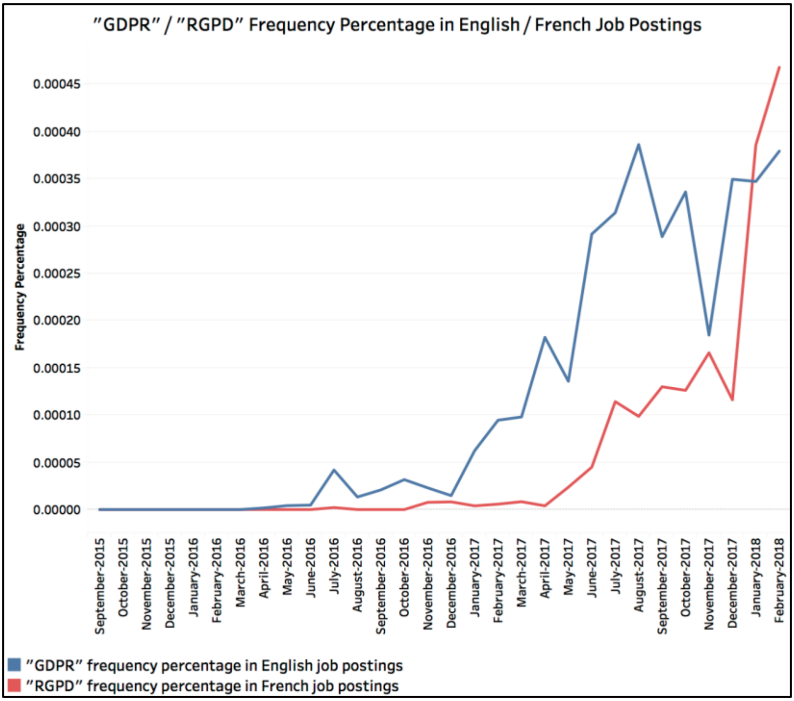


Figure 11.2: DPR job postings

It would be useful to do a robust follow-up study of the impact of GDPR on the job market for privacy and data protection related jobs across Europe to analyze time to fill, compensation trends and other job market indicators.

As with SOX, the demand for GDPR practice advice and implementation exceeds the supply of expertise. In the case of SOX, the skills shortage was with internal auditors and with IT control expertise. SOX had the advantage that audit is an established career/profession with established qualifications and skills. Also, partly on the back of the SOX demand, industry demanded better certification and professional training programmes for IT control expertise. For instance, the ISACA now offers additional privacy education. As German organizations already have the clear obligation for certified data protection officers under the BDSG, the training (*ausbildung*) for DPOs is well established, with standards organizations such as TÜV offering training and universities offering data protection training as an additional course.[120] In countries where the requirement for a data protection officer is new, the need for training will be urgent. While the regulators should not be trainers, they should encourage the development of a strong ecosystem of quality data protection related education.

A useful parallel would be the CIPP (Chartered Institute of Payroll Professionals). It provides education, community and an important professional lobbying function. The IAPP (International Association of Privacy Professionals) was formed in 2000, and offers privacy-related certifications, events and training, and it is developing into a global community. Privacy skills certification has not yet developed the maturity of audit or payroll certification, but the IAPP seems to be on the right path.

11.7.9 Global impact and the need to globalize research

SOX changed the face of global financial reporting and controls. ADA led to the UNCPRD and has influenced accessibility regulations around the world. The GPDR is already making its presence felt, even before the enforcement date, with shifts in corporate behaviour.

Kuner et al[121] note the need for more pan-European, collaborative research, “Let us hope that the GDPR will prove to be an impetus to taking a more global approach to data protection law and scholarship, and to breaking down borders.”

[120] See *https://www.cs.hm.edu/studienangebote/zusatzqualifikation/datenschutz/index.de.html*

[121] Christopher Kuner and others, ‘The GDPR as a Chance to Break down Borders’ (2017) 7 International Data Privacy Law 231.

11.8 Summary: GDPR’s chance of success

The research question that shaped this chapter asked, in the context of enterprise software, “is privacy by design, as defined in the GDPR, likely to succeed?” In one sense, it is too early to make a definitive call in that at the time of writing the law had not yet come into official effect; nevertheless, there are several indications that point to GDPR’s success, and some caveats:

- The threat of sanction has driven a sense of urgency into both vendors and end corporate customers
- Privacy engineering research is thriving
- Cross-disciplinary collaboration between legal theorists and computer scientists is well established
- Guidance from the regulators and experts will gradually reduce confusion
- Regulators are already behaving more assertively
- In the wake of recent incidents, customers’ disquiet is growing
- Practical operating standards are likely to emerge relatively quickly, given the intense industry interest and the obligations to do so under the law

The caveats:

- The regulatory bodies are not currently adequately funded to cope with the responsibility that the threat of the sanctions creates
- New technologies may threaten the underlying assumptions of the law
- A skills shortage of people who can implement GDPR processes will threaten adoption
- The cost of compliance may drive organizations to seek out avoidance tactics
- Changing and educating developers around the world will require new approaches from employers and universities

- Continued customer lethargy towards privacy in practice makes prioritizing privacy in product development difficult
- The promise of European consistency will be undermined by excessive use of the derogations

The concluding chapter will seek to place privacy in a broader ethical context. Whether the software industry provides solutions for its externalities will largely depend on how social norms inside the software industry shift.

12 Returning to Lessig, Wiesenbaum and Cicero

This final section will provide a summary and then provide some suggestions on how the enterprise software industry can be more effective in dealing with negative externalities.

This work began with the observation that the enterprise software industry has built solutions that aid legal compliance, yet it also creates externalities that undermine significant laws. Software developers are an important regulatory force, yet many do not know much about law.

Lessig's modality model provided a framework to explore the relationship between code and law in the context of enterprise software. To understand how regulation works, law, social norms, the market and technology all need examination. SOX, accessibility, payroll and privacy help illustrate the complex interplay between these modalities.

12.1 Revisiting the research questions

12.1.1 What do software developers understand about the law that relates to software?

The survey illustrated that software developers are under-trained about the laws that impact software, whether it be accessibility, privacy, intellectual property or contract. While some felt their organizations had experts to support them, the majority did not. Most expressed a desire to learn more about how law impacts software.

The interview with Nigel, who did a joint business / computer science degree, encapsulates this well:

> *Thomas: Just to make this clear, you weren't getting any exposure to any of the basics of what a contract was, any of the basics of privacy or accessibility or any of those sort of legal concepts? None of that was really taught to you in an academic context?*
>
> *Nigel: No, not at all. It was all basically computer theory and different programming languages and different algorithms and how to write other ones and a few other bits and pieces but nothing to do with what clauses to put in an end user agreement or a privacy legislation or any of the things around where data is stored or anything like that. None of that at all*
>
> *...I think generally, and this is probably the point you're going to make, is that law education at an undergraduate level, is a little bit sadly lacking. When you look at it, a lot of software has a legal ramification and it is a little bit surprising that there isn't any more education, either as optional or enforced, at any point over an undergrad degree. So, I think it's a little bit surprising and something should be done.*[1]

12.1.2 How does the software industry fail to deliver accessible solutions?

The lack of accessibility in web software is a negative externality. It undermines the human rights of people with disabilities. It makes it harder for people with disabilities to shop, to communicate and to find work. Fragmented laws, sporadically enforced; an industry largely "blind" to the market opportunities; and accessibility either ignored or treated as a tick box by many developers mean that the potential for technology to improve

[1] See Appendix E.

the lives of people with disabilities is often missed. The lab assessment empirically illustrated the concept of a negative externality.

12.1.3 How has the development of payroll software supported and influenced tax and social insurance regulations?

Payroll is a clear example of an effective state / software industry collaboration. After 60 years, it remains a dynamic market and, without it, modern tax collection would be impossible. The state has in effect co-opted software companies to collect tax, in exchange for a profitable business model. Technology expands the boundaries of what is collectable.

12.1.4 What drove the investment into software to support Sarbanes-Oxley compliance?

With Sarbanes-Oxley, the threat of massive fines and a hasty overhaul of regulations created an opportunity for the enterprise software industry to create a new market segment that is still thriving today. SOX created a market by accident, a reminder that laws often have unintended consequences and costs.

12.1.5 Is privacy by design, as defined in the GDPR, likely to succeed?

Under the EUDPD, data protection has much in common with accessibility. It has largely been ignored or marginalized in software development. A lack of coherent enforcement and apathy or antipathy from software buyers meant that architecting for privacy made little commercial sense. The last 2-3 years has seen a shift with GDPR, which brings a SOX-like sense of urgency to privacy compliance efforts. The chapter noted that there are issues with some of the assumptions in the GDPR, but it has already changed the privacy compliance focus and investment mix in enterprise software, even before it has come into force. Current regulator and press activity in the consumer software space will also change buyer and vendor behaviour in enterprise software.

From these four very different laws, patterns emerge:

- When organizations face a specific compliance demand and are prepared to invest to reduce the cost of compliance with that regulation, then the market, in the form of software vendors, will move quickly to fill that demand. Investing in compliance software is a form of virtue signalling as well as solving the compliance need.
- There has been minimal direct compliance obligation on the software vendor in law or regulation. If the buyer of the software has a regulatory obligation, then they might place pressure on the vendor to build that capability, but that is not always effective.
- Software development has focused on building compliance for a specific regulation where it is commercially expedient to do so, rather than providing a solution for broad legal principles or ethical concepts.

12.2 Reducing negative externalities in software, suggestions

12.2.1 The coders and their teachers

Left to its own devices, the software industry is unlikely to improve its negative externality track record. Security breaches continue, website accessibility has not improved markedly; indeed, as software becomes more powerful, the scope and impact of its externalities will grow in severity. When the software industry develops software that aids compliance, it is because there is a market incentive to do so.

At the time of writing, consumer software, especially Facebook, is facing its Covair[2] moment. "Go fast and break things" has lost its appeal. This work is not about consumer software, but the recent events with consumer software are likely to embolden the regulators and also shift public opinion, and perhaps even social norms. It is clear that pressure is growing to regulate parts of the software industry.

The software industry and those who work in it are faced with a choice: respond defensively and reactively to the efforts of governments to regulate or become proactive in addressing its negative externalities.

Weizenbaum raised the ethical questions about the role of the computer scientist in society long before it was commonplace to do so. Robotics and AI raise fundamental yet unanswered ethical challenges that may impact the future of humanity, and autonomous vehicles highlight the philosophical trolley problem.[3] New technologies create new ethical challenges. However, software's continued inaccessibility failing raises very awkward, fundamental human rights questions about current, more prosaic technologies. The lack of accessibility is a technical, economic and legal problem, but, at the core, it is an ethical failing too.

Reducing negative externalities will require significant changes to how those who envisage, design and build code are educated. The survey noted the lack of education in basic legal concepts, and others have also called for a code of ethics[4] and teaching[5]. There are in fact ethical codes

[2] The Covair was the GM car that prompted Ralf Nader to push for direct product safety liability in automobiles in the 1960s.

[3] Judith Jarvis Thomson, 'The Trolley Problen' (1985) 94 Yale Law journal 1395.

[4] Dinah Payne and Brett Landry, 'Similarities in Business and IT Professional Ethics: The Need for and Development of A Comprehensive Code of Ethics' (2005) 62 Journal of Business Ethics 73.

[5] Arvind Narayanan and Shannon Vallor, 'Why Software Engineering Courses Should Include Ethics Coverage' (2014) 57 Communications of the ACM 23.

for software engineers, but they have not gained traction.[6] Ethics in computer science has received growing academic attention,[7] but it has had limited impact on teaching and practitioner behaviour in comparison with medical ethics or professions such as civil or structural[8] engineering[9] or architecture. As noted earlier, business schools have compulsory ethics courses as part of MBA curricula, and ethics courses have been strengthened[10] in other financial certifications, such as the CFA.

12.2.2 Rethinking software design methodologies

Two important software design concepts are mentioned several times in this work: universal design and privacy by design (PbD).

Universal design has had a positive impact on the built world, helping move accessibility from an add-on compliance effort after design into an integral element of the initial conception. Mainstreaming universal design into enterprise software development would require the cooperation of the leading software companies and educational institutions. While design thinking has helped improve software design and usability, it has not yet

[6] Don Gotterbarn, "'Once More unto the Breach': Professional Responsibility and Computer Ethics"' (2008) 14 Science and Engineering Ethics 235; Margaret Anne Pierce and John W Henry, 'Computer Ethics: The Role of Personal, Informal, and Formal Codes' (1996) 15 Journal of Business Ethics 425.

[7] Vincent Calluzzo and Charles Cante, 'Ethics in Information Technology and Software Use' (2004) 51 Journal of Business Ethics 301; Terrell Bynum, 'Computer Ethics: Basic Concepts and Historical Overview' [2014] Stanford Encyclopedia of Philosophy; Alan J Thomson and Daniel L Schmoldt, 'Ethics in Computer Software Design and Development' (2001) 30 Computers and Electronics in Agriculture 85; Don Gotterbarn, Keith Miller and Simon Rogerson, 'Software Engineering Code of Ethics' (1997) 40 Commun. ACM 110.

[8] In Canada, since the 1920s, engineers who graduate receive a metal ring and swear an oath on graduation. The ring is symbolic of a Quebec bridge that collapsed.

[9] Hongju Yan, 'Keystone of Engineering Education - Ethics Education', *Lecture Notes in Electrical Engineering* (Springer, Berlin, Heidelberg 2011).

[10] Their effectiveness is a matter for debate, but not here.

met its inclusionary promise. The success stories mentioned in chapter 7 illustrate the potential for an industry attitude shift on accessibility.

Largely because of GDPR, PbD has received renewed attention. It will require both research and practitioner effort to take this promising concept and drive it into standard software methodologies. The pressure that GDPR brings will bring more clarity and urgency to its adoption. SOX helped drive adoption of COSO, ISO 27001 and ITIL so it is likely that GDPR will encourage broader adoption of PdD and PIA.

Both PdD and universal design, if deployed broadly, will positively impact the specific negative externalities this dissertation highlights. They also highlight the need for broader inclusion of ethical, legal and social issues in software design and build. Edwards calls for social impact assessments[11], for instance. Software developers (and their employers) are building solutions today that undermine established human rights and laws, but they lack a deployed methodological framework by which to uncover or assess these impacts, either through the prism of law or ethics. Research in this area is promising, see for instance ethics assessment frameworks, reflective design[12] and Friedman et al's value sensitive design[13], being a "theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process."[14]

Put simply, software developers need to consider human rights,[15] and they require the frameworks and mechanisms to do so effectively and consistently.

[11] Edwards, McAuley and Diver.

[12] Phoebe Sengers and others, 'Reflective Design', *Proceedings of the 4th decennial conference on Critical computing between sense and sensibility – CC '05* (ACM Press 2005).

[13] Batya Friedman and Batya, 'Value-Sensitive Design' (1996) 3 interactions 16.

[14] ibid 348.

[15] Brown and Marsden 200.

12.2.3 Code to the rescue?

Technology may actually help. Today, software is used to analyze law in a variety of contexts, for instance in helping judges with sentencing, checking contracts for errors, and seeking out precedents and case history. In the context of data protection, researchers are developing tools to help developers check compliance in design and code behaviour.[16] This is an important, if nascent, element of privacy by design, but it has broader application possibilities. Improved modelling tools will help to take concepts from statute or regulation in a form that software developers can follow. Software developers should not really have to read the raw statute, but often that is the case.[17] Accessibility tools illustrate the limitations of tools to assess compliance, especially when standards are not precise.

12.2.4 Requirements, the product manager and interpreting the law

In any larger software company, the analysis of customer requirements and creating a specification is typically not done by the person writing the code. There is a product manager who does this. As noted earlier, the role of the product manager is not well researched in computer science literature and, while research into requirements quality[18] is ongoing, it is

[16] Travis D Breaux and Annie I Anton, 'Analyzing Regulatory Rules for Privacy and Security Requirements' (2008) 34 IEEE Transactions on Software Engineering 5; Luca Compagna and others, 'How to Integrate Legal Requirements into a Requirements Engineering Methodology for the Development of Security and Privacy Patterns' (2009) 17 Artificial Intelligence and Law 1; Jeremy C Maxwell and others, 'A Legal Cross-References Taxonomy for Reasoning about Compliance Requirements' (2012) 17 Requirements Engineering 99.

[17] In the course of this work, the author spoke with several engineers who were reading the GDPR in order to figure out how to code for it.

[18] BW Boehm, 'Verifying and Validating Software Requirements and Design Specifications' (1984) 1 Software, IEEE 75; Bashar Nuseibeh and Steve Easterbrook, 'Requirements Engineering', *Proceedings of the conference on The future of Software engineering – ICSE '00* (ACM Press 2000).

well known inadequate requirements are a major cause of software failure. Developing product managers who have broad competence in IT law would seem to be an obvious intervention, but product management education in either business schools or computer science is in its infancy and lacks an IT law component.

12.2.5 Seeking out cross-disciplinary collaboration

A technology may impact multiple laws. For instance, the IoT raises both privacy[19] and accessibility[20] challenges, both requiring consideration across the software development life cycle. While at first glance accessibility and privacy seem to have very little in common, the mechanisms to resolve privacy and accessibility externalities product design are remarkably similar. A scan of IoT research, while not robust, was unable to discover research that looked at both issues. Both privacy and accessibility are concerned with how technology undermines human rights so it is curious that there is so little interdisciplinary collaboration, either academically or in industry. Similarly, auditors have spent the last 40 years researching how to audit enterprise software systems for control weaknesses. So, in order to make PbD and PIAs operationally deployable and measureable, the experience of those who have developed financial controls processes would be invaluable. Payroll illustrates how to embed mechanisms to understand complex regulations into the software build process. In one sense, this work is a call for more inter-disciplinary collaboration.

[19] Lindqvist; Johanna Virkki and Liquan Chen, ‘Personal Perspectives: Individual Privacy in the IOT’ (2013) 3 Advances in Internet of Things 21; Rolf H Weber, ‘Internet of Things: Privacy Issues Revisited’ [2015] Computer Law and Security Review.

[20] Davide Mulfari, Antonino Longo Minnolo and Antonio Puliafito, ‘Wearable Devices and IoT as Enablers of Assistive Technologies’, *2017 10th International Conference on Developments in eSystems Engineering (DeSE)* (IEEE 2017); Shadi Abou-Zahra, Judy Brewer and Michael Cooper, ‘Web Standards to Enable an Accessible and Inclusive Internet of Things (IoT)’, *Proceedings of the 14th Web for All Conference on The Future of Accessible Work – W4A ’17* (ACM Press 2017).

12.2.6 Software industry leadership

While improving the technical tools and education of developers is necessary, the software industry is unlikely to fundamentally address the negative externalities it creates unless the leadership of the software industry prioritizes that effort. While it is relatively easy to make a software company carbon neutral, and deploy profits and shareholder funds for worthy philanthropic endeavours, committing to and delivering privacy neutral or enhancing software will require significantly more effort and consistent engagement. To date, corporate social responsibility initiatives have largely concerned themselves with the physical world.[21] As Marsden notes, ambitious and profit maximizing companies still have social responsibilities towards their users as citizens.[22] As noted in the GDPR chapter, some vendors have already begun virtue signalling on privacy.

12.3 The regulators

Law is most effective when it is consistently enforced. Accessibility and privacy have both suffered from a lack of regulator follow-through and investment. In the case of accessibility, the DOJ's lack of guidelines is not only problematic for those seeking to defend the rights of people with disabilities; it generates costs and confusion for corporations. The lack of urgency in Europe to instantiate the UNCRPD means that there is still no coherent position on private sector web accessibility. The increase in sanctions with the GDPR creates the regulatory responsibility for better guidelines and consistent education and enforcement. The current funding levels of data protection agencies are inadequate for the task. The rollout

[21] See earlier discussion on CSR in the context of the UN global compact.

[22] Christopher T Marsden, 'Beyond Europe: The Internet, Regulation, and Multistakeholder Governance — Representing the Consumer Interest?' (2008) 31 Journal of Consumer Policy 115.

of RTI in the UK illustrates the positive, co-regulatory impact of vendor and government collaboration.

12.4 Peering further ahead

As software becomes part of everything, calls for tighter regulation of the software industry will grow. The pressure is likely to be highest at the intersection between the physical and the digital, in medical devices, cars, and the internet of things, but calls to more tightly regulate social media platforms are also increasing. This, in turn, will impact the enterprise software industry.

Leverrett et al note the need for a strong safety regulator, and propose an EU cyber-security regulator, to set standards, certify and enforce compliance.[23] They note we need to bring security and safety engineers together. “From autonomous cars to smart meters, and from embedded medical devices to intelligent cities, one environment after another will become software driven, and will start to behave in many ways like the software industry.”[24] The state has intervened, with varying levels of success, to reduce negative externalities in almost every industry; so, at some point, it will seek to place more direct obligations on the software industry, for instance, to build safer software. Grimmelmann notes the parallels between privacy and safety.[25]

While web accessibility law is far from clear, the UNCRPD may point the way to a more effective global approach to global regulatory frameworks, although US aversion to most things UN will make that a long road.

[23] Leverett, Clayton and Anderson.

[24] ibid 21.

[25] James Grimmelmann, ‘Privacy as Product Safety’ (2010) 19 Widener Law Journal 793.

12.5 Final words

Brown and Marsden[26] call for:

> *a new multi-disciplinary examination of code and law, incorporating socio-legal studies, economics and game theory, and inter-disciplinary information studies drawing on socio-economic and political analysis. The investigation of governance and standard setting needs increasingly to draw on these inter-disciplinary approaches.*

This work is in essence an attempt to bring a multi-disciplinary perspective to the relationship between enterprise software and laws. It has illustrated the power of software to enable compliance consistently or rapidly, and how it can undermine laws and human rights. It empirically highlighted the gaps in developer education and the negative externality of inaccessibility for blind and visually impaired users. It then applied that perspective to the GDPR.

As Weizenbaum so poignantly noted, the power of software creates great responsibility. The successful software company of the future will have to thrive in a world of stronger regulatory oversight. Those coding software must move on from naïve assumptions of technological determinism and ignorance of laws. This will require new attitudes, skills, roles, methods and strategies.

The regulators have much to learn too. If Cicero lived today, he may have said *ignorantia technologiam informationis non exucsat.*[27]

[26] Brown and Marsden 200.

[27] Thanks to Frau Sieben, my daughter’s Latin teacher, for the translation

Bibliography

Abou-Zahra S, Brewer J and Cooper M, ‘Web Standards to Enable an Accessible and Inclusive Internet of Things (IoT)’, *Proceedings of the 14th Web for All Conference on The Future of Accessible Work - W4A ‘17* (ACM Press 2017)

Acemoglu D and Angrist JD, ‘Consequences of Employment Protection? The Case of the Americans with Disabilities Act’ (2001) 109 Journal of Political Economy 915

Acquisti A, ‘The Economics of Personal Data and the Economics of Privacy’ (2010)

Adam A and Kreps D, ‘DISABILITY AND DISCOURSES OF WEB ACCESSIBILITY’ (2009) 12 Information, Communication & Society 1041

Adam S and Loutzenhiser G, ‘Integrating Income Tax and National Insurance: An Interim Report’ (2007)

Akerlof GA, ‘The Market for “Lemons”: Quality Uncertainty and the Market Mechanism’ (1970) 84 The Quarterly Journal of Economics 488

Akoumianakis D, ‘Managing Universal Accessibility Requirements in Software-Intensive Projects’ (2009) 14 Software Process Improvement and Practice 3

Albrecht JP, ‘How the GDPR Will Change the World’ (2016) 2 European Data Protection Law Review 287

Albusays K and Ludi S, ‘Eliciting Programming Challenges Faced by Developers with Visual Impairments’, *Proceedings of the 9th International Workshop on Cooperative and Human Aspects of Software Engineering – CHASE ‘16* (ACM Press 2016)

Allingham MG and Sandmo A, ‘Income Tax Evasion: A Theoretical Analysis’ (1972) 1 Journal of Public Economics 323

Alonso F and others, ‘On the Testability of WCAG 2.0 for Beginners’, *Proceedings of the 2010 International Cross Disciplinary Conference on Web Accessibility (W4A) - W4A ‘10* (2010)

Ambler T and Barrow S, ‘The Employer Brand’ (1996) 4 Journal of Brand Management 185

Anderson R, ‘Why Information Security Is Hard –
An Economic Perspective’

——, ‘Security Economics’, *Proceedings of the 28th Annual Computer Security Applications Conference - ACSAC ‘12* (ACM Press 2012)

——, ‘Measuring the Cost of Cybercrime Motivation A Framework for Analyzing the Costs of Cybercrime Fitting the Estimates into the Framework’

Anderson R, Clayton R and Moore T, ‘Security Economics and European Policy’, *WEIS 2008 - Seventh Workshop on Economics of Information Security* (2008)

Anderson R and Moore T, ‘Information Security Economics – and Beyond’ in Alfred Menezes (ed), *Advances in Cryptology - CRYPTO 2007*, vol 4622 (Springer Berlin / Heidelberg 2007)

Andrews D, Nonnecke B and Preece J, ‘Electronic Survey Methodology: A Case Study in Reaching Hard-to-Involve Internet Users’ (2003) 16 INTERNATIONAL JOURNAL OF HUMAN–COMPUTER INTER-ACTION, 185

Asakawa C, ‘What’s the Web like If You Can’t See It?’, *Proceedings of the 2005 International Cross-Disciplinary Workshop on Web Accessibility (W4A)* (ACM 2005)

Asprion PM and Knolmayer GF, 'Assimilation of Compliance Software in Highly Regulated Industries: An Empirical Multitheoretical Investigation', *Proceedings of the Annual Hawaii International Conference on System Sciences* (IEEE 2013)

Astbrink G and Tibben W, 'The Role of Public Procurement in Improving Accessibility to ICT' (2013) 63 Telecommunications Journal of Australia

Asvanund A and others, 'An Empirical Analysis of Network Externalities in Peer-to-Peer Music-Sharing Networks' (2004) 15 Information Systems Research 155

Ausloos J and Dewitte P, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' [2018] International Data Privacy Law

Backhaus K, 'Employer Branding Revisited' [2016] Organisation Management Journal

Backhaus K and Tikoo S, 'Conceptualizing and Researching Employer Branding' (2004) 9 Career Development International 501

Bainbridge SM, *The Complete Guide to Sarbanes-Oxley: Understanding How Sarbanes-Oxley Affects Your Business* (Adams Media 2007)

Baker CM, Milne LR and Ladner RE, 'StructJumper: A Tool to Help Blind Programmers Navigate and Understand the Structure of Code' (2015) 1 Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems 3043

Barlow JP, 'A Declaration of the Independence of Cyberspace, 1996' [1996] URL: http://homes. eff. org/~ barlow/Declaration-Final. html

Baron H, 'Occupational Testing of People with Disabilities: What Have We Learnt?' (1995) 3 International Journal of Selection and Assessment 207

Bäumler H and others, 'Marktwirtschaftlicher Datenschutz' (2002)

Bayer N and Pappas L, ‘Accessibility Testing: Case History of Blind Testers of Enterprise Software’ (2006) 53 Technical Communication 32

Beckman SL and Barry M, ‘Innovation as a Learning Process: Embedding Design Thinking’ (2007) 50 California Management Review 25

Beechler S and Woodward IC, ‘The Global “War for Talent’ (2009) 15 Journal of International Management 273

Bell D and Heitmueller A, ‘The Disability Discrimination Act in the UK: Helping or Hindering Employment among the Disabled?’ (2009) 28 Journal of Health Economics 465

Bender D, ‘Having Mishandled Safe Harbor, Will the CJEU Do Better with Privacy Shield? A US Perspective’ (2016) 6 International Data Privacy Law 117

Bernerth JB, ‘Perceptions of Justice in Employment Selection Decisions: The Role of Applicant Gender’ (2005) 13 International Journal of Selection and Assessment 206

Bhandari M, *Philosophical Foundations of Tax Law* (2017)

Bhowmick A and Hazarika SM, ‘An Insight into Assistive Technology for the Visually Impaired and Blind People: State-of-the-Art and Future Trends’ 149

Bieber R, Höckner K and Sauberer G, ‘Accessible Information and Accessibility through ICT: A Mega Trend Creates the Need for Quality Certificates for Web Accessibility Professionals in Europe and Beyond’, *Communications in Computer and Information Science* (Springer, Cham 2017)

Bird P, ‘LEO, the Pride of Lyons’ (1992) 14 IEEE Annals of the History of Computing 55

Birkinshaw J, ‘Introduction to “Beyond Self-Interest Revisited” by Hector Rocha and Sumantra Ghoshal’ (2006) 43 *Journal of Management Studies* 583

Bizer J, ‘Sieben Goldene Regeln Des Datenschutzes’ (2007) 31 Datenschutz und Datensicherheit - DuD 350

Black S and others, ‘Formal versus Agile: Survival of the Fittest’ (2009) 42 Computer 37

Black S, Harrison R and Baldwin M, ‘A Survey of Social Media Use in Software Systems Development’, *Proceedings of the 1st Workshop on Web 2.0 for Software Engineering - Web2SE ‘10* (ACM Press 2010)

Blanck P, ‘eQuality’ [2014] eQuality: The Struggle for Web Accessibility by Persons with Cognitive Disabilities 1

Blanck P, *eQuality: The Struggle for Web Accessibility by Persons with Cognitive Disabilities* (2014)

Blind K, Jungmittag A and Mangelsdorf A, ‘The Economic Benefits of Standardization’ (2014)

Blommestein HJ, ‘How to Restore Trust in Financial Markets?’ in Paul H Dembinski and others (eds), *Enron and World Finance: A Case Study in Ethics* (Palgrave Macmillan UK 2006)

Blume P, ‘Transborder Data Flow: Is There a Solution in Sight?’ (2000) 8 65

Boardman R and Mole A, ‘Guide to the General Data Protection Regulation’ (2016)

Boehm B, ‘A View of 20th and 21st Century Software Engineering’, *Proceedings of the 28th International Conference on Software Engineering – ICSE ‘06* (ACM Press 2006)

Boehm BW, ‘Verifying and Validating Software Requirements and Design Specifications’ (1984) 1 Software, IEEE 75

Bohman PR, ‘Teaching Accessibility and Design-for-All in the Information and Communication Technology Curriculum: Three Case Studies of Universities in the United States, England, and Austria’ (2012)

Borck R, ‘Income Tax Evasion and the Penalty Structure’ (2004) 8 Economics Bulletin

Bosak J and Sczesny S, ‘Gender Bias in Leader Selection? Evidence from a Hiring Simulation Study’ (2011) 65 Sex Roles 234

Boscarol M, ‘A List Apart ALA : For People Who Make Websites.’ (*Accessibility,* 2006) <https://alistapart.com/article/workingwithothers> accessed 9 April 2018

Bott F and others, *Professional Issues in Software Engineering* (3rd edn, Taylor & Francis Group 2001)

Boulier BL, Datta TS and Goldfarb RS, ‘Vaccination Externalities’ (2007) 7 The B.E. Journal of Economic Analysis & Policy

Bräutigam T, ‘The Land of Confusion: International Data Transfers between Schrems and the GDPR’

Breaux TD and Anton AI, ‘Analyzing Regulatory Rules for Privacy and Security Requirements’ (2008) 34 IEEE Transactions on Software Engineering 5

Brown I and Marsden CT, *Regulating Code* (2013)

Bruyère SM and others, ‘Information Technology and the Workplace: Implications for Persons with Disabilities’ (2005) 25 Disability Studies Quarterly

Brynjolfsson E and Kemerer CF, ‘Network Externalities in Microcomputer Software: An Econometric Analysis of the Spreadsheet Market’ (1996) 42 Management Science 1627

Bureau of Labor Statistics, ‘Persons with a Disability:
Labor Force Characteristics Summary’ (2017)
<https://www.bls.gov/news.release/disabl.nr0.htm>
accessed 26 October 2017

Burks TD, ‘Use of Information Technology Research Organizations as Innovation Support and Decision Making Tools’, *Southern Association for Information Systems 2006 proceedings* (2006)

Burkus D and Osula B, ‘Faulty Intel in the War for Talent: Replacing the Assumptions of Talent Management with Evidence-Based Strategies’ (2011) 3 Journal of Business Studies Quarterly 1

Buzzi MC and others, ‘Is Facebook Really “open” to All?’, *2010 IEEE International Symposium on Technology and Society* (IEEE 2010)

Bygrave LA, ‘Privacy and Data Protection: An International Perspective’ [2010] Scandinavian studies in law

Bynum T, ‘Computer Ethics: Basic Concepts and Historical Overview’ [2014] Stanford Encyclopedia of Philosophy

Caers R and Castelyns V, ‘LinkedIn and Facebook in Belgium’ (2011) 29 Social Science Computer Review 437

Calluzzo V and Cante C, ‘Ethics in Information Technology and Software Use’ (2004) 51 Journal of Business Ethics 301

Caminer DT, ‘LEO and the Computer Revolution’ (2002) 13 Computing and Control Engineering Journal 273

——, ‘Behind the Curtain at LEO: A Personal Reminiscence’ (2003) 25 Annals of the History of Computing, IEEE 3

Camp J and Wolfram C, ‘Pricing Security’, *Economics of Information Security* (2004)

Campbell-Kelly M, ‘Development and Structure of the International Software Industry, 1950-1990’ (1995) 24

——, *From Airline Reservations to Sonic the Hedgehog : A History of the Software Industry* (MIT Press 2003)

——, ‘Historical Reflections: The Rise, Fall, and Resurrection of Software as a Service.’ (2009) 52 Communications of the ACM 28

Campbell K and Loyland M, ‘Video as a Recruitment Tool at “Big Four” Public Accounting Firms: Why Video Should Be Part of Accounting Curricula’ (2013) 17 Academy of Educational Leadership Journal 95

Campbell KA, ‘Can Effective Risk Management Signal Virtue-Based Leadership?’ (2015) 129 Journal of Business Ethics 115

Carpentier M and others, ‘Recruiting Nurses through Social Media: Effects on Employer Brand and Attractiveness’ (2017) 73 Journal of Advanced Nursing 2696

Carrera L, Dunleavy P and Bastow S, ‘Understanding Productivity Trends in UK Tax Collection 1 LSE Public Policy Group Working Paper July 2009’ 1

Cavoukian A, ‘Privacy by Design – The 7 Foundational Principles – Implementation and Mapping of Fair Information Practices’ [2009] Information and Privacy Commissioner of Ontario, Canada 5

Cavoukian A and Castro D, ‘Big Data and Innovation, Setting the Record Straight: De-Identification Does Work’ [2014] Information and Privacy Commissioner 18

Chambers EG and others, ‘The War for Talent’ [1998] McKinsey Quarterly 44

Charlesworth A, ‘Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures’ (2003) 54 Hastings LJ 931

Chen P, Deng X and Liu F, ‘A New Explanation of Tax Evasion Behavior Based on Prospect Theory’ [2007] Proceedings of 2007 International Conference on Public Administration (3rd), Vol II 944

Chisholm W and May M, *Universal Design for Web Applications: Web Applications That Reach Everyone* (2008)

Chittenden F, Kauser S and Poutziouris P, ‘PAYE-NIC Compliance Costs: Empirical Evidence from the UK SME Economy’ 635

Clarke R, ‘Roger Clarke’s “PIA vs. DPIA”‘ (2017)

Clarke R, ‘Privacy Impact Assessment: Its Origins and Development’ (2009) 25 Computer Law and Security Review 123

——, ‘An Evaluation of Privacy Impact Assessment Guidance Documents’ (2011) 1 International Data Privacy Law 111

Cliffe S, ‘Human Resources - Winning the War for Talent’

Clifford J, ‘The UN Disability Convention and Its Impact on European Equality Law’ (2011) 6 The Equal Rights Review 11

Coase RH, ‘The Problem of Social Cost’ (1960) 3 The Journal of Law and Economics 1

Coelho CA, De Mello JMP and Funchal B, ‘The Brazilian Payroll Lending Experiment’ (2012) 94 Review of Economics and Statistics 925

Coffee JC, ‘Gatekeeper Failure and Reform: The Challenge of Fashioning Relevant Reforms’ (2004) 160 Virginia Law Review 717

Cohen SL, ‘The Basis of Sex-Bias in the Job Recruitment Situation’ (1976) 15 Human Resource Management 8

Coleman R and others, ‘From Margins to Mainstream’, *Inclusive Design* (Springer London 2003)

Colesky M, Hoepman J-H and Hillen C, ‘A Critical Analysis of Privacy Design Strategies’, *2016 IEEE Security and Privacy Workshops (SPW)* (IEEE 2016)

Coletta A and Bruyère SM, ‘Disability and Employment: New Directions for Industrial and Organizational Psychology’

Compagna L and others, ‘How to Integrate Legal Requirements into a Requirements Engineering Methodology for the Development of Security and Privacy Patterns’ (2009) 17 Artificial Intelligence and Law 1

Couper MP, Traugott MW and Lamais MJ, ‘Web Survey Design and Administration’ (2001) 65 Public Opinion Quarterly 230

Courtpozanis A and Grießmann B, ‘Test von 30 Online-Jobbörsen auf Barrierefreiheit’ (2007)

Cranor LF and Sadeh N, ‘A Shortage of Privacy Engineers’ (2013) 11 IEEE Security and Privacy 77

Curedale, *Design Thinking: Process and Models* (3rd edn, DCC 2016)

Dahlman, ‘The Problem of Externality’ (1979) 22 The Journal of Law and Economics 141 162

Dammann U and Simitis S, *Bundesdatenschutzgesetz* (Nomos 2014)

DATEV, 'Chronologischer Überblick 1966 bis 1975' <https://www.datev.de/web/de/m/ueber-datev/das-unternehmen/geschichte/chronologischer-ueberblick-1966-bis-1975/> accessed 15 September 2017

DeKay S, 'Peering Through Glassdoor.Com What Social Media Can Tell Us About Employee Satisfaction', *CCI Conference on Corporate Communication 2013* (2013)

DeLancey L, 'Assessing the Accuracy of Vendor-Supplied Accessibility Documentation' (2015) 33 Library Hi Tech 103

Demsetz H, 'The Core Disagreement between Pigou, the Profession, and Coase in the Analyses of the Externality Question' (1996) 12 European Journal of Political Economy 565

Desrumaux P, De Bosscher S and Léoni V, 'Effects of Facial Attractiveness, Gender, and Competence of Applicants on Job Recruitment' (2009) 68 Swiss Journal of Psychology 33

Dever JA, Rafferty A and Valliant R, 'Internet Surveys: Can Statistical Adjustments Eliminate Coverage Bias?', *Survey Research Methods* (2008)

Diker Vanberg A and Maunick M, 'Data Protection in the UK Post-Brexit: The Only Certainty Is Uncertainty' (2018) 32 International Review of Law, Computers & Technology 190

Dineen BR and Noe RA, 'Effects of Customization on Application Decisions and Applicant Pool Characteristics in a Web-Based Recruitment Context' (2009) 94 Journal of Applied Psychology 224

DRC, 'Web Access and Inclusion for Disabled People' (2004)

Easterbrook FH, ‘Cyberspace and the Law of the Horse’ (1996) 207 University of Chicago Legal Forum

Easton C, ‘The Web Content Accessibility Guidelines 2.0: An Analysis of Industry Self-Regulation’ (2011) 19 International Journal of Law and Information Technology 74

——, ‘Revisiting the Law on Website Accessibility in the Light of the UK’s Equality Act 2010 and the United Nations Convention on the Rights of Persons with Disabilities’ (2012) 20 International Journal of Law and Information Technology 19

Edler J and Georghiou L, ‘Public Procurement and Innovation-Resurrecting the Demand Side’ (2007) 36 Research Policy 949

Edlin AS and Karaca-Mandic P, ‘The Accident Externality from Driving’ (2006) 114 Journal of Political Economy 931

Edwards L, *Law, Policy and the Internet* (Hart)

——, ‘The Internet and Security: Do We Need a Man with a Red Flag Walking in Front of Every Computer’ (2007) 4 SCRIPTed: A Journal of Law, Technology and Society

Edwards L, McAuley D and Diver L, ‘From Privacy Impact Assessment to Social Impact Assessment’, *2016 IEEE Security and Privacy Workshops (SPW)* (IEEE 2016)

Eisma R and others, ‘Early User Involvement in the Development of Information Technology-Related Products for Older People’ (2004) 3 Universal Access in the Information Society 131

Eldridge SW and Kealey BT, ‘SOX Costs: Auditor Attestation under Section 404’

Ellickson RC, ‘Law and Economics Discover Social Norms’ (1998) 27 Journal of Legal Studies 537

Elving WJL and others, ‘The War for Talent? The Relevance of Employer Branding in Job Advertisements for Becoming an Employer of Choice’ (2013) 20 Journal of Brand Management 355

Ergenoglu AS, ‘Universal Design Teaching in Architectural Education’ (2015) 174 Procedia – Social and Behavioral Sciences 1397

Eurostat, ‘Disability Statistics - Labour Market Access’ [2014] 2014

Fan W and Yan Z, ‘Factors Affecting Response Rates of the Web Survey: A Systematic Review’ (2010) 26 Computers in Human Behavior 132

Feld LP and Frey BS, ‘Tax Compliance as the Result of a Psychological Tax Contract: The Role of Incentives and Responsive Regulation’ (2007) 29 Law and Policy 102

Feldman DC and Klaas BS, ‘Internet Job Hunting: A Field Study of Applicant Experiences with On-Line Recruiting’ (2002) 41 Human Resource Management 175

Ferri D, Giannoumis GA and Edward O’Sullivan C, ‘Fostering Accessible Technology and Sculpting an Inclusive Market through Regulation’ (2015) 29 *International Review of Law, Computers and Technology* 81

Ferry G, *A Computer Called Leo* (2nd edn, Harper Perennial 2004)

Fiedler AM, ‘Adverse Impact on Hispanic Job Applicants during Assessment Center Evaluations’ (2001) 23 Hispanic Journal of Behavioral Sciences 102

Finck M, ‘Blockchains and Data Protection in the European Union’ (2018) 18 Max Planck Institute for Innovation & Competition Research 1

Firth DR and Swanson EB, ‘How Useful Are IT Research and Analysis Services?’ (2005) 48 Business Horizons 151

Flint D, ‘The Forgotten Regulation’ [2018] Business Law Review 27

Frasca KJ and Edwards MR, ‘Web-Based Corporate, Social and Video Recruitment Media: Effects of Media Richness and Source Credibility on Organizational Attraction’ (2017) 25 International Journal of Selection and Assessment 125

Fricker RD and Schonlau M, ‘Advantages and Disadvantages of Internet Research Surveys: Evidence from the Literature’ (2002) 14 Field Methods 347

Friedman B, ‘Value-Sensitive Design’ (1996) 3 interactions 16

Friedman B and Batya, ‘Value-Sensitive Design’ (1996) 3 interactions 16

Fröhlich M, Kahmann J and Kadmon M, ‘Development and Psychometric Examination of a German Video-Based Situational Judgment Test for Social Competencies in Medical School Applicants’ (2017) 25 International Journal of Selection and Assessment 94

Ganassali S, ‘The Influence of the Design of Web Survey Questionnaires on the Quality of Responses’ (2008) 2 Survey Research Methods 21

Gapper J, ‘Comment on Sumantra Ghoshal’s “Bad Management Theories Are Destroying Good Management Practices”’ (2005) 4 Academy of Management Learning and Education 101

Gartner, ‘Gartner Says Global IT Spending to Reach $3.7 Trillion in 2018’ <https://www.gartner.com/newsroom/id/3845563> accessed 28 February 2018

——, ‘SAP Fills Its Compliance Gap With Virsa Acquisition Deal’ (2006)

Gaucher D, Friesen J and Kay AC, ‘Evidence That Gendered Wording in Job Advertisements Exists and Sustains Gender Inequality’ (2011) 101 Journal of Personality and Social Psychology 109

Gay G and Li CQ, ‘AChecker’, *Proceedings of the 2010 International Cross Disciplinary Conference on Web Accessibility (W4A) - W4A ‘10* (ACM Press 2010)

Gellert R, ‘Understanding the Notion of Risk in the General Data Protection Regulation’ *Computer Law and Security Review* (2018)

Ghoshal S, ‘Bad Management Theories Are Destroying Good Management Practices’ (2005) 33 IEEE Engineering Management Review 79

Glen R, Suciu C and Baughn C, ‘The Need for Design Thinking in Business Schools’ (2014) 13 Academy of Management Learning & Education 653

Godwin M, ‘Compliance Costs – The Cost of Paying Tax’ (1978) 6 Omega 389

Goldberg, ‘Automatic Tax Withholding’ (*Washington Post*, 2013) <http://www.aei.org/publication/automatic-tax-withholding/> accessed 14 September 2017

Goldsmith J, ‘Regulation of the Internet: Three Persistent Fallacies’ (1997) 73 Chicago-Kent Law Review

Goldsmith S, *Designing for the Disabled: The New Paradigm* (Architectural Press 1997)

Gordon JN, ‘What Enron Means for the Management and Control of the Modern Business Corporation: Some Initial Reflections.’ (2002) 69 The University of Chicago Law Review

Gotterbarn D, '"Once More unto the Breach': Professional Responsibility and Computer Ethics" ' (2008) 14 Science and Engineering Ethics 235

Gotterbarn D, Miller K and Rogerson S, 'Software Engineering Code of Ethics' (1997) 40 Commun. ACM 110

Graham C, Litan R and Sukhtankar S, 'The Bigger They Are, The Harder They Fall: An Estimate of the Costs of the Crisis in Corporate Governance' (2002)

Grant H, 'Data Protection 1998-2008' (2009) 25 Computer Law and Security Review 44

Greenleaf G, 'An Endnote on Regulating Cyberspace: Architecture vs Law?' (1998) 21

Greenleaf G, 'Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey'

Griffin D and others, 'A Comparison of Self-Esteem and Job Satisfaction of Adults with Mild Mental Retardation in Sheltered Workshops and Supported Employment' (1996) 31 Education and Training in Mental Retardation and Developmental Disabilities 142

Grillo FDN, Fortes RP de M and Lucrédio D, 'Towards Collaboration between Sighted and Visually Impaired Developers in the Context of Model-Driven Engineering', *First Workshop on Graphical Modeling Language Development* (2012)

Grimmelmann J, 'Regulation by Software' 1719

——, 'Privacy as Product Safety' (2010) 19 Widener Law Journal 793

Grobe E, 'Employer Branding' (2008)

Guerriero M and others, ‘Towards DevOps for Privacy-by-Design in Data-Intensive Applications’, *Proceedings of the 8th ACM/SPEC International Conference on Performance Engineering Companion – ICPE ‘17 Companion* (ACM Press 2017)

Guillory J and Hancock JT, ‘The Effect of LinkedIn on Deception in Resumes’ (2012) 15 Cyberpsychology, Behavior, and Social Networking 135

Gunderson J, ‘Functional Accessibility Testing Using Best Practices’, *Proceedings of the 5th International Conference on Universal Access in Human-Computer Interaction. Addressing Diversity. Part I: Held as Part of HCI International 2009* (Springer-Verlag 2009)

Gupta PP and Leech T, ‘Making Sarbanes – Oxley 404 Work: Reducing Cost, Increasing Effectiveness’ (2006) 3 International Journal of Disclosure and Governance 27

Gürses S and Del Alamo JM, ‘Privacy Engineering: Shaping an Emerging Field of Research and Practice’ (2016) 14 IEEE Security and Privacy 40

Guyton JL and others, ‘The Effects of Tax Software and Paid Preparers on Compliance Costs’ (2005) 58 National Tax Journal 439

Hall HK, ‘Restoring Dignity and Harmony to United States-European Union Data Protection Regulation’ (2018) 23 Communication Law and Policy 125

Hanlon CL, ‘Recruiting G.I. Jane: An Analysis of the United States Military’s Advertising Messages on Recruitment Websites’ (2016)

Hardy G, ‘Guidance on Aligning COBIT, ITIL and ISO 17799’ (2006) 1 Information Systems Control Journal 32

Harper S and Yesilada Y, *Web Accessibility: A Foundation for Research* (Springer UK 2008)

Hay M, ‘Strategies for Survival in the War of Talent’ (2002) 7 Career Development International 52

Heim K, ‘The War for Talent’ (2012) 2 MTZ industrial 72

Henderson JV, ‘Externalities in a Spatial Context’ (1977) 7 Journal of Public Economics 89

Hendrick E, ‘What Are the Pros and Cons of Using Video for Recruitment?’ (2011) 10 Strategic HR Review shr. 2011.37210faa.006

Hendriks N, Truyen F and Duval E, ‘Designing with Dementia: Guidelines for Participatory Design Together with Persons with Dementia’, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Springer, Berlin, Heidelberg 2013)

Heyer K, *Rights Enabled: The Disability Revolution, from the US, to Germany and Japan, to the United Nations* (University of Michigan 2015)

Heyer KC, ‘The ADA on the Road: Disability Rights in Germany’ (2002) 27 Law & Social Inquiry 723

Heylighen A, Van der Linden V and Van Steenwinkel I, ‘Ten Questions Concerning Inclusive Design of the Built Environment’ (2017) 114 Building and Environment 507

Hijmans H and Scirocco A, ‘Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty Be Expected to Help?’ (2009) 46 Common Market Law Review 1485

HMRC, ‘Real Time Information (RTI): Improving the Operation of Pay As You Earn’ (2014)

——, ‘Overview of Making Tax Digital – GOV.UK’ (2017) <https://www.gov.uk/government/publications/making-tax-digital/overview-of-making-tax-digital> accessed 14 September 2017

Hochberg Y V, Sapienza P and Vissing-Jorgensen A, ‘A Lobbying Approach to Evaluating the Sarbanes-Oxley Act of 2002’ (2009) 47 Journal of Accounting Research 519

Holm L and Halkier B, ‘EU Food Safety Policy’ [2009] European Societies

Hon WK, Millard C and Walden I, ‘Who Is Responsible for “Personal Data” in Cloud Computing? The Cloud of Unknowing, Part 2’ (2012) 2 International Data Privacy Law 3

Hornung G, ‘Regulating Privacy Enhancing Technologies: Seizing the Opportunity of the Future European Data Protection Framework’ (2013) 26 Innovation 181

Horton S and Quesenbery W, *A Web for Everyone: Designing Accessible User Experiences* (Rosenfeld Media 2014)

Hosein I, Tsiavos P and Whitley EA, ‘Regulating Architecture and Architectures of Regulation: Contributions from Information Systems’, *Regulating architecture and architectures of regulation: contributions from information systems. International review of law, computers & technology* (Taylor & Francis Group 2002)

Houlder V, ‘Payroll Reforms Help UK to Close Tax Gap’ *Financial Times* (2016)

Hsu CL and Lin JCC, ‘Acceptance of Blog Usage: The Roles of Technology Acceptance, Social Influence and Knowledge Sharing Motivation’ (2008) 45 Information and Management 65

Huang HW, Raghunandan K and Rama D, ‘Audit Fees for Initial Audit Engagements before and after Sox’ (2009) 28 Auditing 171

Ishii K, ‘Code Governance’ (Berlin 2005)

Iversen EJ and Tee R, ‘Standards Dynamics and Industrial Organization in the Mobile Telecom Sector’ (2006) 8 info 33

Jobst B and others, ‘The Faith-Factor in Design Thinking: Creative Confidence Through Education at the Design Thinking Schools Potsdam and Stanford?’, *Design Thinking Research* (Springer Berlin Heidelberg 2012)

Johansson-Sköldberg U, Woodilla J and Çetinkaya M, ‘Design Thinking: Past, Present and Possible Futures’ (2013) 22 Creativity and Innovation Management 121

Johnson DR and Post DG, ‘Law And Borders – The Rise of Law in Cyberspace’

Justesen T and Justesen T, ‘An Analysis of the Development and Adoption of the United Nations Convention Recognizing the Rights of Individuals with Disabilities: Why the United States Refuses to Sign this UN Convention.’ (2007) 14 Human Rights Brief 36

Kane SK, Morris MR and Wobbrock JO, ‘Touchplates: Low-Cost Tactile Overlays for Visually Impaired Touch Screen Users’, *Proceedings of the 15th International ACM SIGACCESS Conference on Computers and Accessibility* (2013)

Kannan K, ‘An Economic Analysis of Market for Software Vulnerabilities’ (2004)

Kapsi M and others, ‘The Usability of Web Accessibility Guidelines: An Approach for Evaluation’ in Constantine Stephanidis (ed), *Universal Access in Human-Computer Interaction. Applications and Services,* vol 5616 (Springer Berlin / Heidelberg 2009)

Katz ML and Shapiro C, ‘Technology Adoption in the Presence of Network Externalities’ (1986) 94 Journal of Political Economy 822

Kemmerer CH and Shawver TJ, ‘Tyco: A Top-Down Approach to Ethical Failure’ [2007] SSRN Electronic Journal

Kenny S and Borking J, ‘The Value of Privacy Engineering’, Refereed Article (2002) 1 The Journal of Information, Law and Technology (JILT) 1

Kerr DS and Murthy US, ‘The Importance of the COBIT Framework IT Processes for Effective Internal Control over Financial Reporting in Organizations: An International Survey’ (2013) 50 Information and Management 590

Kim GS, Park SB and Oh J, ‘An Examination of Factors Influencing Consumer Adoption of Short Message Service (SMS)’ (2008) 25 Psychology and Marketing 769

Kimbell L, ‘Rethinking Design Thinking: Part I’ 3 Design and Culture 285

Kirchmaier Owen, Geoffrey and Grant, Jeremy T, ‘Corporate Governance in the US and Europe: Where Are We Now?’ (2005)

Kleven HJ, Kreiner CT and Saez E, ‘Why Can Modern Governments Tax So Much? An Agency Model of Firms as Fiscal Intermediaries’ (2016) 83 Economica 219

Klitou D, ‘A Solution, But Not a Panacea for Defending Privacy: The Challenges, Criticism and Limitations of Privacy by Design’ (2014)

Knittl S and Hommel W, ‘SERVUS@TUM: User-Centric IT Service Support and Privacy Management’, *Proceedings of the 13th International Conference on European University Information Systems (EUNIS 2007), Grenoble, France, June 2007* (2007)

Köbsell S, 'Towards Self-Determination and Equalization: A Short History of the German Disability Rights Movement' (2006) 26 Disability Studies Quaterly o. A.

Kock M, 'Disability Law in Germany: An Overview of Employment, Education and Access Rights' (2002) 5 German Law Journal 1373

Koops B-J, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250

Krechmer K and Baskin E, 'The Fundamental Nature of Standards: Technical Perspective' (2000) 38 IEEE Communications Magazine 70

Krings F and Olivares J, 'At the Doorstep to Employment: Discrimination against Immigrants as a Function of Applicant Ethnicity, Job Type, and Raters' Prejudice' (2007) 42 International Journal of Psychology 406

Krishnan J, Krishnan J and Song H, 'The Effect of Auditing Standard No. 5 on Audit Fees' (2011) 30 AUDITING: A Journal of Practice & Theory 1

Kroener I and Wright D, 'A Strategy for Operationalizing Privacy by Design' (2014) 30 Information Society 355

Kude T, Dibbern J and Heinzl A, 'Why Do Complementors Participate? An Analysis of Partnership Networks in the Enterprise Software Industry' (2012) 59 IEEE Transactions on Engineering Management 250

Kulesza J, 'Transboundary Data Protection and International Business Compliance' (2014) 4 International Data Privacy Law 298

Kumler T and others, 'Enlisting Employees in Improving Payroll-Tax Compliance: Evidence from Mexico' (2013)

Kuner C and others, 'The GDPR as a Chance to Break down Borders' (2017) 7 International Data Privacy Law 231

Lachaud E, ‘Why the Certification Process Defined in the General Data Protection Regulation Cannot Be Successful’ (2016) 32 Computer Law & Security Review 814

Langer M and others, ‘Dear Computer, Teach Me Manners: Testing Virtual Employment Interview Training’ (2016) 24 International Journal of Selection and Assessment 312

Larissa-Margareta B and Ramona-Anca N, ‘A Neuroeconomic Approach of Tax Behavior’ (2012) 1 Annals of Faculty of Economics 649

Latzel J and others, ‘Perspektivwechsel Im Employer Branding’, *Perspektivwechsel im Employer Branding* (2015)

Law CM, ‘Responding to Accessibility Issues in Business’ (RMIT Australia 2010)

——, ‘Unresolved Problems in Accessibility and Universal Design Guidelines’ (2007) 15 Ergonomics in Design: The Quarterly of Human Factors Applications 7

Lawson A, ‘The EU Rights Based Approach to Disability: Strategies for Shaping an Inclusive Society’ (2005) 6 International Journal of Discrimination and the Law 269

——, ‘The United Nations Convention on the Rights of Persons with Disabilities: New Era or False Dawn’ (2006) 34 Syracuse Journal of International Law and Commerce

Lazar J, Goldstein D (Lawyer) and Taylor A, *Ensuring Digital Accessibility through Process and Policy*

Lazar J, Olalere A and Wentz B, ‘Investigating the Accessibility and Usability of Job Application Web Sites for Blind Users’ (2012) 7 Journal of Usability Studies 68

Lee I, ‘The Evolution of E-Recruiting: A Content Analysis of Fortune 100 Career Web Sites’ (2005) 3 Journal of Electronic Commerce in Organizations 57

Lessig L, *The Architecture of Privacy*, vol 1 (1998)

——, *Code and Other Laws of Cyberspace* (Basic Books 1999)

——, ‘The Limits in Open Code: Regulatory Standards and the Future of the Net’ 759

Leverett E, Clayton R and Anderson R, ‘Standardisation and Certification of the ‘Internet of Things’’ [2017] Proceedings of WEIS 1

Lidwell W, Holden K and Butler J, *Universal Principles of Design: 100 Ways to Enhance Usability, Influence Perception, Increase Appeal, Make Better Design Decisions, and Teach through Design* (Rockport Publishers 2003)

Lindqvist J, ‘New Challenges to Personal Data Processing Agreements: Is the GDPR Fit to Deal with Contract, Accountability and Liability in a World of the Internet of Things?’ (2017) 26 International Journal of Law and Information Technology 45

Lloyd I, *Information Technology Law* (2014)

Long WJ and Quek MP, ‘Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise’ (2002) 9 Journal of European Public Policy 325

Ludi S and others, ‘Teaching Inclusive Thinking to Undergraduate Students in Computing Programs’, *Proceedings of the 49th ACM Technical Symposium on Computer Science Education – SIGCSE ‘18* (ACM Press 2018)

Luo N, Zhou Y and Shon J, ‘Employee Satisfaction and Corporate Performance: Mining Employee Reviews on Glassdoor.com’ [2016] ICIS 2016 Proceedings

Lutterbeck B, ‘IT and Society: One Theory to Rule Them All?’ (2006) 4 Poiesis & Praxis: International Journal of Technology Assessment and Ethics of Science 1

Madia SA, ‘Best Practices for Using Social Media as a Recruitment Strategy’ (2011) 10 Strategic HR Review 19

Malherbe E, ‘Standardization of Textual Data for Comprehensive Job Market Analysis’ (Université Paris-Saclay 2016)

Manders B, De Vries HJ and Blind K, ‘ISO 9001 and Product Innovation: A Literature Review and Research Framework’ (2016) 48–49 Technovation 41

Marlow J and Dabbish L, ‘Activity Traces and Signals in Software Developer Recruitment and Hiring’, *Proceedings of the 2013 Conference on Computer Supported Cooperative Work - CSCW ‘13* (ACM Press 2013)

Marsden CT, ‘Beyond Europe: The Internet, Regulation, and Multistakeholder Governance—Representing the Consumer Interest?’ (2008) 31 Journal of Consumer Policy 115

Martin RL, *Design of Business: Why Design Thinking is the Next Competitive Advantage* (Harvard Business Press 2009)

Martins LL and Parsons CK, ‘Effects of Gender Diversity Management on Perceptions of Organizational Attractiveness: The Role of Individual Differences in Attitudes and Beliefs.’ (2007) 92 Journal of Applied Psychology 865

Mathieu L and others, ‘The Distribution of UK Personal Income Tax Compliance Costs’ (2010) 42 Applied Economics 351

Mattmüller, Roland; Hugo Grote, Jasper; Reif, Marcus K.; Buckmann, Jörg; Hesse, Gero; Mahlodji, Ali; Diercks, Joachim; Kupka, Kristof; Flohr, Benita; Bender J, 'Fallstudien zu Aktuellen Herausforderungen im Employer Branding und Personalmarketing', *Perspektivwechsel im Employer Branding* (2015)

Maxwell JC and others, 'A Legal Cross-References Taxonomy for Reasoning about Compliance Requirements' (2012) 17 Requirements Engineering 99

Mayer-Schonberger V, 'Demystifying Lessig' (2008) 2008 Wisconsin Law Review

Mayerson A, 'The History of Americans with Disabilities Act: A Movement Perspective' (*Disability Rights Education & Defense Fund*, 1992) <https://dredf.org/news/publications/the-history-of-the-ada/> accessed 28 August 2017

McDonnell A, 'Still Fighting the "War for Talent"? Bridging the Science Versus Practice Gap' (2011) 26 Journal of Business and Psychology 169

McEwan T and Weerts B, 'ALT Text and Basic Accessibility', *Proceedings of the 21st British HCI Group Annual Conference on People and Computers: HCI...but not as we know it - Volume 2* (British Computer Society 2007)

Mealin S and Murphy-Hill E, 'An Exploratory Study of Blind Software Developers', *Proceedings of IEEE Symposium on Visual Languages and Human-Centric Computing, VL/HCC* (IEEE 2012)

Medema SG and Samuels WJ, 'Ronald Coase and Coasean Economics: Some Questions, Conjectures and Implications' [1997] The economy as a process of valuation 72

Meinel C, Leifer L and Plattner H (eds), *Design Thinking* (Springer Berlin Heidelberg 2011)

Meiselwitz G and Wentz B*, Universal Usability: Past, Present, and Future*, vol 3 (Now Publishers, Inc 2010)

Merhout JW and Buchman SE, ‘Requisite Skills and Knowledge for Entry-Level IT Auditors’ (2007) 18 Journal of Information Systems Education 469

Miao M and others, ‘Tactile Paper Prototyping with Blind Subjects’, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Springer, Berlin, Heidelberg 2009)

Michaels E, Handfield-Jones H and Axelrod B, ‘The War For Talent: Harvard Business School Press’ [2001] MA., USA

Mintzberg H, ‘How Inspiring. How Sad. Comment on Sumantra Ghoshal’s Paper’ 108

Mohan V and Ben Othmane L, ‘SecDevOps: Is It a Marketing Buzzword? Mapping Research on Security in DevOps’, *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016* (IEEE 2016)

Moore R, ‘Standardisation: A Tool for Addressing Market Failure within the Software Industry’ (2013) 29 Computer Law and Security Review 413

Moss-Racusin CA and others, ‘Science Faculty’s Subtle Gender Biases Favor Male Students’ (2012) 109 Proceedings of the National Academy of Sciences of the United States of America 16474

Mowery DC, ‘50 Years of Business Computing: LEO to Linux’ (2003) 12 The Journal of Strategic Information Systems 295

Mulfari D, Minnolo AL and Puliafito A, ‘Wearable Devices and IoT as Enablers of Assistive Technologies’, *2017 10th International Conference on Developments in eSystems Engineering (DeSE)* (IEEE 2017)

Mullen T and Malouf R, 'A Preliminary Investigation into Sentiment Analysis of Informal Political Discourse', *American Association for Artificial Intelligence. Spring Symposia* (AAAI 2006)

Mulligan D and King J, 'Bridging the Gap between Privacy and Design' (2011) 14 Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems 989

Murphy R, *The Joy of Tax* (Random House 2015)

Murray D and Renaud K, 'Privacy and the Citizen', *Usability in Government Systems* (Elsevier 2012)

NAO, 'Automatic Enrolment to Workplace Pensions' (2015)

Narayanan A and Shmatikov V, 'Robust de-Anonymization of Large Sparse Datasets', *Proceedings – IEEE Symposium on Security and Privacy* (IEEE 2008)

Narayanan A and Vallor S, 'Why Software Engineering Courses Should Include Ethics Coverage' (2014) 57 Communications of the ACM 23

Neckerman KM and Kirschenman J, 'Hiring Strategies, Racial Bias, and Inner-City Workers' (1991) 38 Social Problems 433

Neumayer E, 'Do International Human Rights Treaties Improve Respect for Human Rights?' 925

Nikolaou I, 'Social Networking Web Sites in Job Search and Employee Recruitment' (2014) 22 International Journal of Selection and Assessment 179

Nissenbaum H, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2009)

Norberg AL, *Computers and Commerce: A Study of Technology and Management at Eckert-Mauchly Computer Company, Engineering Research Associates, and Remington Rand, 1946-1957* (MIT Press 2005)

NPR interview, 'Has Accounting World Changed Since Enron? : NPR' (2005) <http://www.npr.org/templates/story/story.php?storyId=4673933> accessed 20 September 2017

Nuseibeh B and Easterbrook S, 'Requirements Engineering', *Proceedings of the Conference on The Future of Software Engineering - ICSE '00* (ACM Press 2000)

O'Donnell JB and Rechtman Y, 'Navigating the Standards for Information Technology Controls' (2005) 75 The CPA Journal 64

O'Leary DE, 'Gartner's Hype Cycle and Information System Research Issues' (2008) 9 International Journal of Accounting Information Systems 240

Ohm P, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1701

Olson J and Grudin J, 'Toward Understanding Preferences for Sharing and Privacy'

Onu D and Oats L, '"Paying Tax Is Part of Life": Social Norms and Social Influence in Tax Communications' (2016) 124 Journal of Economic Behavior and Organization 29

Otter T, 'Western Europe: The Impact of the EMU on HR and Payroll Systems' (1999) III HRIM Journal 85

——, 'Data Protection Law: The Cinderella of the Software Industry?' (2007) 23 Computer Law & Security Report 67

Oxner T and Oxner K, ‘Boom Time for Internal Audit Professionals: Thanks to the Profession’s Growing Stature, Internal Auditors Are Enjoying Higher Salaries and Greater Career Opportunities, The IIA’s Latest Job Market Survey Reports’ (2006) 63 Internal Auditor 50

Palmer A, ‘The War for Talent’ (2003) 148 The RUSI Journal 62

Parry IWH, Walls M and Harrington W, ‘Automobile Externalities and Policies’ 373

Pavlov OV, Melville N and Plice RK, ‘Mitigating the Tragedy of the Digital Commons: The Problem of Unsolicited Commercial E-Mail’ (2005) 16 Communications of the Association for Information Systems

Payne D and Landry B, ‘Similarities in Business and IT Professional Ethics: The Need for and Development of A Comprehensive Code of Ethics’ (2005) 62 Journal of Business Ethics 73

Pelling N, ‘The Case For The First Business Computer –
Nick Pelling’ (2002) <http://www.nickpelling.com/Leo1.html#Part3>
accessed 15 September 2017

Personalwirtschaft, ‘Software für Payroll’ [2015] *Personalwirtschaft*

Petrausch V and Loitsch C, ‘Accessibility Analysis of the Eclipse IDE for Users with Visual Impairment’, *Studies in Health Technology and Informatics* (2017)

Petrausch V, Seifermann S and Müller K, ‘Guidelines for Accessible Textual UML Modeling Notations’ (Springer, Cham 2016)

Peucker M, ‘Equality and Anti-Discrimination Approaches in Germany’ [2007] European Forum for Migration Studies 1

Pfeffer J, ‘Why Do Bad Management Theories Persist? A Comment on Ghoshal’ (2005) 4 Academy of Management Learning and Education 96

Pickhardt M and Prinz A, ‘Behavioral Dynamics of Tax Evasion – A Survey’ 1

Pierce MA and Henry JW, ‘Computer Ethics: The Role of Personal, Informal, and Formal Codes’ (1996) 15 Journal of Business Ethics 425

Pigou AC, *Wealth and Welfare* (Macmillan 1912)

Pollock N and Williams R, ‘The Sociology of a Market Analysis Tool: How Industry Analysts Sort Vendors and Organize Markets’ (2009) 19 Information and Organization 129

——, ‘Industry Analysts – How to Conceptualise the Distinctive New Forms of IT Market Expertise?’ (2015) 28 Accounting, Auditing & Accountability Journal 1373

Posner EA, ‘Law and Social Norms: The Case of Tax Compliance’ (2000) 86 Virginia Law Review 1781

Post DG, ‘What Larry Doesn’t Get: Code, Law, and Liberty in Cyber-space’ (2000) 52 Stanford Law Review 1439

——, ‘Against “Against Cyberanarchy” – a Reply to Jack Goldsmith’ (2002) 17 Berkeley Technology Law Journal 1365

Poujol JF, Tanner JJ and Fournier C, ‘The Employer Brand as Perceived by Salespeople: A Study Based on Glassdoor Reviews’ (2017) 4 World Academy of Science, Engineering and Technology, International Journal of Economics and Management Engineering

Poullet Y, ‘EU Data Protection Policy. The Directive 95/46/EC: Ten years after’ (2006) 22 Computer Law and Security Report 206

Pullin G, *Design Meets Disability* (MIT press 2009)

Quelle C, ‘The “Risk Revolution” in EU Data Protection Law : We Can’t Have Our Cake and Eat It , Too’, vol 17 (2017)

Raabe O, ‘Beiträge Zu Einer Systemtheorie Sicherheit’ (2018)
Forthcoming Acatech

——, ‘14 Thesen Zum Datenschutz Im Smart Grid’ (2011) 35 Datenschutz und Datensicherheit - DuD 519

Racz N, Weippl E and Seufert A, ‘A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC)’, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Springer, Berlin, Heidelberg 2010)

Raghunandan K and Rama DV, ‘SOX Section 404 Material Weakness Disclosures and Audit Fees’ (2006) 25 AUDITING: A Journal of Practice & Theory 99

Ramos M, ‘Just How Effective Is Your Internal Control?’ (2004) 15 Journal of Corporate Accounting & Finance 29

RAND Europe, ‘Review of EU Data Protection Directive’ (2009)

Rao JM and Reiley DH, ‘The Economics of Spam’ (2012) 26 Journal of Economic Perspectives 87

Reidenberg JR, ‘Lex Informatica: The Formulation of Information Policy Rules Through Technology’ (1998) 76

Reidenberg JR, ‘E-Commerce and Trans-Atlantic Privacy’ (2001) 38 Houston Law Review

Rice D, ‘Geekonomics: The Real Cost of Insecure Software’ 362

Richards JT and Hanson VL, ‘Web Accessibility: A Broader View’, *WWW* (ACM 2004)

Richards S, ‘Selwyn Goldsmith: 1932 to 2011’ (2011) 74 British Journal of Occupational Therapy 359

Rickard A, Wagner J and Schull J, ‘Observations on the Technology and Economics of Digital Emissions’ (2017) 48 Technology in Society 28

Ridley G, Young J and Carroll P, ‘COBIT and Its Utilization: A Framework from the Literature’, *Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 2004* (IEEE 2004)

Riley-Huff DA, ‘Web Accessibility and Universal Design.’ (2012) 48 Library Technology Reports 29

Rother SV and Schiering I, *Privacy in the Life-Cycle of IT Services – an Investigation of Process Reference Models*, vol 421 (Springer, Berlin, Heidelberg 2014)

Rynes SL, ‘Editor’s Foreword Carrying Sumantra Ghoshal’s Torch: Creating More Positive, Relevant, and Ecologically Valid Research’ (2007) 50 *Academy of Management Journal* 745

Sahib NG and others, Participatory Design with Blind Users: A Scenario-Based Approach 2013 685

Sahibudin S, Sharifi M and Ayat M, ‘Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations’, *Proceedings - 2nd Asia International Conference on Modelling and Simulation, AMS 2008* (IEEE 2008)

Sánchez-Gordón M-L and Moreno L, ‘Toward an Integration of Web Accessibility into Testing Processes’ (2014) 27 Procedia Computer Science 281

Sandford CT, ‘International Comparisons of Administrative and Compliance Costs of Taxation’ (1994) 11 Australian Tax Forum

Santos G, ‘Road Fuel Taxes in Europe: Do They Internalize Road Transport Externalities?’ (2017) 53 Transport Policy 120

——, ‘Part I: Externalities and Economic Policies in Road Transport’ (2010) 28 Research in Transportation Economics 2

Schaar P, ‘Privacy by Design’ (2010) 3 Identity in the Information Society 267

Schleyer T and Forrest J, ‘Methods for the Design and Administration of Web-Based Surveys’ (2000) 7 The Journal of the American Medical Informatics Association 416

Schneier; Bruce, ‘Information Security and Externalities’ (2006) 2 ENISA Quarterly Review

Schuhmacher F and Geschwill R, ‘Employer Branding: Anleitung zur Erarbeitung einer Employer-Branding-Strategie’, *Employer Branding Human Resources Management für die Unternehmensführung* (2009)

Schulze-Hagen A, ‘Die Bindungswirkung technischer Normen und der Anscheinsbeweis im Baurechtsprozess’ (2005) 65 Festschrift für Prof. Ulrich Werner zum 65. Geburtstag 355

Schweik S, ‘Lomax’s Matrix: Disability, Solidarity, and the Black Power of 504’ (2011) 31 Disability Studies Quarterly

Seligman E, *The Income Tax: A Study of the History, Theory, and Practice of Income Taxation at Home and Abroad* (The Lawbook Exchange Ltd 1914)

Sengers P and others, ‘Reflective Design’, *Proceedings of the 4th decennial conference on Critical computing between sense and sensibility – CC ‘05* (ACM Press 2005)

Shaw M, ‘Prospects for an Engineering Discipline of Software’ (1990) 7 IEEE Software 15

Shayan Ahmadian A and others, ‘Supporting Privacy Impact Assessment by Model-Based Privacy Analysis’ (2018) 8

Shinohara K and others, ‘Who Teaches Accessibility?’, *Proceedings of the 49th ACM Technical Symposium on Computer Science Education - SIGCSE ‘18* (ACM Press 2018)

Sivertzen AM, Nilsen ER and Olafsen AH, ‘Employer Branding: Employer Attractiveness and the Use of Social Media’ (2013) 22 Journal of Product & Brand Management 473

Slater DJ and Dixon-Fowler HR, ‘The Future of the Planet in the Hands of MBAs: An Examination of CEO MBA Education and Corporate Environmental Performance’ (2010) 9 Academy of Management Learning and Education 429

Slemrod J, ‘Optimal Taxation and Optimal Tax Systems Three Cornerstones of the Theory of Optimal Taxation’ (1990) 4 Journal of Economic Perspectives 157

Sloan D and others, ‘Contextual Web Accessibility – Maximizing the Benefit of Accessibility Guidelines’, *Proceedings of the 2006 international cross-disciplinary workshop on Web accessibility (W4A) Building the mobile web: rediscovering accessibility? - W4A* (ACM Press 2006)

Sloan D and Kelly B, ‘Reflections on the Development of a Holistic Approach to Web Accessibility’, *ADDW08 Conference* (University of Bath 2008)

Smith A, *An Inquiry into the Nature and Causes of the Wealth of Nations* (1776)

Sneller L and Langendijk H, ‘Sarbanes Oxley Section 404 Costs of Compliance: A Case Study’ (2007) 15 Corporate Governance 101

Sohaib O and Kang K, ‘E-Commerce Web Accessibility for People with Disabilities’, *Complexity in Information Systems Development* (Springer, Cham 2017) 87

Solove DJ, ‘A Taxonomy of Privacy’

——, ‘Understanding Privacy’ (2008) 420

Spence M, ‘Signaling in Retrospect and the Informational Structure of Markets’ (2002) 92 American Economic Review 434

Spina A, ‘A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics’ (2017) 8 European Journal of Risk Regulation 88

Stein MA, ‘Quick Overview of the United Nations Convention on the Rights of Persons with Disabilities and Its Implications for Americans with Disabilities’ (2007) 31 Mental & Physical Disability Law Reporter

Story MF, ‘Maximizing Usability: The Principles of Universal Design’ (1998) 10 Assistive Technology 4

Sullivan T and Matson R, ‘Barriers to Use: Usability and Content Accessibility on the Web’s Most Popular Sites’, *Proceedings on the 2000 conference on Universal Usability - CUU ‘00* (ACM Press 2000)

Sumners GE and Soileau JS, ‘Addressing Internal Audit Staffing Challenges’ (2008) 37 EDPACS 1

Sweeney L, ‘Simple Demographics Often Identify People Uniquely’ (2000) 671 Health (San Francisco) 1

Swire P, ‘No Cop on the Beat: Underenforcement in E-Commerce and Cybercrime’ (2009) 7 Journal on Telecommunications & High Technology Law 107

Swire PP, ‘Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in Privacy and Self-Regulation in the Information Age by the U.S. Department of Commerce.’ [1997] SSRN Electronic Journal

Takagi H and others, ‘Accessibility Designer: Visualizing Usability for the Blind’, *Proceedings of the 6th international ACM SIGACCESS conference on Computers and accessibility* (ACM 2004)

Tassey G, ‘Standardization in Technology-Based Markets’ (2000) 29 Research Policy 587

Thaler RH and Benartzi S, ‘Save More Tomorrow^{TM}: Using Behavioral Economics to Increase Employee Saving’ (2004) 112 Journal of Political Economy 164

Thaler RH and Sunstein CR, *Nudge* (Penguin 2008)

Thatcher J, Kirkpatrick A and Heilmann C, *Web Accessibility: Web Standards and Regulatory Compliance* (friends of ED 2006)

Thomson AJ and Schmoldt DL, ‘Ethics in Computer Software Design and Development’ (2001) 30 Computers and Electronics in Agriculture 85

Thomson JJ, ‘The Trolley Problen’ (1985) 94 Yale Law Journal 1395

Ting KLH and Lewkowicz M, ‘From Prototype Testing to Field Trials: The Implication of Senior Users in the Evaluation of a Social Application’ (2015) 67 Procedia Computer Science 273

Tippett E and others, ‘When Timekeeping Software Undermines Compliance’ (2017) 19 Yale Journal of Law & Technology

Tran Quang Thanh and others, ‘Embedding Security and Privacy into the Development and Operation of Cloud Applications and Services’, *2016 17th International Telecommunications Network Strategy and Planning Symposium (Networks)* (IEEE 2016)

Trank CQ, Rynes SL and Bretz, Jr. RD, ‘Attracting Applicants in the War for Talent: Differences in Work Preferences Among High Achievers’ (2002) 16 Journal of Business and Psychology 331

Trost A, *Employer Branding* (Luchterhand in Wolters Kluwer Deutschland 2009)

Trost A, *Talent Relationship Management. Personalgewinnung in Zeiten des Fachkräftemangels* (Springer 2012)

Tsormpatzoudi P, Berendt B and Coudert F, ‘Privacy by Design: From Research and Policy to Practice – the Challenge of Multi-Disciplinarity’ (Springer, Cham 2016)

Tuttle B and Vandervelde SD, ‘An Empirical Examination of CobiT as an Internal Control Framework for Information Technology’ (2007) 8 International Journal of Accounting Information Systems 240

Tynan A, ‘Recruitment Equality: Accessibility, Equality and Diversity on Recruitment Websites’ (2011)

Uerpmann-Wittzack R, ‘Die UN-Behindertenrechtskonvention in der Praxis des Ausschusses für die Rechte von Menschen mit Behinderungen’ (2016) 54 Archiv des Völkerrechts 181

Vigo M and others, ‘User-Tailored Web Accessibility Evaluations’, *Proceedings of the eighteenth conference on Hypertext and Hypermedia* (ACM 2007)

Vigo M, Brown J and Conway V, ‘Benchmarking Web Accessibility Evaluation Tools’, *Proceedings of the 10th International Cross-Disciplinary Conference on Web Accessibility - W4A ‘13* (ACM Press 2013)

Virkki J and Chen L, ‘Personal Perspectives: Individual Privacy in the IOT’ (2013) 3 Advances in Internet of Things 21

Von Solms B, ‘Information Security Governance: COBIT or ISO 17799 or Both?’ (2005) 24 Computers and Security 99

Waddell C, ‘Overview of Law and Guidelines’ in Jim et al Thatcher (ed), *Web Accessibility* (Springer 2006)

Waldschmidt A, Berressem H and Ingwersen M, *Encounters between Disability Studies and Cultural Studies* (2017)

Walker HJ and others, ‘So What Do You Think of the Organization? A Contextual Priming Explanation for Recruitment Web Site Characteristics as Antecedents of Job Seekers’ Organizational Image Perceptions’ (2011) 114 Organizational Behavior and Human Decision Processes 165

Watchorn V and others, ‘Strategies and Effectiveness of Teaching Universal Design in a Cross-Faculty Setting’ (2013) 18 Teaching in Higher Education 477

Watkins LM and Johnston L, ‘Screening Job Applicants: The Impact of Physical Attractiveness and Application Quality’ (2000) 8 International Journal of Selection and Assessment 76

Weber RH, ‘Internet of Things: Privacy Issues Revisited’ [2015] Computer Law and Security Review

Werle R and Iversen E, ‘Promoting Legitimacy in Technical Standardization’

Whetstone KW, ‘Upholding Accessibility Standards When Selecting Tech Tools’, *Association Supporting Computer Users in Education* (ASCUE 2017)

Wiese Schartum D, ‘Making Privacy by Design Operative’ (2016) 24 International Journal of Law and Information Technology 151

Wild G and Craddock D, ‘Are PDFs an Accessible Solution?’ 355

Wilden R and others, ‘Employer Branding’ [2013] Lebensmittel Zeitung

Wilkes MV and Renwick W, ‘The EDSAC (Electronic Delay Storage Automatic Calculator)’ (1950) 4 Mathematical Tables and Other Aids to Computation 61

Wilkes MV, ‘John Pinkerton and Lyons Electronic Office’ (2001) 10 Engineering Science and Education Journal 183

Wilson C and Cameron, ‘Hour of Code’ (2014) 5 ACM Inroads 22

Wright D, ‘Making Privacy Impact Assessment More Effective’ [2013] The Information Society

Wright KB, ‘Researching Internet-Based Populations: Advantages and Disadvantages of Online Survey Research, Online Questionnaire Authoring Software Packages, and Web Survey Services’ (2005) 10 Journal of Computer-Mediated Communication 0

Wu S and others, ‘Automatic Alt-Text: Computer-Generated Image Descriptions for Blind Users on a Social Network Service’

Wu T, ‘When Code Isn’t Law’ (2003) 89 Virginia Law Review 679

Wu TS, ‘Cyberspace Sovereignty? - The Internet and the International System’ (1998) 10 Harvard Journal of Law & Technology 647

Yan H, ‘Keystone of Engineering Education - Ethics Education’, *Lecture Notes in Electrical Engineering* (Springer, Berlin, Heidelberg 2011)

Youngblood SA, ‘Communicating Web Accessibility to the Novice Developer: From User Experience to Application’ (2013) 27 Journal of Business and Technical Communication 209

Zhang IX, ‘Economic Consequences of the Sarbanes-Oxley Act of 2002’ (2007) 44 Journal of Accounting and Economics 74

Zimmermann L, Hillman M and Clarkson PJ, ‘Wheelchairs: From Engineering to Inclusive Design’, *Include 2005* (2005)

Zittrain J, ‘Internet Points of Control’ (2003) 44 Boston College Law Review 653

Zuboff S, ‘Big Other: Surveillance Capitalism and the Prospects of an Information Civilization’ (2015) 30 Journal of Information Technology 75

Appendices

Appendix A Anne Tynan interview

Thomas: So, Anne, perhaps start by giving me a little bit of background about yourself, what's your involvement with accessibility and disability, and give me some context here.

Anne: Right. I've been working in issues, related to disability for about 20 years. During that period I've done probably about 15 years direct work with disabled people in various contexts, initially in a university museum and art gallery and then, subsequently, at the University of London supporting students. After the initial period of doing that, I became interested in transmitting information to other people, because I was aware of the ignorance in the issues. [1:08] So, in 1997, I published a book that I wrote about attitudes to disability, and that was the start of me recording things and trying to promote the issues. At the University of London, I carried on writing and publishing, and I've got to come onto that in a few minutes.

I also spent three years working as a Government Advisor on building accessibility. It was a Government Committee for Building Regulations which produced new guidelines for builders and planners on making buildings accessible and useful by disabled people. So, I was involved in that.

Thomas: So your interest in accessibility and support of disabled people goes beyond the software, the web context.

Anne: [2:08] Yes, it's a holistic approach given that I have always tried to look at the position of disabled people in the whole. In the last years I've also had a look at other equality issues related to it, such as ethnicity and issues, for example, of women who are disabled because, again, they're all interconnected.

Thomas: [2:35] Would you say that there is a difference in terms of the understanding between, say, software people and architects?

Anne: [2:50] I've had more contact directly with architects than I have with software people. But I think one of the differences is that architects are legally obliged now, certainly in the UK, with any new build or certain amendments to older buildings. That, they won't get permission for a building to be approved unless they have considered details of accessibility. I'm not aware of a law in the UK which obliges software developers to do that in the same way.

Thomas: [3:29] No. It's one of the debates at the moment is, indeed, the exact nature of the disability law relating to the IT software. Perhaps you could just help me a little bit by explaining the connection between disability and accessibility. How would you define those two terms? As, I've come across a variety of definitions in my research so far.

Anne: [4:01] Yes. In the UK concepts, to have a disability is a legal term, and people can be judged by courts either to be disabled or not disabled. I'll give you an example. Somebody who is diagnosed with cancer or has had cancer is legally considered to be disabled from the moment of their diagnosis. Other people with certain mental health conditions may or may not be deemed to be disabled. [4:32] In the broader term than what the ordinary people in the street would understand, would be disability in the broader sense, which would include people who wouldn't necessarily in a court be considered to be disabled. One of the conditions is that your particular impairment or condition needs to be of lost inability, lasts for a minimum of 12 months or be a terminal condition. I think there's a broader thing.

Now, I think in terms of disability and accessibility, accessibility is used a lot in the UK now but in terms of just everybody being able to get to something. So, at the moment, accessibility to Olympic tickets for next year in the UK is almost impossible for people to obtain. So it's used in a broader sense meaning, I would, say, just clouds this everybody of any age, able to get something.

[5:43] Now, in contrasting two terms in the context we're talking about, I'd just say briefly that not all disabled people, using the term in the broader sense, have an issue with web access. I know people who have multiple sclerosis, for example, who don't actually have a problem with any issues of Internet or web or software access.

It will generally tend to be people with visual impairments or blindness, dyslexia, deafness, learning difficulties, mental health issues in some cases, and physical disabilities. But the fact of being disabled doesn't mean you have a problem with accessibility, either physical or with the Internet.

[6:34] Then the other issue is, it's not only disabled people who need access, and again, I would say both physical and Internet or web access. Children, for example, and adults as they age may have problems with both physical and Internet access, and it's noticeable. I was thinking that for many children's websites, and I think the BBC children's websites, for example, it's noticeable that they're to be larger font size, attractive colors, clear, not complicated sites to look at, because they're geared at them. But I think that's another important issue.

[7:17] I think one thing I have always tried to promote, as well, in terms of website accessibility is that people are generally quite lazy.

[7:27] If they go on the Internet and they're looking to buy something, say, a new bicycle, well, if they go and look at different websites – I haven't done a study, but I think it would be interesting to do one – a website which is well presented and you can work your way through it quickly, you don't need too many clicks to get to the relevant information, it's very easy to read what's on the page, I would have thought would be more likely to gain the sale of that person and other people.

[8:03] So that's another issue, I think, in terms of accessibility, if you want to use it as a tool to attract people to your website or to buy your product, whatever that might be.

Thomas: [8:17] OK. Perhaps you could give me a little bit of an overview of the law in the UK, the DDA as I understand it. If you could put that into context to me, especially within, perhaps start off with a broad overview, and then bring it into the context of web accessibility in particular.

Anne: [8:42] Yeah. Just very briefly, the DDA was the new law passed in 1995, and it was the first substantial piece of legislation in UK history which provided rights for disabled people. Previous legislation had dealt with them as chronically ill and sick people. But this was from a very different perspective, and it was offering rights to disabled people as individuals. [9:17] Amendments have been made to the Act since it was passed in 1995, most noticeably in 2005. It covers broad areas, such as employment and education, goods, rights and services, building, renting, for example, tenants. It's very broad, and to be honest, it covers most aspects of life. Goods, facilities and services, for example, would happen often, most of what we would buy in the shop.

[9:54] Now, to some extent it has been cemented by the Equality Act, which has had several versions, but the last one was in 2010. Now, the Equality Act, it does take further some aspects of the Disability Discrimination Act, which it would take me too long to go into the details of that at the moment. But it sets them within a broader context of people as individuals who may be disabled, who may be of a particular ethnicity, who may be women, et cetera, et cetera. So, that's the broader context.

[10:40] In terms of accessibility, that's covered in some ways in different contexts within the DDA. For example, in education, universities are required to offer equality of opportunity to applicants and students and graduates. That would cover everything from making sure that the application process is accessible to them, that they may be, if the application process is online, offered alternative methods of applying. The interview process, if it subjects a student to use, especially, sign language, they must be offered a signer for the interview process, et cetera. So, that's very broad.

[11:33] Now, in terms of students receiving their education, the issue breaks out accessibility as relevant in terms of, nowadays a lot of course work is carried out and marked online, and a lot of university education takes place online. Therefore, a disabled student who has an issue with website accessibility therefore must have equal access to the curriculum as other students.

[12:07] That may be judged on an individual basis, and the system in the UK is that students can apply to receive a grant which would pay, for example, for them to have one of the software programs which would speak out the text on the page to them. Some of that is already, becoming outdated, because there are programs which will do that from the website itself. I think you're probably familiar with that.

Thomas: [12:37] Yes.

Anne: [12:39] In some ways it's quite a fast-moving aspect. There are issues about what the university must provide and the student themselves are able to obtain individually. But I think the bottom line with everything is that institutions and companies have got very prescribed requirements placed upon them that they must achieve. [13:10] There is a concept of reasonableness within the Disability Discrimination Act that would say, for example, that a university which is financially in difficulty, which some in the UK are, particularly at the moment, would not be required to pay thousands and thousands of pounds to make adjustments to buildings when they wouldn't be able to afford that within their particular budget.

[13:43] So there is a, a lever there, but at the same time, the expectation is that the institution will eventually work towards full accessibility, and that would include website accessibility.

Thomas: [13:56] Now, there have been a lack of, I would say a lack of active court cases that have gone to judgment with regards to accessibility. The best thing that I could find was the Australian case with the Olympics. There was a disabled agent in Australia who took the Australian Olympic Committee, and IBM, who were the software contractor, to task in terms of the accessibility to both the ticket buying with sporting results, in terms of the Australian Olympics. [14:47] I understand that in the UK, I think it's the Royal National Institute for Blind People has been relatively assertive with - I think there was a case with Tesco where they were assertive in getting them to redo their website. But I'm not aware of any significant other court activity around the media, at least as it relates to websites. Do I have that right?

Anne: [15:23] To my knowledge, yes. I think that is right. I say to my knowledge because as with you, I get a lot of my information by the Internet, because obviously that's where most legal information is posted. I'm not aware of very many. [15:44] On one of the reports that I did at university, was a study to the extent to which disabled students would be able to train to be qualified as doctors, dentists, or veterinary surgeons, the professional requirements. But the name of that report was "Time to Take Stock". If you look on my LinkedIn publications list at the end, you should be able to located it. I've put a lot of links in there, which unfortunately, given the nature of the Internet, are now outdated.

[16:19] But I trawled everywhere, looking for relevant legal cases. I looked it up, I haven't got the report beside me here. I can't remember. But I did trawl around, and I couldn't find anything. But I think the reason for that is the effort involved in pursuing it, I was hopeful through the recruitment reports that I did, that somebody somewhere might be able to use that as a lever to encourage a company to change their website.

[16:58] But I think the other issue as well is that the Disability Rights Commission, which was the organization founded at the same time by the Government, when the DDA was passed in 1995, were not keen to promote a lot of legal cases, because of the stress on the individuals involved obviously, but also the cost. Now that body has finished, and the current equality body in the UK is the Equality and Human Rights Commission, to some extent the follow the same policy.

[17:36] They are using public money. They do certainly support legal cases taken, but I think the attitude which I would agree with would be to try to persuade people to follow best practices, rather than immediately taking them to court.

Thomas: [17:56] It seems similar to the way that the UK authorities have had the rules about data protection EM. For a long time, the Information Commission in the UK was about educate rather than prosecute, and it seemed a similar attitude towards accessibility.

Anne: [18:14] I think so, because I think in terms of adverse publicity, for example, there was a case recently in the UK of another issue, an employment case, a company were taken to an employment tribunal about issues of a disabled employee. Again, the issue is that most of these large companies don’t want to be taken to court because of publicity.

Thomas: [19:33] Yeah. So in terms of the two studies of yours that have done, the recruitment study and the colleges study, could you talk to me a little bit about those?

Anne: [19:46] Yes. The first study I did, which I published in January of this year, 2011, I looked at accessibility, equality and diversity on recruitment websites. Now, this was an initiative of my own. Because in the previous year, I had become more and more involved in different events and other issues with the recruitment industry – which is the industry which either is made up of people who work in HR, who do recruitment for the company, or much more broadly, many hundreds and thousands of companies, either very small with one person, and coming up to the multi-international companies.

Thomas: [20:40] The Michael Page's and --

Anne: [20:41] Yeah, that's an exact example. It was my own initiative, because some of these people who are fairly critical of things going on in other fields, and fairly critical when people did criticize the "Equality Act" last year. So I decided that I would actually have a look at their websites. Now, I looked not just at the accessibility, but the equality and diversity, which meant that I looked at the extent to which it appeared to be accessible. [21:15] I'm not too much a specialist myself with the technical knowledge, but I did it from the point of view of an ordinary lay person looking at the website. Does it appear to offer accessibility? Secondly, does it, on transmit a modern, up-to-date, 21st century awareness of equality and diversity issues, which means recognizing, and people of different ethnicity and the broader context.

[21:49] Within that study, I looked up three – the websites of 300 companies, and then I produced the report, and I looked at a wide range of issues. One, looking at did they actually have an accessibility button on their website? Did they offer adjustable text size, and did they make reference to the W3C guidelines, which are the international guidelines on website accessibility? So there were a range of issues.

Thomas: [22:25] But you didn't go - that's a fairly base level test. You didn't even do an alternative texts test, or any of the more sophisticated tests for --

Anne: [22:39] No, I didn't for two reasons. One, I don't think I probably have the technical ability to do that. I'm sure I could if I were to spend the time actually following the guidelines, but this was a self-funded study, which I did out of interest, but also to educate. Because one of the things I did with the study was to actually try and explain a little bit what were these guidelines, what did it mean when you saw a W3C logo on the website page? So I didn't feel it would've been appropriate for me, as a non-technical person, with that judgment.

Thomas: [23:26] So what did you find out, that a vast majority of recruitment sites were essentially inaccessible?

Anne: [23:35] Yes. I mean, I can actually give you a couple of stats from the websites that were picked up quite broadly by the media, as they tend to --

Thomas: [23:47] Yeah, that's how I found it. I was looking at it. That's how I found you, was via that study.

Anne: [23:56] Well, I could start by saying that 54% of websites had no accessibility or equality and diversity information on them at all, and then 34% of websites did have some accessibility information on them. So again, that could range from having an accessibility button an accessibility statement, a reference to access keys. So it was quite broad. That, in itself is pretty telling. Just looking to see if there's anything else which - I think in terms of your study, that's the main --

Thomas: [24:51] I mean, that's quite damning information, because you've set the bar lower than actually a formal test of the website.

Anne: [25:01] Yes. I mean that's why. Even a formal - I have got no idea - certainly if I had gotten somebody to fund me to do that, study, I would then do it. I could invest the necessary time doing it. But given that only 34% even mentioned it, I can't guarantee that the other sites hadn't followed some of the W3C guidelines in that. But generally speaking, I find that if people have an awareness of the issue, they'll make sure they put something on their website. Because for me, the two go together.

Thomas: [25:42] Indeed. That would actually be something interesting to test, would be a correlation between the presence of any accessibility dimension, and the score in terms of accessibility on a technical level.

Anne: [26:04] Yeah, for me, and I think that's the other issue why I've more recently in the last year started talking about - talking about marketing equality and diversity. But particularly marketing accessibility, equality, and diversity. Because for me, the issue is, and this may cover some of your other questions, one thing is making your website accessible, but the second thing is actually using that as a tool to tell people your website's accessible. [26:32] So that in my perspective, they can see immediately that you are a modern company aware of legislation and best practices.

Thomas: [26:41] Because that's not only been a buying signal to the disabled market, I don't really like that term, but also a message to the broader society that you are a responsible corporation.

Anne: [26:59] Exactly, yes.

Thomas: [27:03] So if we say look, the DDA has been around for the best part of a decade now. The web standards, they are some - you can get, technical about the debates about whether the standards themselves show accessibility or not. We won't get into that today. But the standards have been around for ten years. The law in the UK has been around for ten years. The standards are reasonably well defined. [27:36] Why is it do you think that most websites today, and I will put the figure – I don't know, according to my research, and you put it at other numbers, but – let's for the sake of argument say it's 70 percent of significant commercial and public websites are inaccessible in the UK. What is your view of why we have this failure in producing accessible websites?

Anne: [28:07] I think there's a failure because of the lack of understanding of the legal requirement.

Thomas: [28:16] Who has that lack of understanding? Is it the software developers, or is it the people that are commissioning the websites, or is it both?

Anne: [28:26] Well, without knowing many personally, I think it's clear that software developers must have a lack of knowledge, because otherwise they would be more active in this area. But I think that there is a gap between software developers, IT people, if I can just call them that broadly, and lay people, and I consider myself a semi-lay person in this area, which is that the ball is passed from one to the other. [29:08] So that in institutions, generally speaking, people rely on the IT people, from the help desk with email to the website developers, to just get on and do it. Their primary concern is this envelope about, I would say that about universities but I think it also applies to companies, where everyone who has an interest, the different stakeholders within the institution, want their part of the institution to feature prominently on the website. That will be their main interest.

[29:47] How the website is presented and how the website manager and software developers do that, I don't think that most people in the institutions in other roles outside of IT perceive it as being their role to promote that. I think they will accept what they're so keen on, the content of their own message, that sometimes how that message is delivered through the website, they don't give it the same attention.

Thomas: [30:26] Have you come across, in your university activities, any universities that are doing a better job at educating developers, or is that not something you've come across?

Anne: [30:39] It's not an issue that I have focused. I have to say, you're the first person who's droved it with me. It certainly is something I will look at now. That, I very briefly today did have a look on the Internet, a little bit in a few minutes, but I certainly now will have a look. [31:01] Interestingly, the company which sponsored the second report on colleges, they actually do develop software. So I will certainly want to come up to them and speak to them about a few of the issues.

Thomas: [31:19] I might like to have a chat with them, actually. I think that might be interesting.

Anne: [31:23] Yeah, certainly. If you want me to say something about that report now, connected to this?

Thomas: [31:28] Yeah, I think that would be good. Yeah, the recruitment one you've pretty much covered often and general issues we've pretty much covered off. I think the one thing I wanted to pick up of, one thing I've sensed in my academic research is that, when it comes to web accessibility – and this is going to sound horrible, but – the demands of the blind tend to overwhelm some of the other demands. [crosstalk]

Anne: [31:59] Yeah. I don't think that sounds terrible. So does that, then, answer your question, or I'll answer it?

Thomas: [32:08] Yeah. I was just thinking of a way to phrase that politely. But it seems, too, that the blind lobby has been stronger and more effective than some of the other lobbies, at least in terms of if I look at the technical web standards. The technical web standards are relatively clear in terms of the excess ability with regards to the issues of blind people and, to a lesser extent, of deaf people. But they have not done a particularly good job, for instance, on some other disabilities that you mentioned, dyslexia and some of other other disabilities. They've probably done a less good a job on those.

Anne: [33:01] Yeah. I'm not entirely sure that the compliance framework itself focuses on particular forms of disability at the expense of others. Like, my having looked at it, I didn't particularly have that impression. [33:20] The international guidelines, because they're international, they don't all use the same terminology, and because their source, they're embedded within the whole of the, ethos, and that's what I'm aware of. I've always been aware of that, and it's one of the things that's interested me about the legal documents. It's why, in the studies I've done, I've usually looked at the law and unpicked it. Because they're coming from different concepts.

[33:54] I didn't feel, particularly, when I've looked at them that they wouldn't meet the needs of different people. But what I have observed is that the usual perception … If I were to go into work tomorrow and say, "Oh well, who do you think would have a problem with website accessibility?" I would expect most people to say, "Yes," people who have a vision impairment or who are blind. I would also expect that some people would say to me why would blind people be using the Internet, for God's sake?

Thomas: [34:34] Yes. I found quite a bit of that. I spent some time today on the software discussion boards. There was quite a lot of those comments like why are blind people on the Internet anyway?

Anne: [34:50] Yeah, well funny enough, this is just a little anecdote, in 1995, I forgot to mention the other day I interviewed Stephen Hawking. Within the context I was curating an exhibition at the Science Museum in London. It was an art gallery exhibition and we used a portrait of Professor Stephen Hawking. It was in the collections which was the BOCES and [inaudible 35:23] . [35:23] I wrote what I would have called accessible exhibit labels and then we also had Braille labels and what are called Makaton symbols. They're probably not particularly relevant to your context at the moment although you could get them on websites. When I went to interview him and explained about the exhibition about the braille the first comment he made was well why would blind people be going to an art exhibition?

[35:55] It's relevant in that perception of what blindness is. But coming back to your original question, I think the general public and probably website developers' perception would be blind people. My observation, and again from the last two studies I've done, is that deaf people's needs are very rarely recognized.

[36:21] People have this perception that deaf people can read and therefore a website is fine for them. Well obviously websites now are full of interactive video material, etc, etc. So in actual fact some of the colleges had video interviews with students in the college talking about what it was like for them to encourage new occupants.

[36:52] The perception that deaf people wouldn’t have a problem is a false one. One of the things that I did notice was that although websites had video material very rarely did they have captions underneath, subtitles, and very rarely, understandably to one extent, did they have put their signing going on.

[37:19] In fact, even the BBC itself is very inconsistent with that. The general, news, if you watch BBC news, most of the time you won’t have a signer but there are times when suddenly the BBC news will have somebody signing the news by the side of it. It’s inconsistent.

[37:39] If you want to watch the news as a deaf person in the morning and want signing well I can understand why you wouldn’t want that 24 hours a day. Anyway, that is one of the main areas where people’s needs have been neglected. Looking at college websites they were very often doing it in a very cheap way which was they would do a video and post it on YouTube and then link to the YouTube video from their website.

[38:15] So that’s a very democratic, totally open way of putting up something and I would argue that OK not every college and institution can pay for BSL signing but surely it must be possible to provide that video material and text underneath so a deaf person could read it.

Thomas: [38:39] Or at least a transcript.

Anne: [38:40] Yeah. Yeah.

Thomas: [38:42] I’m going to send this hour discussion off to India and this time next week I will get a transcript back at something like a Euro a minute if not less for that transcription service. Yes there are costs involved in doing that; but I think they are bearable.

Anne: [39:17] Yes and I think again just in terms of marketing to company's attitudes about disability. Understandably you may not be able to do that for everything. But at least you can give a taste of it and show that you're aware that these means exist. If the second report does contain links there are very sophisticated ways for institutions to have information up and accessible. The examples are in the second report.

Thomas: [39:50] Yes. I've had a good look through that.

Anne: [39:52] Yeah. [inaudible 39:40] . There were some quite extraordinary. I found them quite extraordinary actually the way that they were which was that they were fun to use but they didn't look all disability tinged, charity for disabled people. They actually looked quite fun.

Thomas: [40:20] I think Apple, for instance, it creates some issues into one type of disability but then on other types of disability it's very useful is the iPad type interface for people for whom the keyboard is a problem. For many users there's a whole lot of new technical opportunities with regards to accessibility. [40:54] If we look to the future from your perspective, the reason why I'm asking you this question is I've been looking through the academic research and there was a wealth of studies done between five and 10 years ago on web accessibility and most of the results were pretty damning.

[41:19] They would compare Government websites against the Level A Bobby test, and 90% of Congressmen's websites failed Bobby Level A. 75% or 80% of UK parliamentarian's websites failed Bobby A.

[41:43] Recent studies don't show much of an improvement. They show a slight tick up, maybe a slight improvement in the public sector. But on the whole, website accessibility hasn't improved dramatically over the last ten years. Do you think anything's going to happen to change that?

Anne: [42:02] Can I just ask - most of the studies you looked at, have they been US studies?

Thomas: [42:07] A bit of both. I've come across a few - I'm going to send you it. There's been quite a bit of research done out of - is it Worcester or Winchester? I think it's Worcester. I'll send you the link. But you know, most of the studies show – they haven't shown a really dramatic – there may be a five percentage point improvement, but I'm not seeing, a 40 or 50% level. It's still ten to 30%, depending on which study, and which sector.

Anne: [42:53] Yeah, that doesn't surprise me at all. But at the same time, I wouldn't have continued working in disability issues if I hadn't had a long term vision of expectation of improvement, if you like. Just for example, when I first started working on a full-time basis with disabled people, it was in about 1992, and the contrast between attitudes and structures then and now is quite amazing. [43:32] When I look back on it, it really was quite - and people were ignorant, and they just didn't understand. I would have to contrast that with, for example, issues of racism in the UK, which was when I was at school lever, I witnessed many incidents of racism in London. That was at the stage when we didn't have the legislation, and there wasn't the awareness that there is now.

[44:04] I'm not saying that the problems have gone away by any means at all, but there have been dramatic improvements. I think the same with this. It does take a long time to change.

[44:17] There are three reasons why this, improvement is slow. I say with web and software access. I would say in the first place, there's indifference. Some of the people I've spoken to, including IT people, have said that they don't really care. I mean, their interest is in IT issues and development, and a fast moving field.

[44:49] It's not their problem, they see it as some, social inequality problem, and they have said to me with admirable honesty that they don't really care, which in actual fact is a much easier attitude to deal with than someone who says that they are interested but they're all the same.

Thomas: [45:11] I think it’s an interesting parallel that’s worth thinking about, is the ratio of the gender ratios in IT are pretty out of whack as well. You can understand, to some extent, that ancient professions, in ancient professions that have developed over decades with prejudices, and so on, or centuries, would be gender – you would have a gender bias. [45:40] But when you think about IT, it’s a modern discipline, it’s only really been around – it’s been around roughly as long as the human rights movement. It’s, grown up in parallel with gender issues. You would, in theory, it’s not a job that requires great physical prowess. It’s not a job that requires a, behavior, it’s relatively cerebral. You would have expected, naively, that IT would be a more egalitarian profession from a gender perspective. But it’s arguably the worst profession from a gender perspective.

Anne: [46:30] Well, interestingly, in the UK I think that the IT profession has a bit of a reputation of having people working in it who are happiest working, as you said, the cerebral, and they’re happiest working with material, are not happy interacting with groups of people, and tending too often. [47:00] I’m just saying this is the reputation in the UK a little bit - tending towards people who may have Asperger’s Syndrome, which I think the figures it’s on the spectrum of autism, and as far as I’m aware, I haven’t checked the figures recently, it does tend to be a condition which is mainly male, rather than female. So I think it does tend to have that reputation.

[47:31] I would say certainly, without stereotyping everybody I’ve ever worked with who has that inclination, I would say that there is some truth in it. I’ve seen problems of communication between IT people and other people, because I’ve found that many IT people just tend to say the facts, and don’t dress them up in a social nicety. Certainly in the university context, depending on their discipline, university staff sometimes find that quite difficult to manage.

[48:09] They like to be given things in a package, if you like, rather than a black and a white, speaking professionally, who will say what the problem is but don’t want to spend all day discussing why it happened and how they feel about it, if you understand what I mean.

[48:26] We’re probably getting away from the topic here. But it probably is a little bit relevant to this.

[48:35] I think the other issue, which is a barrier to development, if you like, is Inertia. But the whole IT field has just raced ahead. It’s quite difficult to keep up with it. I think that brings with it, because I’m just imagining that software developers have to be so focused on – for competitive reasons, for keeping up with the latest, that there’s a certain inertia. To anything that isn’t central to that, that having within that process to try and incorporate other features about accessibility, which aren’t in their opinion, directly relevant to progressing a particular program or something, they’ve been left behind. To a certain extent I can understand that.

Thomas: [49:37] Perhaps there’s a final, question. This has been really useful, I think I’ve got a lot of good stuff here, I think I’ll get a couple of good, juicy quotes here. Do you think we’re missing – there’s a role that I’ve been thinking we need more of in one of my – giving a bit away here in terms of my dissertation. [50:08] One of the things I’m suggesting is that the university look to develop more hybrid courses that combine not just legal, but societal and technical requirements in one course. So the, things I’m thinking about here is that – one of the things I’m finding is that software developers on the whole are very unaware of contract issues. They’re very unaware of issues with regards to privacy, or with regards to intellectual property.

[50:44]would see accessibility as a pillar, or a component of an almost software and society type of intervention. Because what I’ve seen is that the law profession has actually been quite good in the last decade in coming up with courses for lawyers on technology. For instance, if you look at Queen Mary, or Strathclyde, where I went, you will find that the law departments offer an LLM in IT law.

[51:24] But I'm not yet seeing the equivalent from the technical side of the house. My perception is that is missing, and that's something that computer science faculties should look to introduce more of in terms of their work in computer science. Science faculties on the whole have been relatively poor in involving ethics and other issues in terms of scientific training in general, but if you do a physics degree today, there are elements of ethics that you're taught in that exercise.

[52:16] You look at the impact of physics on society, you go back to Einstein and Niels Bohr, and folks involved in the Manhattan Project and so on. There's a whole technology can do bad and technology can do good argument. I'm of the view that I think we need, as a software industry, we need to become more aware of our societal responsibilities as we develop technology.

Anne: [52:47] Well, I agree with you completely, and I think if somebody could develop that, course, I would probably want to go and do it myself. I think there is a constant in the UK. I was just thinking when I worked in the professional faculty, the students were starting to be more involved in the issues of the humanities, because the idea of being that they're client-based, previously were predominantly farmers, and were now small animal and companion animal owners, and therefore they needed to --

Thomas: [53:21] Almost generate a bedside manner.

Anne: [53:23] Yeah, but I think - I would've put it up, but I think you probably find it via Google. There should be references to humanity and the sciences. I think that the subject central was in university, which was the Higher Education Academy of Medicine, Dentistry and Veterinary Medicine. I imagine there's probably a link on there. I'm certain you could find something which would describe what we're talking about, which I would say would be introducing humanities into the sciences. [54:02] Because I think that, that describes exactly what you are describing to me, because there's a scientific, technical profession, but now there is the issue of how to link up both professionals, and to get them – one of the courses for veterinary students is on communication skills, which the vets of last century would've probably laughed their heads off at the idea that students are being taught how to speak to people. But there is a necessity, and also there's a parallel with that.

Thomas: [54:39] Yeah, I think so.

Anne: [54:42] But certainly, and I suspect that probably there will become more of a need for the type of course that we're talking about. Not just in terms of accessibility. I mean, interestingly, the Internet really, raised its head around 1995 anyway. I remember I was working at the science museum at the time, and we had an exhibition with an interactive thing where people could press the button to say whether they thought the Internet was a good idea. [55:16] The point being that it has developed now into a stage where, just as people are standing back and looking at the policing of the Internet, and that they're aware, obviously, at the moment. In the UK, different issues that there have been about hacking into people's email accounts and the use of Twitter. How, even today, I've seen that people have been charged with criminal offenses because of what they've put on Twitter.

[55:44] So, I think the whole question of the role of the Internet in society is very topical. Coming back to the, courses that you're talking about, I would have thought that it would be increasingly important for software developers and others in IT and those people to understand the legal context of what they do. So I would expect that to develop to some extent fairly rapidly, because misuse of something often brings about legislation quicker than no use at all, as it were.

Thomas: [56:22] Yeah, I would agree with you. Anne, I think I've got a lot here. I've taken, gee, an hour of your time, so it probably … further as well so we'll see from there.

Anne, it's been lovely talking to you this evening.

Anne: Yeah, OK. Well same to you, Thomas. Good luck with it.

Appendix B Matthew Holloway interview

Thomas: Now you know. No. Well, thanks for doing this today. I think, maybe to kick it off, if you could just give me a little bit of background about yourself – what you studied, what your work background is, where you've worked and so on. And then talk to me a little bit after that about what Design Thinking is and how it applies to software. I'll interject every now and again with questions. All right?

Matthew: OK.

Thomas: But over to you.

Matthew: Yes, that sounds good. So my background is I have an undergraduate degree in industrial design from Ohio State. So actually the 3D design program. And then I have a masters degree in cognitive systems engineering, which is basically the study of how people interact with complex systems like air traffic control systems or anesthesiology equipment.

And having finished the masters degree, I worked at a number of companies in Silicon Valley – Apple, Netscape, Healtheon, WebMD. And now currently I was at SAP running a team running a team that focused on design thinking and spreading that throughout the culture of the company, and now I'm at Shutterfly as their Vice President of User Experience.

Thomas: OK, cool

Matthew: So in regards to the design thinking, it's interesting, I just had breakfast yesterday with a colleague from Intuit. They're also rolling out a design thinking program. And in a nutshell, it's basically teaching non- designers to problem-solve the way designers problem-solve. It's not a linear process, it tends to be pretty rapid iteration. It's a very broad approach, looking at lots of different options, looking at adjacencies and allegories in the marketplace, but then using that information to rethink the paradigms that you might have put in place for the current products. And then building rapidly through a series of prototypes new paradigms that you could explore.

And then using those to drive the requirements process, rather than say, a Word document or PowerPoint slide, actually having an artifact that people can actually see what the product's going to look like, so you can capture more of the nuances of the product as opposed to just a feature check-list.

Thomas: And this method now is relatively well established? It's used by a number of software companies, right?

Matthew: It is. The interesting thing is that different companies call it different things. Intuit, for example, calls it 'Design for Delight', because delighting their customers was a big program or a big push by Scott Cook. SAP called it design thinking. Now I think they call it something else. But different companies have gone through iterations of what they call it.

Proctor and Gamble, who's one of the leaders in this, actually has 17 different programs around this topic, which, given the size of Proctor and Gamble, you can kind of see it.

Most software companies are smaller and giving employees too many choices for tools to pick from for doing innovation is probably not a good thing. But design thinking is pretty well established at this point, yes.

Thomas: And how is it taught?

Matthew: Experientially. The best way that I've found, and talking with other people who are rolling these programs into companies is to actually have people do it. So you could actually have a small one-day workshop where you teach them the concepts in a very hands-on kind of way, probably in a non-work related context, having them design or redesign something that they're familiar with that's in the world that they've used, but is probably not a product their company makes.

And then the second step is to have them apply it to a product their company actually makes and then begin to have them learn the behavior.

One of the folks at IDEO that we were working with in the roll-out of the program said, "It's kind of like riding a bike. I could show you a video of how to ride a bike, I can write a paper on how you ride a bike, but until you actually get on the bike and start pedaling, you're probably not going to understand how to actually ride the bike."

Thomas: OK. OK. But it's now actively taught at universities and so on? I mean, there are programs at several universities that teach design thinking in a software context?

Matthew: Yes, the leading ones of that would be the school in Potsdam, the school of design thinking. And then also the d.school Institute for Design in Chicago teaches a program around this. There's a couple of other programs that teach it as well. The interesting thing is that the traditional design schools, like the big, powerhouse traditional industrial design and graphic design schools tend not to appreciate it as much. The traditional design community still kind of sees this as an… An affront is too strong of a word, but they see it as a threat, at least, to their role in the product development process as being the creative people.

But in truth, it actually underscores the need to have those types of people in the organization. I can come up with a great idea. Taking that from just being a really great idea into being a really great product still requires more skills and experience than what design thinking has.

And so there's always going to be… It actually increases the need for really good design talent.

Thomas: So talk to me a little bit about how this works, then, in the context of software. So how would you go about applying design thinking to a software problem?

Matthew: Well, I think that there's, you can apply it in a multiple of ways. One of the ways that we were looking at at SAP and we're currently looking at at Shutterfly and Intuit has done this as well. So has Autodesk and Kaiser Permanente has done it as well, is that you can kind of take a multi-pronged approach. One approach is to use the design thinking workshop that I described, kind of that early hands on piece. And use that to kind of do a hack day. So that, you know, in the software world, a lot of companies do these hack days, where, twice a year, you get everyone in the company together, they give them a big audacious problem. Say you've got three days to come back with a prototype, go make it happen.

And so, a lot of companies will use the design thinking approach, where you bring in some users, you have them do some observational studies of them. You look at the problems they have, you synthesize it, you start building a prototype. And you use that as the framework for the hack day. So, they're still building software, but they're thinking about it the way a designer would think about it, not the way an engineer would think about it.

Another approach is to have the kickoff of every project, and this is the approach that we got more traction with at SAP was, at the beginning of each project, you would have the team go through this exercise and have about a two week deep dive using the design thinking framework to drive a new model or a new paradigm.

And then, longer term, just having the team, if they use an Agile development process, for example, like, a two week design exercise, where they can apply those same principles to refine the current product that they're working on. So, if there's some, just kind of, rough edges to the thing that they're working on that they need to smooth out, or there's something that they just haven't been able to quite solve yet. You take a two week sprint and just have the team focus on solving that problem, using the design thinking method.

So, there’s a couple different ways like that that you can roll it out into a company.

Thomas: So, if we talk about design in automotive for a moment, in the automotive industry. When you build a car, there are certain constraints. Some of these constraints are set by law. Like, it has to have air bags, it has to have, a certain fuel economy and all the rest of it. It seems to me that car designers are relatively aware of the legal constraints in which they operate. They will take those legal constraints and build them into the process of designing the car. Whereas, with software, it seems that that’s not always the case. And so, what I’d like you to maybe talk about is a little bit about how you see that. And do this broadly at an industry level, don’t pick out one company. But how the design process links into accessibility or not.

Matthew: Yeah. It’s mostly the “or not” part, unfortunately, I think, from my experience. I think, unlike the auto industry where the consequences of not complying with the regulations have often fatal consequences for the people using your product, the lack of compliance to those similar laws in the software world doesn’t result in the same catastrophic outcome. I think that a lot of companies are willing to play the numbers game and say, there’s only such a small percentage of users with this particular disability, therefore, we can write off that part of the market, if they don’t like our product or if it’s too hard to use. Or we’ll just rely on the operating system to take care of this for us, because the major operating systems are much more compliant focused, because they have to sell their products to the government.

Most of the individual software companies, the bigger ones that have government contracts, tend to build in more compliance. But, often times, they make it a modal switch in their application. So, it’s kind of like you go into the accessibility mode, as opposed to a graceful degradation kind of thing, into an accessibility path, or building it into the websites, for example.

They rely on the browser to manage most of those issues for them. So, if they need to increase font size or contrast or if they need to do text to speech, they rely on third party applications, the browser and the operating system, to provide that for them. Which is unfortunate, because the sites that do build in the accessibility issues into the style sheets of the websites or into the software that runs on the desktop, have a much better experience with users. They don't have the challenges that…

Thomas: They're for disabled and non-disabled users in that context, you mean.

Matthew: Yeah.

Thomas: So, you'd say that, I don't want to put words in your mouth here, but you would say that the private software companies on the whole's take accessibility as haphazard.

Matthew: At best, yeah. And I think, I've worked in some companies where they specifically just take it off the table. I mean, their approach is simply just to say, we're not going to do it. If they get push back from a user group or, you know, there used to be more advocacy groups that seemed to be more prevalent back in the '90s than there are now for this kind of a topic, but unless they're really pressured into doing it, or contractually, they have a requirement to do that, like to sell software to a state or federal level, they usually are pretty much haphazard at it. The exceptions have been companies where family members of the executives actually have these types of logistical challenges. And those people tend to be much more sensitive, because they have a family member who actually has that same issue.

Thomas: Right, right. So, if we're going to fix disability in the software industry, we need some more disabled software executives.

Matthew: Yes, and not just emotionally crippled, but, you know…

Thomas: Yeah. So, in terms of the education of designers, then, do you, in the education process, do they actually look at accessibility at all? Is it something that they, you know, if you take those programs you mentioned, do they actually talk to you about designing for, say, visually or aurally disabled people, or is it just kind of, you pick it up a little bit here and there?

Matthew: It's primarily, you can pick it up here and there. Some of the programs do focus on it more, but it really depends on the faculty. There's a fellow that I knew at San Diego State, who teaches in the industrial design program, who actually has a strong interest in designing for aging. And so, within his program, he actually has a class that focuses on how to design simple utilities around the house. Like, bowls and plates and coloring for people. He also has worked on projects where he has students that work on things like walking sticks and canes that are well designed, sustainably created, but also improves the mobility of the people using them. And so, in that case, there's more focus on the accessibility issues.

But most of the programs don't really do much about it. You might have it as part of a class, but there's no, I'm not familiar with any ACI program for the human computer, actually, a piece of software design.

Thomas: Right.

Matthew: But that actually focuses on that specifically.

Thomas: That's interesting with the aging angle, because I picked that up a bit in my research, that if you start to include an aging population, then the ratio of disability increases quite dramatically with age. So, it might be, you know, in a bit, at fine motor skills for mouse usage, or it might be a sight or hearing. So, do you think that we're going to see improvement in the longer term or do you think it's still going to be an area that the industry largely ignores?

Matthew: I actually think it’s going to be a much bigger issue moving forward, I think. The baby boomers are much more vocal, much more well organized and have a lot more discretionary income than their predecessors. And I think that the baby boomers have forced a lot of changes already around other aspects of health care and of other things. They’ve kind of redefined what it means to be getting old. They’re much more active and they spend a lot more money, they travel a lot more. I think that generation’s going to drive a lot of expectations around accessibility, at least for aging issues. I think that they are technically savvy enough to basically make informed purchase decisions that can be partially, if not completely driven by their ability to actually use the device.

So, unlike their parents, who probably got a computer because the boomer bought it for them, the boomers will buy their own computers. And if they don’t like the computer because it doesn’t allow them to actually surf the web, send email, do whatever they’re doing, they simply will move on to the next device and see what else they can find.

Thomas: Or, indeed, lobby for legislation.

Matthew: Right. Yeah.

Thomas: Because there is, actually, legislation in many countries around disability. There’s quite strong legislation in the UK, for instance. And in the US, there are, there’s relatively strong legislation in public sector. And in fact, there’s a case going on at the moment where Target have been sued by the National Blind, the Association of Blind People in North America, arguing that the ability to buy online is the same as going into a shop. And you can’t, according to the disability regulations in US, you can’t say to somebody who’s in a wheelchair, hey, you can’t come in this shop. You have to open the shop up.

So, I think that there are some, there is some activity on the legal front there. I think that the challenge is not so much that there aren’t laws, but the laws aren’t clearly articulated and defined. So, in other words, if I want to build a payroll, you know, I'd phone up the Department of Taxation, and they send me a specification. If I was to phone up somebody about, asking about accessibility, I get very limited information in order to do that.

Matthew: Yes. I know one of the companies here in the Valley, it's a really large company, it's one of the largest networking companies, they have one accessibility person for the entire company. And it's just not something that is a high priority. I think a lot of people just assume that you have to have sight, you have to have hearing, you have to have good motor skills to use a computer and they just see it as the price of entry.

And I think even if the regulations were clear around how to do it well, my experience has been companies would still prioritize this relatively low based on the way that they prioritize features and functionalities on ROI and market position.

They wouldn't necessarily see this as a core competitive differentiation because their competitors aren't doing it either. It's kind of like sustainability. Until somebody starts a way to make money off of it, nobody's really going to pay much attention to it. Or until the regulations become some onerous that you start losing substantial money because you're not complying with it.

I think as long as there's neither a positive or negative influence financially on their spreadsheets, there's not much of an incentive to move forward, even if they have access to that information.

Thomas: Right.

Matthew: I mean, morally and ethically, I think everybody's keenly aware that they should be doing this, it's the right thing to do. And they might hide behind the excuse of saying, "I can't get to that information." But my experience has been more around if there's no financial gain or financial impact, there's not much of an incentive to do it.

Thomas: Right. And moving on just quickly, because I know we're running out of time here, but privacy-wise, would you say it's similar? Organizations are really not aware of privacy regulations and haven't really thought about how to architect them into products? Would you see that in the same light, or would you see privacy as differently?

Matthew: I think privacy is changing. I would have said privacy was similar a few years ago, but privacy's always been an issue for the Internet. Whether it's storing a credit card or your home address or your telephone number, people have always been skittish about sharing too much information with their software companies. But I think now more than ever, people are becoming more keenly aware of the privacy issues, because of things like Facebook where that information is just so out there and there's so much of it.

And I think that unlike accessibility, where a percentage of the population is impacted by a software company's failure to provide accessible solutions, everybody is impacted if a company's extracting too much information and using it for their own personal gain and potentially damaging people.

I think there's probably a greater backlash against the privacy issue than there is against the accessibility issue, just simply because the numbers are bigger.

Thomas: Right. And are you seeing an awareness of privacy in design? The reason why I ask that question specifically is that there's a push by the European data protection authorities. They've launched a project called 'Privacy by Design', where they actually want design principles of things like less data, more secure data, ability to delete data – those basic privacy concepts embedded in software design from the beginning. Do you think that's likely to get some legs? Are we going to see designers actually understanding the nuances of privacy, or is it something that gets engineered in at the end of the process?

Matthew: Well, it's interesting. I think most of the designers I know are probably more sensitive to the privacy issue than their development or business counterparts, and I think it's because of where design sits in the relationship to the consumer or the user of the software. I think the challenge has been that in order to provide the high-quality service that users come to expect, you have to know a little bit more about them.

If you go into a bricks and mortar shop to buy your suits and ties, the longer you keep going back to buy suits and ties from that store, the better the service gets, because they know that you like a certain cut of suit or a certain color palate for your ties. But we don't really think of that as a privacy violation, because the store owner just has a good rapport with you, right?

But with a website, the challenge is that it's much easier for a website to take that same information that drives the rapport, and sell it to 50 other companies. It's much harder for the guy at the haberdashery shop to take all that information out of his head and put it in the hands of all of his competitors.

And I think the issue is that designers try to inform users of the benefit of doing this and they also will put things in place to let them know what the company's intentions are, but the problem is the companies change their intention. It's like Facebook changes its policies and publishes them on their page, but they don't really tell you that they've changed their policies.

Thomas: Yes.

Matthew: They'll reset your privacy settings as part of this policy change, and if you go dig through their announcements on their "About Facebook" page you can find something about it but they're not really working very hard to inform their users that these changes have happened.

Thomas: Essentially there's an anti-patent there.

Matthew: Yeah.

Thomas: Facebook has an interest in gaining as much information about you as you can and being able to as widely distribute that information as they can. But if you move away from Facebook and we talk about, you mentioned a financial software company earlier, do you think those organizations, are they taking legal requirements into account? Do they understand this is the European law, this is the US law, this is the UK law, this is the Canadian law and so on? Have they got that connection between the legal stuff and the software code or is it just privacy in sort of a vague sense?

Matthew: I think when you get into the financial and health care space the privacy is much more serious. Even just experientially on the sites that you go to or the software that you use from those companies, it's much more prevalent. It feels like you're really going into something that's far more secure. You get emails from them that say, "We've sent you an email. Please go to our website, log in and you can read the email." Then you log in and you have to go through two or three more steps to acknowledge the privacy steps and then the email gets displayed to you. I think those institutions tend to focus more on it and do a much better job of understanding the regulations.

I think from the consumer's perspective though, given that they probably went to their banking site or their health care site right after looking at a post from Facebook, they see all of those things as having some level of sameness to them. I think the challenge is that it's so easy for people to move between the non-secure, non-private focused sites and the very secure, very private sites that the contrast becomes much more salient and that contrast becomes the awareness and the concern about it, because it's really evident some sites aren't and some sites really are. That makes it much more evident to people that there's a question that needs to be answered for them.

Thomas: Right, right. OK, that's cool. What else did I want to ask you? In terms of going forward, going back to the design that's called a profession, are you seeing a growth in demand for software companies for this resource that sits between the customer and the developer, this designer? So the methodology and the practices is working in the market, seeing benefit, that software companies are seeing benefit from the designer concept?

Matthew: Yeah, I think more so now than ever. I think in the last couple years, consulting with a number of different companies, even early stage start up companies with two or three people in them understand they've got to get a designer in there to help them figure this stuff out.

Thomas: Right.

Matthew: Previously the designers would come at the very end so they would create a product, they'd create a website and then they'd hire a designer to tart it up and make it look pretty.

Thomas: Right, right.

Matthew: But now they're realizing that in order to really have the value differentiation up front and really make a product that people want to use, they've got to get the designers in at the beginning. And there's a lot more designers who are either starting new software companies as a co-founder or who are in executive positions in the organization to help drive programs and strategy. And a lot of the designers are actually changing t heir career paths to go more into product management or development management.

Thomas: Right, OK.

Matthew: So they still bring the design sensibilities to the task but they might be the head of product management for a company and not a designer per se.

Thomas: OK. So if we go back to the accessibility and privacy question in that context, if we look to the future where the software industry is probably where the car industry was in the 1920s, there wasn't much regulation, we could build pretty much what you'd like and there wasn't a market for seat belts because if you gave me a choice between having more horsepower or having a seat belt, I'm going to choose the horsepower because I'm immortal. That was kind of the automotive industry, let's say, even in the '40s or the '50s. And then with the automotive industry basically compliance drove a change in behavior in the automotive manufacturers, and the education program then drove a change of behavior in the consumer side where consumers actually started to say well actually it's a pretty good idea that I wore my seat belt. But that exercise took 30 or 40 years to go through that cycle from no compliance to a relatively compliance driven development process.

I'm kind of postulating that in software we're at a point where we're going to start having more compliance factors into software. As software takes over more of our lives, does more of our things for us, software designers will come more in contact with compliance related issues but at the moment I'm seeing a total lack of focus on those compliance issues in developer and designer education. Would you agree?

Matthew: Yeah, I think overall it's on a very much faculty by faculty basis in the design education world. If you faculty that have worked on projects like that or done consulting on those types of projects it shows up more. I want to go back to the car analogy because it's interesting that in the '20s the volume of cars on the road was still pretty low despite that it hit in the '50s and '40s. Coming out of World War II there was a lot of learnings around things like seat belts from aviation and planes and a whole bunch of other things, and a lot of people's lives were saved by those types of technologies and devices. That transitioned into the consumer space then when these guys came home and started driving around with their kids and their wives and the seatbelt thing became a bigger issue for them.

What's interesting is that we definitely have a seen a massive spike in people online. The volume of traffic in the software world, the digital world, has really gone up, but there hasn't been that global epiphany around what safety is for the Internet, whether it's privacy or accessibility.

Thomas: Or there's SPAM.

Matthew: Yeah.

Thomas: There's a whole bunch of identity theft. I think there's a bunch of areas where security and safety and those things are still largely ignored or there's less focus on them.

Matthew: But the people providing the mechanism…you could still have people standing by the side of the freeway throwing rocks at your car, right, which is kind of the SPAM thing, but there's only a dozen or so car manufacturers globally that really matter from a market sizing perspective. But from a software perspective there's still thousands of software companies out there and it's too easy for these small guys… Think about even Skype, it started off as a very tiny little company that has been sold five or six times for more money each time. It started off as a very small thing. I'm just wondering if there's a proportionate thing where it's like you have thousands of software companies versus a dozen car manufacturers and it was much easier for the entire consumer population to look to those 12 companies and say, "Make your product safer," than it is for them to point to thousands of software companies and say, "Make your software safer." Because there isn't…

Operating systems are the exception because there's really only two operating systems so it's much easier to point to those two companies and say, "Make your operating system safer." I'm just wondering if there's something where there's a ratio problem. It's just too easy for very small software companies to show up, provide software and be very intangible, kind of hiding in the background somewhere.

Thomas: Yeah, I think you’re right. My personal thought is this is only going to drive, this is only really going to come if there’s more legislative pressure.

Matthew: Yeah.

Thomas: If there are more fines and more shutting websites down and so on. And then on the privacy side we do see a little bit of that in Europe but not a lot. All these dynamics come together, I think.

Matthew: Yeah. It will be interesting because I can see for companies like [inaudible 32:59] , the big software companies like Microsoft, Apple or someone like that, Intuit, Adobe, levying fines against them would have consequences. But if you have a three-person start up company in Estonia who’s built some really awesome piece of software that people just love but it’s very dangerous from a privacy or accessibility perspective, and somebody swoops in on them with a big fine, it’s three guys working out of an apartment above a bakery somewhere.

Thomas: Sure.

Matthew: The next thing is they turn into a hacker and release the software virally somewhere. It’s going to be an interesting challenge.

Thomas: I think for the formal interview now I’ve got lots here that’s been really useful. I think this will make a good addition for the disc, so from that point of view I’m going to stop the recording now

Appendix C Liz Buck interview transcript

Thomas: Liz, maybe we’ll kick off. If you could just give me some background on yourself, what’s your involvement been in payroll, and then perhaps a couple of minutes on what Ultimate Software do.

Liz: OK. My name is Liz Bucko. I'm the Director for what we call the Foundation, which is really the transactional parts of Ultimate Software. I run the product management group that works closely with our development team to develop and maintain what I would call the transactional areas of our products. Payroll, tax, tax filing and time and attendance, so the core transactions that build the pieces of an exigent system that result in an employee getting paid. Then, I'm also on compliance. I come from a background, originally, in accounting. I worked with Ernst & Young for a while doing state and local tax consulting, and then also worked at a company called Ceridian. That's also in the same HTM market, a little bit of a different spin. They're more of a service bureau than Ultimate Software is. But I worked there for 14 years before I became …

Thomas: Your academic background is tax?

Liz: My main background is tax, correct.

Thomas: OK. Then Ultimate, as a company, they do HR and payroll systems in the US and Canada?

Liz: US and Canada, correct. Some global employee administrations, but for the purpose of the foundational components, we do not pay global employees.

Thomas: Talk me through. This has got a really high level guide to how the payroll process works in the US. You've got states' and federal rules. Let's imagine you decided, "Hey, today we're going to build a payroll." How would the process work?

Liz: The United States has pretty complex tax law in that you can have a federal law, a state law and, actually, even a local law to the city, or school district even within some of the states, to those areas. The way that most of the laws read is that, whichever one is most favorable to the employee is the one you implement. Even if federal minimum wage may be one rate, a state minimum wage may be higher, and so, you have to go with that minimum wage. There's a little bit of complexity there. Canada's a little bit more simple because, for one, their taxing system is much more straightforward, and there's fewer provinces and, within the provinces, you have less likelihood, at this point, of varying regulations.

We do both of them, and because they're of the complexity and the diversity in laws all the way down, like I said, to the school district level in the United States, there's a lot of services that I would call employment legislation aggregators. There's a company called CCH. There's a company called B and A. The American Payroll Association is good at aggregating. But they all send out what I would call spools of upcoming legislation, just passed legislation and break it down to the impact to employers.

Typically we keep a watch on all of those spools. There's several publications that we subscribe to so that we know what's coming. Then we have contacts at every state to help work directly with the states when things are coming through, and then to get people who obviously are in charge of the federal and provincial and then the Canadian.

I have five people in my compliance research group, and they each own a portion. They're in charge of staying ahead of the legislation in those areas through these services but also through their own individual contacts at the state and individual research. Part of their day, every day, is spent just looking at what's coming.

Thomas: Maybe let me just take you through an example. On the one hand, a lot of those updates are going to be relatively simple. They're going to be, essentially, in technical terms table data changes.

Liz: Right, like the rate.

Thomas: The rate goes up; the rate goes down. That's essentially an exercise of configuration of a system to maintain it. But let's say for a moment there's a new rule that comes up, a totally new rule. Let's say that the State of California decides that, if you have a company car and it is an eco-friendly company car, you get some sort of reduced taxation. I'm just making this up. That would require somewhere in the system that you would actually have to capture that information about that eco car.

How does the process go from, you find out about a rule, and then you end up having to build that rule into the system? How does that process work?

Liz: There are tax research analysts, one of those team of five who keeps up with the laws, probably when it was coming down the pipe if we had enough notification, if not, once it passed but hopefully before it was effective, would get all those requirements together. They typically come in the form of an IRS code change or a California code change. They typically print out all the legalese around it, and they work with what we call a product analyst. The product analysts are actually the people who are going to convert that legalese into requirements for our developer to code from and for a quality assurance tester to create test cases from. They're what I would call the middleman between jurisdictional tax research analysts and the developers.

They would take that requirement and, in working with the tax research analysts, they would convert it into what we need to do in products. We need to add a data field to support the eco-friendly car, and then we need to reduce taxes.

If you're in the State of California and you're paying this, you reduce it however the law reads, like this. That product analyst would take it and convert it into what the developer needed to do, and obviously the tester would write test cases to support that.

The product analyst would also prepare customer-facing documentation to help the customers understand, if you want to have this tax reduction, you will need to go in for everybody with a company car and mark this eco-friendly box, and perhaps answer the five questions California wants you to answer. You know, date of purchase, manufacturer, model number;

whatever you need to track to get that tax credit. Does that answer your question?

Thomas: It does. Yeah, it does. You mentioned briefly the differences between U.S. and Canada. Can you expand on those for a little bit more for me?

Liz: Canada basically has what they call payroll deductions, but they're similar to taxes. In the United States the frequency at which you have to withhold them every payroll. You don't have to deposit them or report them near as frequently as you do in the United States. For most customers, because it's a flat rate, it's for all employees, there's not a whole of tiering, or looking at well they live in this province, they work in that province, and they spend 30% of time in yet another province; there aren't the complexities in Canada. It's a lot easier. Plus there aren't the complexities that the United States has with deductions like health care and things like that; that are pre-taxed in some states but aren't pre-taxed in other states.

In the United States only a portion of a deduction can be pre-tax. Let's say you have a domestic partner, and you have health care coverage for your family. In most states even though domestic partners can be covered with your family plan the portion related to that domestic partner is not pre-tax. We don't have those kind of rules in Canada. It's just more straightforward to code, but the process for coding it is the same.

My analyst who's in charge of Canada gets the change in Federal and Provincial Law in Canada, works for the product analyst to interpret it into product requirements. Obviously, you've been around products a lot of your career. Any time you have to add a data field, ask clients to update something, or automatically update something for clients it's more complex. If it's retroactive it becomes much more complex, or if it adds a look back. It just depends on the complexity on how long it takes, but that's basically how the process works.

Thomas: How do you--what sort of training, I'm especially interested in that high red wall between the developer and the payroll. What sort of training do those people have? Do courses exist and so on? Does the government provide any training about payroll, or is there training done by an association; how does that work?

Liz: All of our tax research analysts--or most of tax research analysts, and our product analyst in the compliance area have a certification that's call a CPP. It's given by the American Payroll Association--so it's an association certification. It stands for Certified Payroll Professional. Basically it means they've been through a course, and then taken a test that tests their knowledge of the payroll area. That includes a pretty heavy section on compliance. Additionally, we have a CPA on staff that's a certified professional accountant that helps with that in an advisory role for all of Ultimate Software at the product world. He works in development. He's not like someone who works in corporate. We have a CPA in corporate too, certainly, that does our finance stuff but this is someone who works in development that all he does is helps makes sure the accounting law we're abiding by, especially since we've added our tax filing services.

Thomas: OK. In the US are there bodies that actually certify your product? For instance the UK tax authority, the HMIC, actually has a certification process where they'll check the product and give you a stamp of approval about that payroll. Is there such a thing in the US?

Liz: Not for compliance. There are certain things you can get for your coding methodologies and things like that but not a government seal of approval that you're complaint in the way you calculate. One of the steps we do in that tax research – I'm not sure what other vendors do – I know Ceridian did it as well, but once we have the calc written, the requirements for the calculation, that tax research group takes it back to the jurisdiction and gets written confirmation that we've interpreted the legislation appropriately, usually provided with examples of how that calc was resolved. We get that confirmation before we put that code into an official build of our software.

Thomas: Right. Do the authorities come to you guys and say we're thinking about this new rule. What kind of impact is it going to have on your product?

Liz: They do not.

Thomas: There's no communication? They just pull the law out of the hat and say this is what it's going to be in three month's time, we're going to pass it and get on with it?

Liz: Correct. There are members of like the American Payroll Association that have lobbyists out there that try to work with the different jurisdictions to make sure that they're creating legislation that can be supported by service providers and software creators because sometimes the legislation is so complex it's virtually impossible to implement because maybe they're requiring nuances that are very difficult to systematically deliver.

Thomas: Would you say today that it would be almost impossible to calculate a payroll manually in the US?

Liz: It would be almost impossible to calculate a payroll manually in certain states in the US and after a certain threshold of employees. I think a dozen employees and you're in Florida, where they have no state income tax withholding, you could probably do it. It'd be timely, but anything over about 25 employees I think it'd be virtually impossible. We have a new piece of code, for example, that came through effective August 1st and to manually calc a single employee it takes even me, I'm fast, I'm fast at calculating. I'm not good at a lot of things but I can calculate really fast, and it takes me, using tools like Excel, it takes me about 45 minutes per employee to calculate a paycheck.

In many, many states like California, Connecticut, New York, the states that have a lot more people in them and therefore a lot more employment, or the states that lean to be a little bit more liberal, it would be impossible to even do a 12-man payroll.

Thomas: So, in Massachusetts, for instance, you couldn’t do that. To do that manually would be hugely challenging.

Liz: Yes. To do it manually and have faith that you’ve treated everything correctly. But I think in the US we have a lot of places… There’s a tool built by Symmetry Software – I don’t know if you’re familiar with them--called PaycheckCity.com. That, for a simple payroll, for free you can go online and enter the components and it will do the calc behind the scenes. A lot of states have published calculators on their websites. And the reason they do that is for those lower-end employers that have six to 10 employees and don’t really want to pay the price.

Ultimate does not service employers that have under 200 employees. A lot of the US businesses are small businesses. If you look at the census unit, that’s the bread-and-butter America, in these little, tiny businesses, mom-and-pop shops. You get employers with six to 10 employees and a service would probably cost them $15 to $25 per check. That’s a big hit if they can just go onto the state’s website and manually calc it. Not manually, but you know what I mean, without using a service.

Thomas: I’m just trying to think how to phrase this question here. Give me a second here. My mind was going somewhere else. How do you communicate to the customers? What’s the process by which you educate your customers?

Liz: There’s several ways, and this is not detailed in the document I’ll send you. This is probably something that you’ll definitely have to get back to the recording and listen to. But, after each release of the software, which, sometimes tax legislation can be put in a release and sometimes it has to go out immediately because of timing, we do webinars that focus on just what’s in there. There’s a whole section on compliance and payroll. Obviously, the Canadian and the US audiences get separate webinars to detail what we’ve delivered for their market in that release.

Especially things like healthcare reform, which is a multi-year Act passed in the US--I'm sure you're familiar with it--that the legislation comes in at different hits. What we're trying to do is get way ahead of that so that we can have focused webinars. When that law came through, we did just a Healthcare and HIRE Act webinar for our clients.

We also have a blog that I post on regularly. I would say, almost daily. On the blog we try to educate our customers not only on employment legislation that they'll need to use our product to support, but also employment legislation that they'll have to change their processes to support. So that, we're more wholistic. Versus just saying, "Here's what our product does," we say, "Here's what the law is, and here's the pieces you can facilitate in our product. Here are the pieces that may require process changes."

Then, anything that's urgent, so let's say we get… Unfortunately, the lobbyists have not been able to get much of anywhere with the flurry of retroactive laws that are being passed so we're having laws passed, not in Canada so much as the US, where they pass a law on August 1st and it's effective January 1st of the current year so you have to go back.

If we have legislation like that that we have to build really quickly for we'll publish what's called a news wire that actually goes to people's email boxes and says hey there's a change that's coming up immediately. It's going to be applied tonight. Here's the impact and here's how we're helping you.

Multiple ways of communicating depending on the urgency and what the client needs to do to prepare for it.

Thomas: OK. Just talk me through how this works in a software as a service model for a second. My understanding is, this is more for my notes than anything else, that Ultimate runs the vast majority of their business on a SaaS model, software as a service model. How does the software service model impact how you support your clients from a payroll point of view?

Liz: SaaS makes it easier. For one, software service you have less customization. You have a lot of what I call configuration or customer specific design work but not a lot of customization so it's very easy when I have those late-breaking laws, as I like to call them, to go and just update my whole SaaS farm and then I know the client is current. I'm not asking them to do something that maybe they've got because they have it on premise they've customized or they have developers that are going to have to work with it. They can pretty quickly adapt in a SaaS model to getting that through. With the blog, our blogs are pretty readily watched by clients for compliance.

Actually, the number one thing people hit our blogs for are the compliance postings. Then email, I can get to them pretty quickly and say tonight I am updating every client with this tax rate. It's retroactive so I'm going to do some updates to their history. Here's what you'll see, here's your expectation.

With the SaaS model, personally, having worked in a mainframe model, true service bureau for years, it's much easier to get clients updated quickly and stay on top of the legislation. Was that your question, Thomas?

Thomas: That was exactly. That was exactly spot on. Spot on. I think this is probably what I need, Liz. I think this is pretty much nailed what I need here. Just to summarize to see if I've got this right, for payroll there's a pretty clear defined process in how you work with the various governments to get the information. There's aggregators that help you collect the laws, but through direct contacts and also through the payroll associations you have reasonable good dialogue with the authorities so that much of the time you tend to know in advance what the legal changes are going to be. Then when you understand what the legal changes are going to be you have people that are able to assist the legal changes and then convert them into a specification that a developer can then work with.

Often you validate those specifications back with the authorities. Then when the changes are then made, obviously you test them based on test scripts, and then once you've tested that software, you then deliver it through the Software as a Service model to your customers.

At the same time as you deliver it, you provide significant education services to those customers about what those changes mean, both at a legal level and also at a process level.

Liz: Correct.

Thomas: OK. Cool. It's very different from how people handle things like accessibility.

Liz: Oh, very different. Obviously, accessibility we have to work with, and it's unfortunate but having, let's say, a page or something that someone who is hearing impaired or sight impaired, can't manage, better example, isn't as urgent as getting a paycheck wrong. [chuckles] I don't know why, but it's a very different process on how you work through that. I assume when you were talking about accessibility you were talking about …

Thomas: Exactly. Yeah, because I've just been checking out some other research, and something like 80 percent of websites aren't accessible.

Liz: Right. On a tangent, just, we have done some work in our software this year for accessibility because of people who have braille writers that pop out of the software or things like that they need – or readers that will say it out loud – because they're blind. We've done some work in the software, and it's really difficult work to do. Trying to build that into every requirement has not been easy, but we know we need to do it.

Thomas: Right, and have you found it hard to understand what the requirements are?

Liz: For accessibility?

Thomas: Yeah.

Liz: I found it difficult because it’s so broad, really, and I think that the laws in the United States read something like “reasonable.” When there’s a word like that in the law, reasonable to me and you might not be reasonable to the guy who can’t see. There’s a lot left over for interpretation there, and certainly you want everyone to be able to. The reason a decade, a decade and a half ago, all these vendors came out with self-service softwares was so employees could see their own stuff and manage their own stuff. You certainly wouldn’t want to discriminate against anybody just because he can’t see.

So I struggle with any … Tax laws, the word reasonable never goes into a piece of tax legislation. It is black and white. There is a right and wrong answer. A lot of the other legislation that is on the broader HR realm has words like reasonable in it, and that makes it difficult to know how far you go.

Thomas: Yeah, but you guys have done work to cover accessibility, for instance, on ESS and stuff, so.

Liz: We have. Like the paychecks, the W-2s, things like that, all of them automatically pop out in a PDF. Most of the companies--Adobe is the primary one in the market, obviously, that does PDF readers--they have pretty high accessibility functionalities. So by doing that, we’ve made it where you can have any page in a PDF and that will make it where you’re accessible. But as we’re continuing to evolve the product, you want to make it natively accessible, not just by popping it in a PDF.

Thomas: Yeah, sure. OK. Cool. It’s kind of interesting, because that’s the area I’ve been looking at, and it’s just amazing that the average developer ignorance on accessibility is quite horrifying. It’s very interesting to see, comparing one set of laws where the industry has sat down and really made a plan for, in this case, payroll, and you have another set of laws that are equally important yet are largely misunderstood.

Liz: Even if you read through some of it – I'm sure you have in your research – they leave a lot open for interpretation, which makes it much harder to implement something in a software system. So I would say that, the fact that I have a transactional staff and there's lots of players… Keeping up with the legislation is virtually impossible and overwhelming. Every day I get on phone calls with customers who have interpreted the law one way, and it's not the way we interpreted the law, but you ultimately have a state where people say yes or no. I don't think accessibility and some of those broader human rights type laws have as much of a black-and-white interpretation. That just makes it difficult for everybody, and especially the employee, at the end of the day, who you're trying to accommodate.

Thomas: Yeah, yeah. No, I would agree, and there's not clear case law. It's generally a mess.

Liz: Yes. Do you have any other questions?

Thomas: No, I think I'm pretty much done. This has nailed exactly what I wanted. As I say, what I'll do is I'll get this sent over to the transcript person, and I should have it back in about a week or so.

Thomas: Thank you. I will do, Liz, and thanks very, very much for doing this. It's really, really very kind of you.

Liz: My pleasure. Have a great day.

Thomas: Thank you. Bye now.

Liz: Bye-bye

Appendix D Nigel James interview transcript

Thomas: OK. I'm back on. We're all on here. OK. We're starting now. OK. So Nigel, just kick off, give me a little background about yourself, where you've worked, what you studied, and so on.

Nigel James: Sure. So I work as a freelance software developer working mainly in the enterprise software space with SAP clients, basically. So I work normally with end user clients or through a system integrator to an end user. That's about 95 percent of what I do. I did a bachelor degree at Macquarie University in New South Wales, Australia where I did a Bachelor of Information Communication Systems. Sorry, it's a long name. Bachelor of Technology in Information Communication Systems which is kind of like a computer science degree with a few other little bits and pieces, to make it something different, with a long name.

Thomas: All right. Was it a three year or four year degree?

Nigel: It was a three year degree. Most degrees in Australia are three years unless you're doing honors, unless you're doing architecture or law or other silly things, but then, they're standard long degrees. It's just a normal undergraduate three year degree. I kind of came to that as a mature aged student and decided to change from working in retail to go into the wonderful world of computing and decided that instead of either a short vocational nine month major in [inaudible 01:41] course or a polytechnic course that a university degree would be better in the long term. So that's what I did. Then I got a graduate position with [inaudible 01:56-01:58] and went into their SAP group and the rest is history.

Thomas: OK. So where in the world have you worked?

Nigel: Where in the world have I worked? New South Wales, companies like the Australian Broadcasting Corporation, Westbank Bank. I'm currently working with BOC, the gas company. They sell cylinders of gas to various recipes. I also worked in the UK, in Europe with companies like

Shell, Xerox, Schlumberger. Schlumberger is just Schlimmer, who sort of bought and sold each other out at different times. Companies like Marstons and a whole bunch of county councils, like London boroughs, like Suffolk, Surrey County Councils, and probably a whole bunch of others.

Thomas: OK. So broad experience. What particular applications have you focused on? Is there any particular type of application you've been centered on?

Nigel: Sure. So I've done early in my career, like 12, 13 years ago, I started out basically doing logistics and materials management, a little bit of finance and banking work, as in electronic banking statements, so that the banking statements would come directly from the bank into SAP and be read and passed automatically. From then, basically HR. I've probably done about four to five years worth of HR and about the same of CRM and then a few bits of [inaudible 04:06] . Let's take SAP and [inaudible 4:12] it as much as we can, kind of roles.

Thomas: OK. So you have access to both end users and also you get quite technical so you do actually code stuff?

Nigel: Yes, I do actually code stuff. That's a lot of what I do but not all obviously. Coding's not the whole thing of coding.

Thomas: OK. So moving on to the main theme of this. You answered the survey and you actually helped me in publicizing the survey. You helped push it across the web. I ended up having about well over 500 responses.

Nigel: That's very good.

Thomas: I feel that turned out pretty well. If we go back to your education a second, during your course did you get any exposure to any of the legal issues around software, either in terms of the IP issues or in terms of the issues relating to law when you actually code stuff?

Thomas: The short answer to that is no. As I said, my course wasn't just a pure Bachelor of Science degree but it was kind of that degree with a long name. I won't bother repeating it. I so we did have subjects other than just pure computer science theory subjects. So we had some things like communication and management and those sorts of things. But we didn't have any law components at all, at least not the ones I went to when I went to university, had any law components aside from doing a double degree with a law school or something like that.

Thomas: Just to make this clear, you weren't getting any exposure to any of the basics of what a contract was, any of the basics of privacy or accessibility or any of those sort of legal concepts? None of that was really taught to you in an academic context?

Nigel: No, not at all. It was all basically computer theory and different programming languages and different algorithms and how to write other ones and a few other bits and pieces but nothing to do with what clauses to put in an end user agreement or a privacy legislation or any of the things around where data is stored or anything like that. None of that at all. The context for that was that I was studying between the years of, let's remember correctly. '96, '97, '98 are my three years at university so the Internet was still very young and a lot of that stuff still hadn't really been threshed out. Of course, the whole packaged software, shrink-wrapped stuff was still very thin, but no one said if you're running a product then you need to put a [inaudible 07:43] in it and disclaim all warranty of anything that might drop a plane out of the sky or anything like that. No discussion about that whatsoever.

Thomas: None of that was covered at all as part of your education, despite the degree being positioned as a sort of management-meets-development qualifications?

Nigel: Yes. Yeah.

Thomas: All right. That's interesting. If we talk in a practical concept then, now over the last 15 years of working how have you actually informed yourself about those kind of issues, assuming you dropped a few terms there, so you do know a little bit about this. How did you educate yourself on those topics?

Nigel: Really by osmosis, I'd have to say. I'm dropping the terms, but let's not pretend I'm a lawyer and specialized in this sort of thing. I talked to an IP lawyer at a party once. I don't think that really counts as being informed but you pick up some of the lingoes. You kind of become a little bit aware of the conversations around privacy and if you've got a website you've got to have a privacy statement and these sorts of things prominently displayed. Just through I guess various online sources where developers go to hang out and be educated about technical things and then they also seem to have a few legal things or the other concepts around what you need to have on a site. So really only those sorts of things. It's not like I actively sought out data protection law or those sorts of things.

Thomas: So if we talk about data protection law for a second, you've worked with some pretty big companies around the world and as part of your work you've been working HR systems and CRM systems, both of which process personal data.

Nigel: Indeed.

Thomas: In those organizations, what sort of guidance and focus did they have on data protection? Did you receive clear guidelines as a coder about what you should, what you shouldn't do or were these things largely ignored?

Thomas: I'd say it's somewhere between clear guidelines and completely ignored. Most corporate systems you sign onto either at signing onto the operating system or signing onto SAP software, you get some sort of message to say, this is largely ignored. It's like the thing you just click through. But it's got a statement in there saying, this is for this company's systems only, and any misbehavior will be frowned on with a very large frown.

Thomas: Yeah. Maybe I can give you a practical example. Have you ever used live data for testing purposes?

Nigel: I would have to say, in most situations, and for, say, a big company like [inaudible 11:15] , where we did live upgrades and those sorts of things, or even Shell, where we did a live upgrade, that 90 percent of the time you're working on a development or a testing system. And in those systems, you've either got a very, very small data set, which has been grown yourself, or it's been a small subset of productive data to encapsulate the whole productive scenario, but it's been copied back and obfuscated or randomized in some way, so that you can't really tell.

Thomas: So you are seeing companies actually do the obfuscation and randomization of test data. That's good.

Nigel: Absolutely. Yeah.

Nigel: Yeah. We generally use tools. And there's a couple of tools, particularly for SAP HR systems, because it's such a big issue that there's software that will copy back from a production system. They give you tools to say "Make it John Doe one, two, three, four" kind of thing, instead of "CEO" or whoever.

Thomas: OK. Now, moving on from privacy for a second, if we talk for a moment about accessibility.

Nigel: OK.

Thomas: In your course of doing HR systems, you've obviously been involved with things like employee self-service and customers accessing CRM and so on. Have you had much exposure to the issue of accessibility?

Nigel: A little. More from the angle of websites. And I’ve been to some conferences where they’ve talked about accessibility. There have been some topics around accessibility, and one particular acronym that comes to mind is ARIA, that you can probably know what it means more than me, [inaudible 13:23- 13:25] I assume that ARIA being a key accessibility concept, and that particular components of software packages would give you this sort of accessibility, kind of bagged in, so that was interesting. In terms of HR and CRM systems, it’s been more about usability rather than accessibility, I would say. So, just making sure that it’s usable by someone, but not without too much regard for someone needing a high contrast site or someone who is blind and has to ... ,you think about the screen readers and those sorts of things. So I haven’t really had too much of exposure to that level of accessibility, but more just on usability.

Thomas: Have you ever found it come up in a project, or is it just one of those things that never really gets picked up on?

Nigel: I’ve never had anyone come to me and say, we’re designing this website. We need to make sure that people who are blind or color blind or need screen readers need to be able to access this site. And probably that’s mostly because a lot of stuff that I’ve done in that space has been Internet or, probably let’s say, extranet, like a B to B scenario. So, I guess that they weren’t too concerned about it. It’s not like a general website.

Thomas: So you don’t come across things like the Disability Discrimination Act in the UK or the equivalent in Australia? Those have never really come up as issues on IT projects for you?

Nigel: I’ve gotten vaguely aware about them, but yeah, never really as a driving force in a development project. No.

Thomas: Right. OK. That’s interesting, because that fits in with what I’ve heard from everyone else is despite the fact that there are all these laws that exist for these things and they’re quite a big social issue they’re largely ignored on a project basis.

Nigel: Yes. Absolutely. I think there are places and some people who take care of that sort of stuff really well, and some sites do do it, not that I could name any of them. I have, on some websites and blogs and those sorts of things, come across if you want to do accessibility then you need to think about screen readers. That means you don't put this sort of things in the tags, or you put this sort of information or you structure your website in this fashion. As to how well or how much website developers or any other developers pick up on that, I'm not sure. I've never heard it being an issue in tablets or smart phone applications either, but that could just be I've not been exposed to that.

Thomas: What I was really asking was to see whether you'd come across it because you've been working for a number of years across a number of companies. If it had been a common discussion point in projects, then you would have been exposed to it.

Nigel: No, not really.

Thomas: In terms of, I'm jumping around a bit here, if we go back to the data protection side of things, have you had projects where you've had data protection come up as an issue?

Nigel: Are you more concerned about me seeing private data or data protection as in…

Thomas: No, more in terms of the architecture. Let's say you're involved in, I don't know, one of those big corporates in the design of the HR system. Did data protection come up as a design topic?

Nigel: Yeah. I think it did, fittingly on one of those large corporates that I mentioned earlier. Obviously it was a large corporate and a global company so they've got data centers in Europe and they've got probably similar data centers in America. So there was the whole, where is the data located, kind of issue. That's come up on one or two projects. But then some of the smaller projects that I've worked on, are either not global entities but smaller companies that are just located in one region so they've either got their own equipment on site, or it's in a data center that's hosted in the same country. So, it's not like they've got the whole issue of sending their data overseas and all of that sort of thing.

Thomas: If I asked you bluntly could you differentiate between trademark patent and copyright could you?

Nigel: Trademark patent and copyright. So if I create something, it gets ascribed to me in a copyright. Generally, to do that I have to kind of show that I'm serious about protecting my copyright, generally by putting the little C symbol on it and my name and the date. If I want to get really serious I would put it in an envelope and post it to myself, to prove the date. A trademark is something you would do to a symbol or a logo like the Apple symbol, which they vigorously defend. A patent would apply to a process, and there are lots of arguments about software patents. So with Google just buying out Motorola a lot of discussion is that they could have enhanced their patent. They're more gentle with patents that they have on different mobile technologies. I'm not sure if they're definitions, but that's part of my understanding of each of the three.

Thomas: OK. Good. If I talk for a second about open source and the contract licenses around open source are you comfortable with open source licensing? Do you understand how that differs from proprietary software licensing?

Nigel: Yeah. Basically, open source, as I understand it, and there are unfortunately many variations. And to be honest I don't understand all the variations, like the MIT license, the petty license, and goodness knows how many others, but basically open source means that you have a license to copy and share the code with various restrictions. Some of which mean, that if you make any changes to the code, then you should submit that back to the original project, so that everyone else can benefit. The problem with that is if you're in a proprietary or a company situation where you want to get a competitive advantage, is that if you're forced to do that your competitors see exactly what you're doing.

So I think people like, and I think the most famous example is MySQL that had a jeweled licensing model where you could, under certain circumstances, just use the open source version of the license. Or if you were in a company situation and you didn't want to give up your IP then you could pay for a proprietary license and that funded development and kept open source people very happy.

A lot of our companies have used a similar model or used a model like, if you're an education or non-profit license then you can see the source code for free but if you're doing paid development or a commercial type activity on top of it, libraries, then you have to pay for a license.

Thomas: OK. OK. Let me think of a way of phrasing this. If you were structuring the degree that you did today again, based on the hindsight of 15 years experience, would you think that a component on the legal and ethical issues of software would be a useful addition to the program?

Nigel: Yes, I think it would be. I think it could probably be maybe a one semester second year unit, or something like that. Here comes the, whether you force people to do it or it's one of the electives. I think that would be possibly an elective subject. Then you still have the problem that people get out the door and don't know any better, as I have, but I think that would be at least a good start in appraising all the issues perhaps towards a better degree than what I've explained. I think those people, particularly those who work in, let's say, open source and actively develop open source products and proponents of that methodology of open software, I think they kind of self-educate themselves in the different licenses and what they mean, and that sort of thing.

So, if someone was coming from that environment then it might be a little bit redundant. It might be a cakewalk type subject. But I think there are still lots of other issues about protection and accessibility and the other things you’ve mentioned that it would be a good one-semester type subject.

Thomas: In terms of ongoing education, when you worked with clients have you ever had to educate to any of those topics as part of an on-boarding process or as part of any type of ongoing application?

Nigel: I think it’s part of on-boarding. Then you certainly get the talk about, you’re accessing, not always but in some companies, you’re going to be accessing personal information here and you’d better not share it or you’d better not do anything with it. Or in other cases, production access was so limited that you basically had to apply for production access to investigate a very strange scenario, or investigate a bug that was occurring and then you got access for one day and that was it. Then you’re back to the testing and development systems.

There have been scenarios that they have come up in those sorts of on-boarding procedures.

Thomas: OK. I think I’m about done from a question point of view. I’m just thinking if there’s anything else I wanted to ask you. Oh yeah, one last thing. When you get involved in software specifications, I’m thinking here especially on the HR angle, there’s often legal issues in specifying HR stuff. How’s that handled? So there’s a payroll change or there’s a change in the needs policy and you have to build that into the process. How do you go from law to code?

Nigel: Sorry, you just started dropping out a bit.

Thomas: If you’re in that context there and you’re designing a new HR process and there are legal implications in this? How do you learn about the law and how do you transport that into the code?

Nigel: This is a little bit hypothetical, but basically, if you were coding to an RFC, as in a specification, then you would have the specification in front of you and you would work through it, and do your design and whatever. If you were coding to legislation, be that tax legislation or for a finance something, or an HR remuneration type thing, or even a privacy type thing, then a good start would be to have the law on the desk. So that you can ensure that you've been compliant to its specification, if I can put it that way.

Thomas: What I mean about that is do you find in those contexts that you have people that know the law that can help you on that specification or do you find yourself reading the law yourself and trying to figure it out?

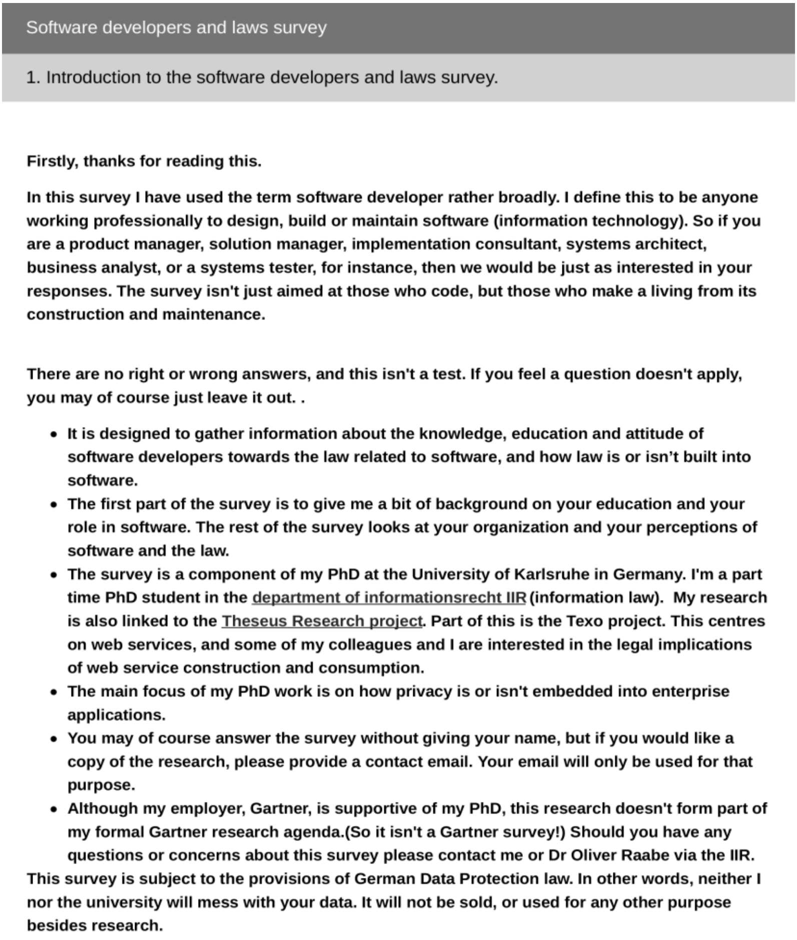
Nigel: Again, a little bit hypothetical. I can't remember a time where I had to specifically code something that wasn't already coded in an HR system, in terms of a legal type requirement. In SAP systems much of those things came through in patches that were made to update your system to the latest income tax rates and all those sorts of things. In that context, if I was sitting in the mother ship and coding that I would expect to have someone advising me and I'd probably have a copy of the law on my desk as well.

Thomas: That's enough. That helps me. Nigel, I think I'm about done here unless there's anything else you want to add from your side.

Nigel: I think generally, and this is probably the point you're going to make, is that law education at an undergraduate level, is a little bit sadly lacking. When you look at it, a lot of software has a legal ramification and it is a little bit surprising that there isn't any more education, either as optional or enforced, at any point over an undergrad degree. So, I think it's a little bit surprising and something should be done.

Thomas: You're essentially making my point there. That's very much what I needed. All right. I'm going just going to stop the recording, my good man.

Appendix E Survey print out



Software developers and laws survey

1. Introduction to the software developers and laws survey.

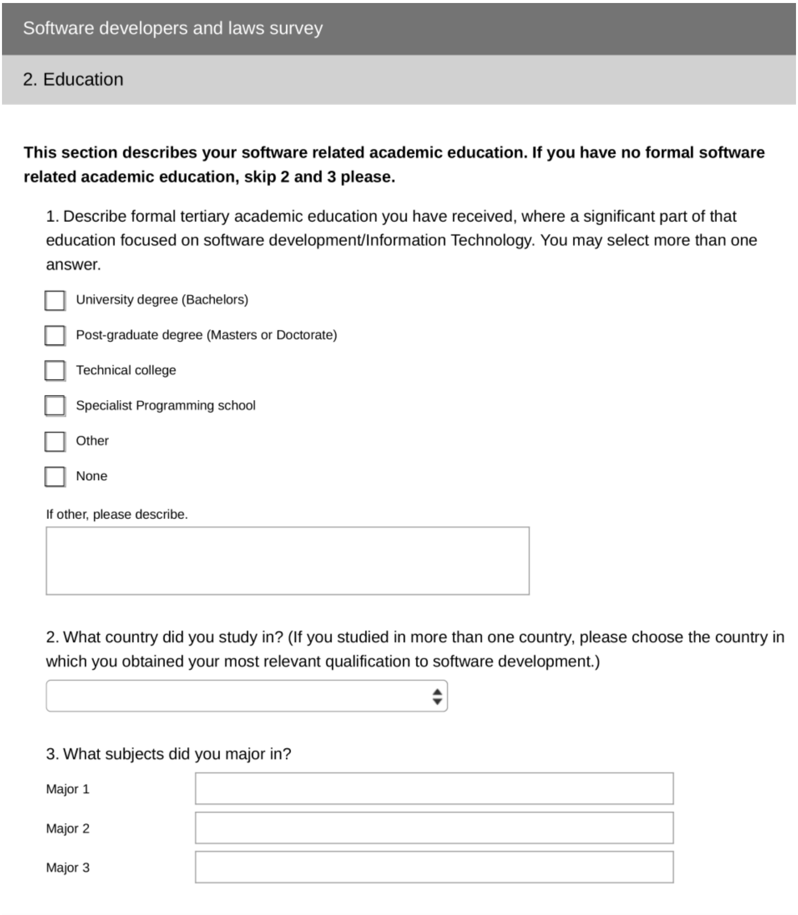
Firstly, thanks for reading this.

In this survey I have used the term software developer rather broadly. I define this to be anyone working professionally to design, build or maintain software (information technology). So if you are a product manager, solution manager, implementation consultant, systems architect, business analyst, or a systems tester, for instance, then we would be just as interested in your responses. The survey isn't just aimed at those who code, but those who make a living from its construction and maintenance.

There are no right or wrong answers, and this isn't a test. If you feel a question doesn't apply, you may of course just leave it out. .

- **It is designed to gather information about the knowledge, education and attitude of software developers towards the law related to software, and how law is or isn't built into software.**
- **The first part of the survey is to give me a bit of background on your education and your role in software. The rest of the survey looks at your organization and your perceptions of software and the law.**
- **The survey is a component of my PhD at the University of Karlsruhe in Germany. I'm a part time PhD student in the department of informationsrecht IIR (information law). My research is also linked to the Theseus Research project. Part of this is the Texo project. This centres on web services, and some of my colleagues and I are interested in the legal implications of web service construction and consumption.**
- **The main focus of my PhD work is on how privacy is or isn't embedded into enterprise applications.**
- **You may of course answer the survey without giving your name, but if you would like a copy of the research, please provide a contact email. Your email will only be used for that purpose.**
- **Although my employer, Gartner, is supportive of my PhD, this research doesn't form part of my formal Gartner research agenda.(So it isn't a Gartner survey!) Should you have any questions or concerns about this survey please contact me or Dr Oliver Raabe via the IIR.**

This survey is subject to the provisions of German Data Protection law. In other words, neither I nor the university will mess with your data. It will not be sold, or used for any other purpose besides research.



Software developers and laws survey

2. Education

This section describes your software related academic education. If you have no formal software related academic education, skip 2 and 3 please.

1. Describe formal tertiary academic education you have received, where a significant part of that education focused on software development/Information Technology. You may select more than one answer.

□ University degree (Bachelors)

□ Post-graduate degree (Masters or Doctorate)

□ Technical college

□ Specialist Programming school

□ Other

□ None

If other, please describe.

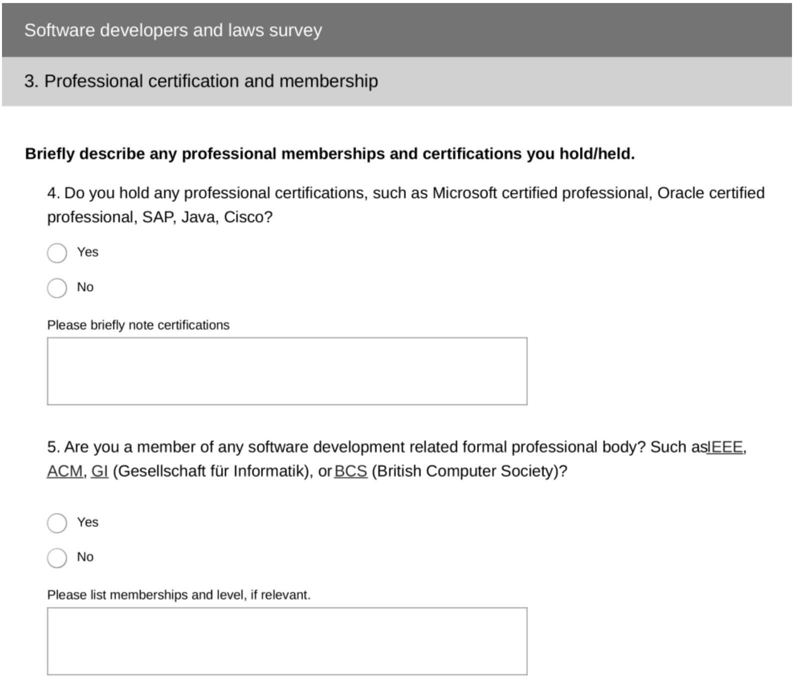
2. What country did you study in? (If you studied in more than one country, please choose the country in which you obtained your most relevant qualification to software development.)

3. What subjects did you major in?

Major 1

Major 2

Major 3



Software developers and laws survey

3. Professional certification and membership

Briefly describe any professional memberships and certifications you hold/held.

4. Do you hold any professional certifications, such as Microsoft certified professional, Oracle certified professional, SAP, Java, Cisco?

○ Yes

○ No

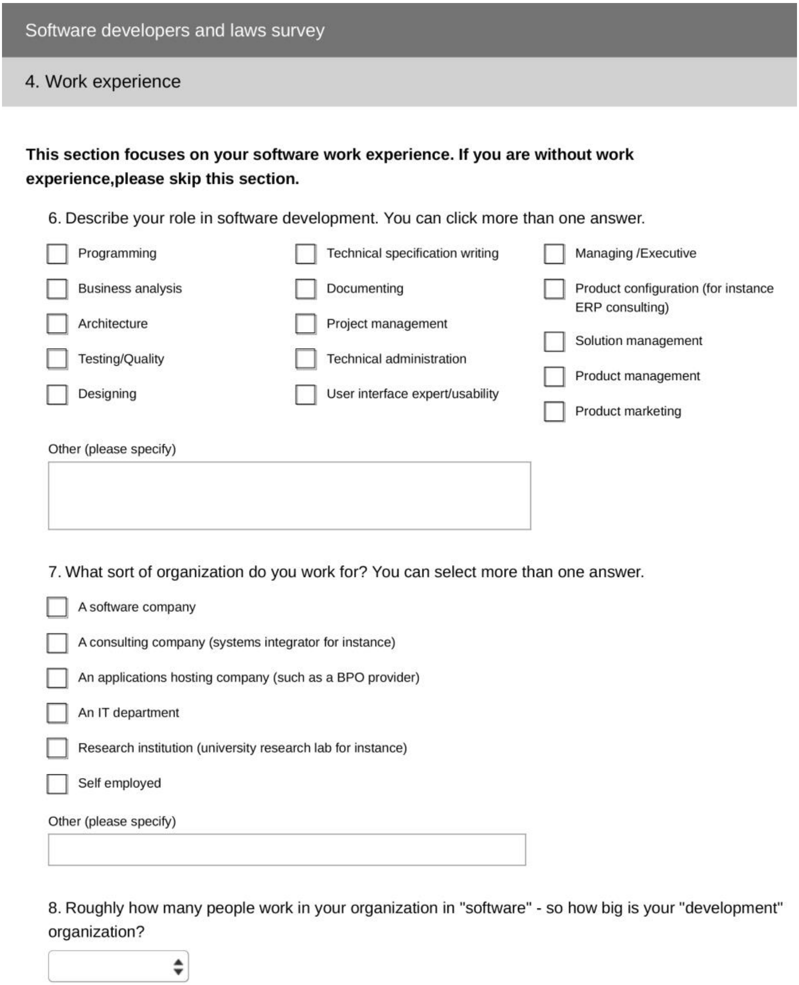
Please briefly note certifications

5. Are you a member of any software development related formal professional body? Such asIEEE, ACM, GI (Gesellschaft für Informatik), or BCS (British Computer Society)?

○ Yes

○ No

Please list memberships and level, if relevant.



Software developers and laws survey

4. Work experience

This section focuses on your software work experience. If you are without work experience,please skip this section.

6. Describe your role in software development. You can click more than one answer.

□ Programming

□ Business analysis

□ Architecture

□ Testing/Quality

□ Designing

□ Technical specification writing

□ Documenting

□ Project management

□ Technical administration

□ User interface expert/usability

□ Managing /Executive

□ Product configuration (for instance ERP consulting)

□ Solution management

□ Product management

□ Product marketing

Other (please specify)

7. What sort of organization do you work for? You can select more than one answer.

□ A software company

□ A consulting company (systems integrator for instance)

□ An applications hosting company (such as a BPO provider)

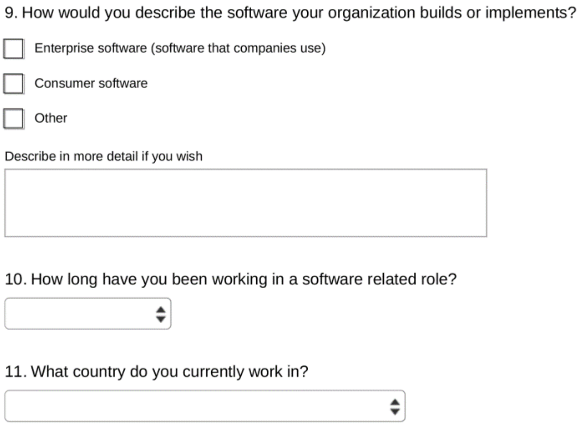
□ An IT department

□ Research institution (university research lab for instance)

□ Self employed

Other (please specify)

8. Roughly how many people work in your organization in "software" - so how big is your "development" organization?



9. How would you describe the software your organization builds or implements?

□ Enterprise software (software that companies use)

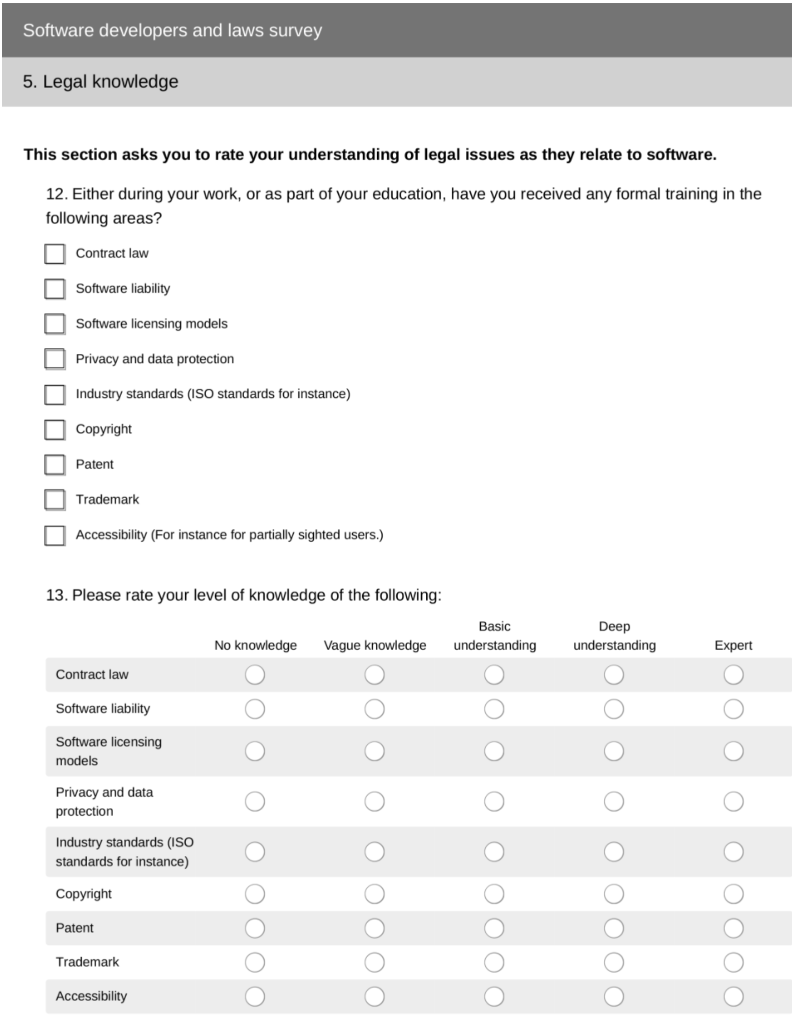
□ Consumer software

□ Other

Describe in more detail if you wish

10. How long have you been working in a software related role?

11. What country do you currently work in?



Software developers and laws survey

5. Legal knowledge

This section asks you to rate your understanding of legal issues as they relate to software.

12. Either during your work, or as part of your education, have you received any formal training in the following areas?

□ Contract law

□ Software liability

□ Software licensing models

□ Privacy and data protection

□ Industry standards (ISO standards for instance)

□ Copyright

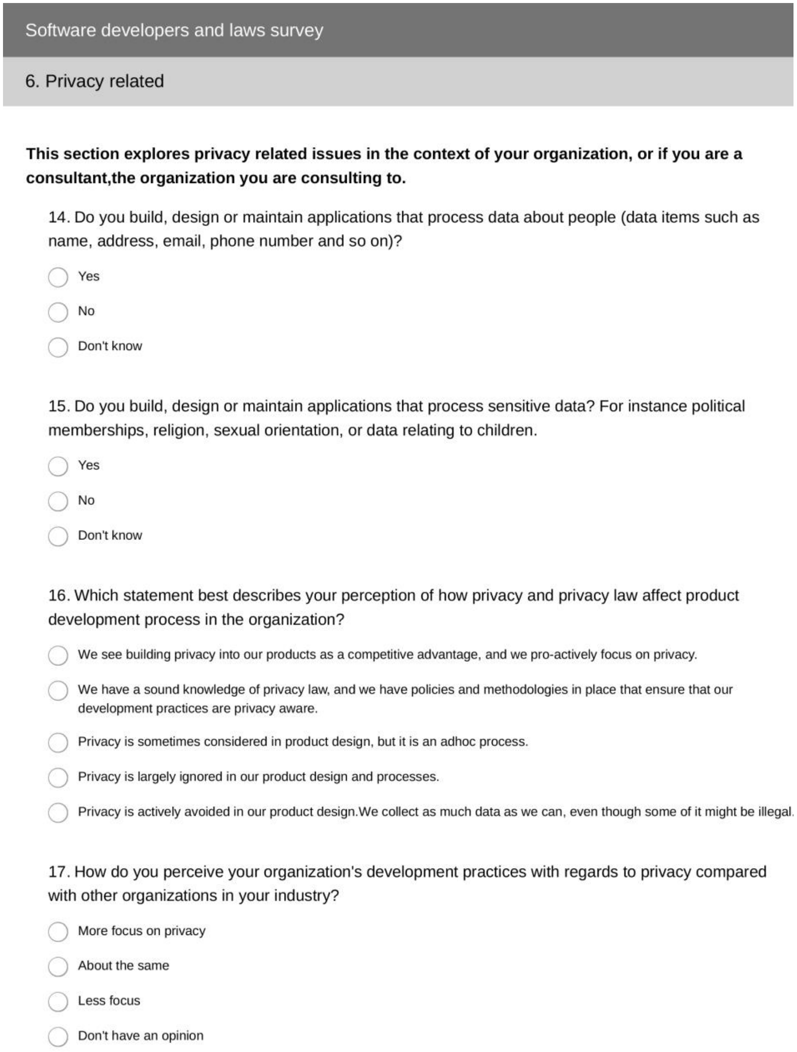
□ Patent

□ Trademark

□ Accessibility (For instance for partially sighted users.)

13. Please rate your level of knowledge of the following:

	No knowledge	Vague knowledge	Basic understanding	Deep understanding	Expert
Contract law	○	○	○	○	○
Software liability	○	○	○	○	○
Software licensing models	○	○	○	○	○
Privacy and data protection	○	○	○	○	○
Industry standards (ISO standards for instance)	○	○	○	○	○
Copyright	○	○	○	○	○
Patent	○	○	○	○	○
Trademark	○	○	○	○	○
Accessibility	○	○	○	○	○



Software developers and laws survey

6. Privacy related

This section explores privacy related issues in the context of your organization, or if you are a consultant,the organization you are consulting to.

14. Do you build, design or maintain applications that process data about people (data items such as name, address, email, phone number and so on)?

○ Yes

○ No

○ Don't know

15. Do you build, design or maintain applications that process sensitive data? For instance political memberships, religion, sexual orientation, or data relating to children.

○ Yes

○ No

○ Don't know

16. Which statement best describes your perception of how privacy and privacy law affect product development process in the organization?

○ We see building privacy into our products as a competitive advantage, and we pro-actively focus on privacy.

○ We have a sound knowledge of privacy law, and we have policies and methodologies in place that ensure that our development practices are privacy aware.

○ Privacy is sometimes considered in product design, but it is an adhoc process.

○ Privacy is largely ignored in our product design and processes.

○ Privacy is actively avoided in our product design.We collect as much data as we can, even though some of it might be illegal.

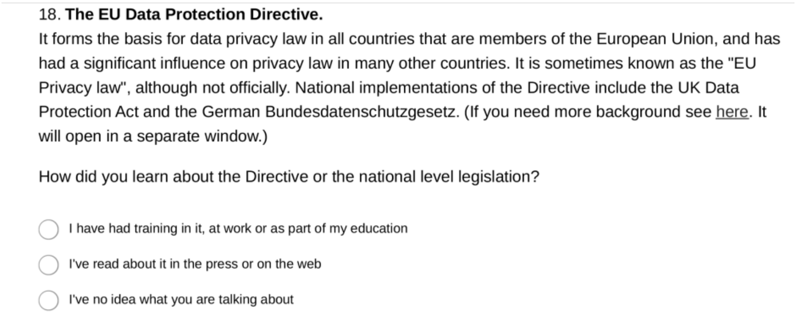
17. How do you perceive your organization's development practices with regards to privacy compared with other organizations in your industry?

○ More focus on privacy

○ About the same

○ Less focus

○ Don't have an opinion



18. **The EU Data Protection Directive.**

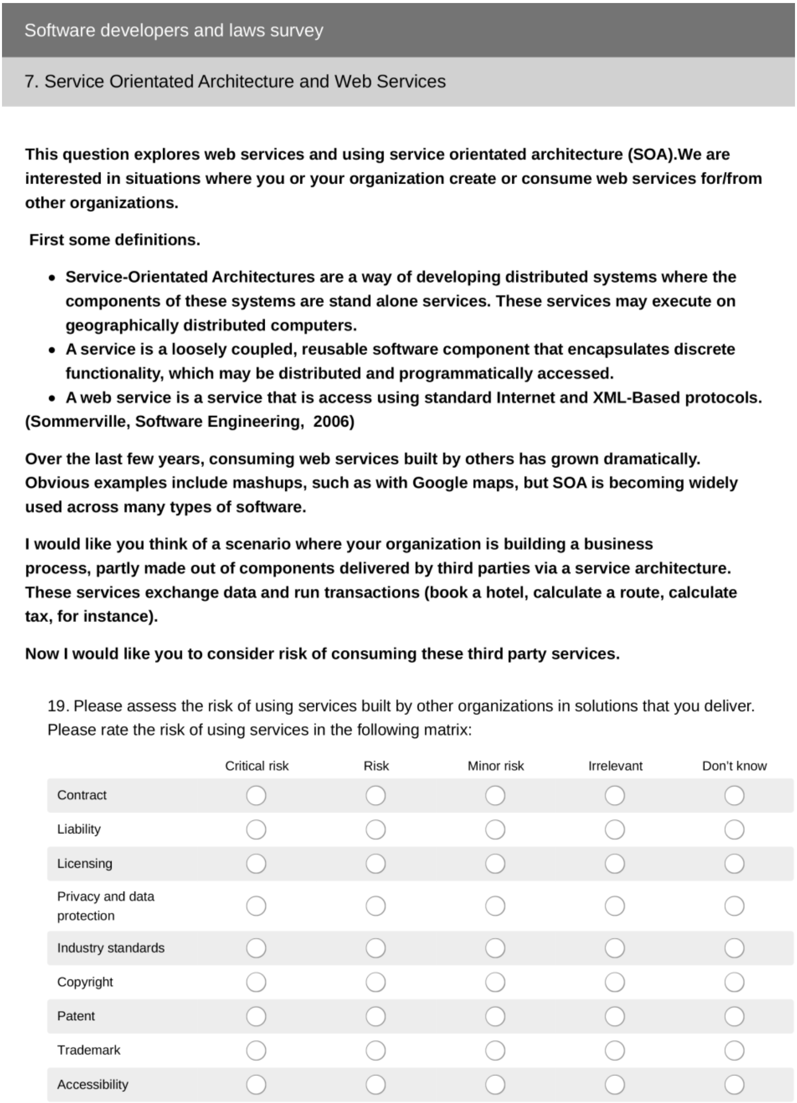
It forms the basis for data privacy law in all countries that are members of the European Union, and has had a significant influence on privacy law in many other countries. It is sometimes known as the "EU Privacy law", although not officially. National implementations of the Directive include the UK Data Protection Act and the German Bundesdatenschutzgesetz. (If you need more background see here. It will open in a separate window.)

How did you learn about the Directive or the national level legislation?

○ I have had training in it, at work or as part of my education

○ I've read about it in the press or on the web

○ I've no idea what you are talking about



Software developers and laws survey

7. Service Orientated Architecture and Web Services

This question explores web services and using service orientated architecture (SOA).We are interested in situations where you or your organization create or consume web services for/from other organizations.

First some definitions.

- **Service-Orientated Architectures are a way of developing distributed systems where the components of these systems are stand alone services. These services may execute on geographically distributed computers.**
- **A service is a loosely coupled, reusable software component that encapsulates discrete functionality, which may be distributed and programmatically accessed.**
- **A web service is a service that is access using standard Internet and XML-Based protocols.**

(Sommerville, Software Engineering, 2006)

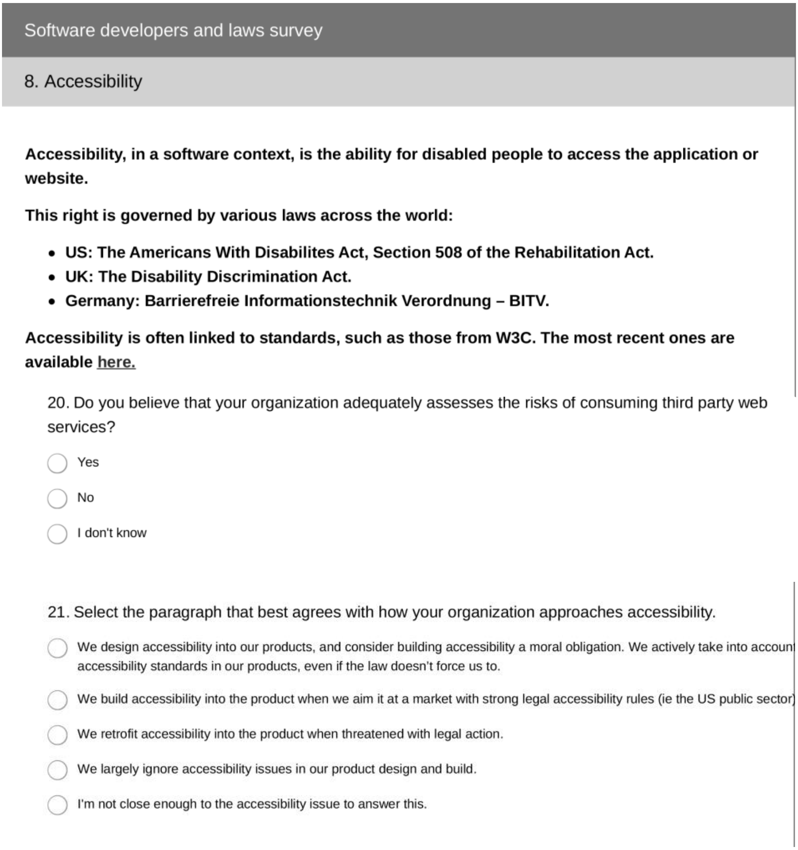
Over the last few years, consuming web services built by others has grown dramatically. Obvious examples include mashups, such as with Google maps, but SOA is becoming widely used across many types of software.

I would like you think of a scenario where your organization is building a business process, partly made out of components delivered by third parties via a service architecture. These services exchange data and run transactions (book a hotel, calculate a route, calculate tax, for instance).

Now I would like you to consider risk of consuming these third party services.

19. Please assess the risk of using services built by other organizations in solutions that you deliver. Please rate the risk of using services in the following matrix:

	Critical risk	Risk	Minor risk	Irrelevant	Don't know
Contract	○	○	○	○	○
Liability	○	○	○	○	○
Licensing	○	○	○	○	○
Privacy and data protection	○	○	○	○	○
Industry standards	○	○	○	○	○
Copyright	○	○	○	○	○
Patent	○	○	○	○	○
Trademark	○	○	○	○	○
Accessibility	○	○	○	○	○



Software developers and laws survey

8. Accessibility

Accessibility, in a software context, is the ability for disabled people to access the application or website.

This right is governed by various laws across the world:

- **US: The Americans With Disabilites Act, Section 508 of the Rehabilitation Act.**
- **UK: The Disability Discrimination Act.**
- **Germany: Barrierefreie Informationstechnik Verordnung – BITV.**

Accessibility is often linked to standards, such as those from W3C. The most recent ones are available here.

20. Do you believe that your organization adequately assesses the risks of consuming third party web services?

○ Yes

○ No

○ I don't know

21. Select the paragraph that best agrees with how your organization approaches accessibility.

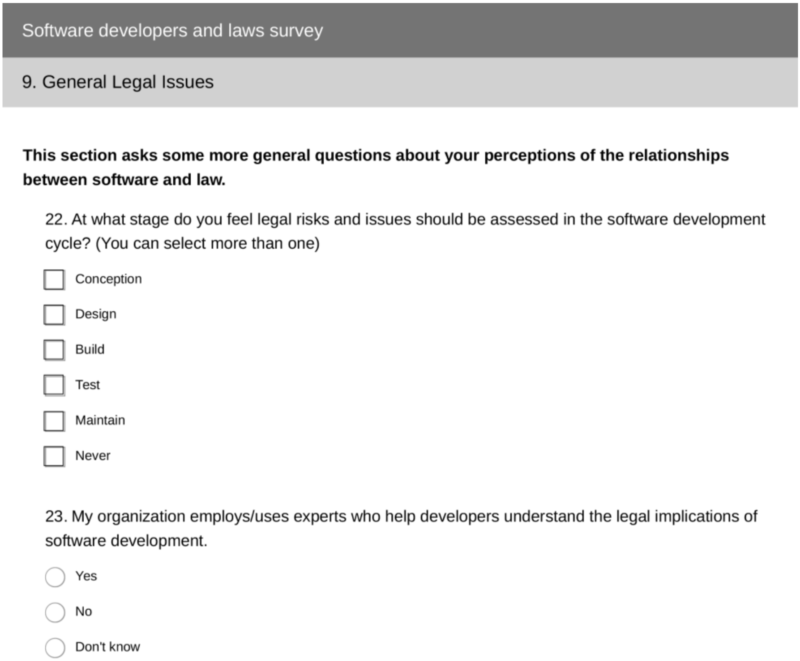
○ We design accessibility into our products, and consider building accessibility a moral obligation. We actively take into accoun accessibility standards in our products, even if the law doesn't force us to.

○ We build accessibility into the product when we aim it at a market with strong legal accessibility rules (ie the US public sector)

○ We retrofit accessibility into the product when threatened with legal action.

○ We largely ignore accessibility issues in our product design and build.

○ I'm not close enough to the accessibility issue to answer this.



Software developers and laws survey

9. General Legal Issues

This section asks some more general questions about your perceptions of the relationships between software and law.

22. At what stage do you feel legal risks and issues should be assessed in the software development cycle? (You can select more than one)

□ Conception

□ Design

□ Build

□ Test

□ Maintain

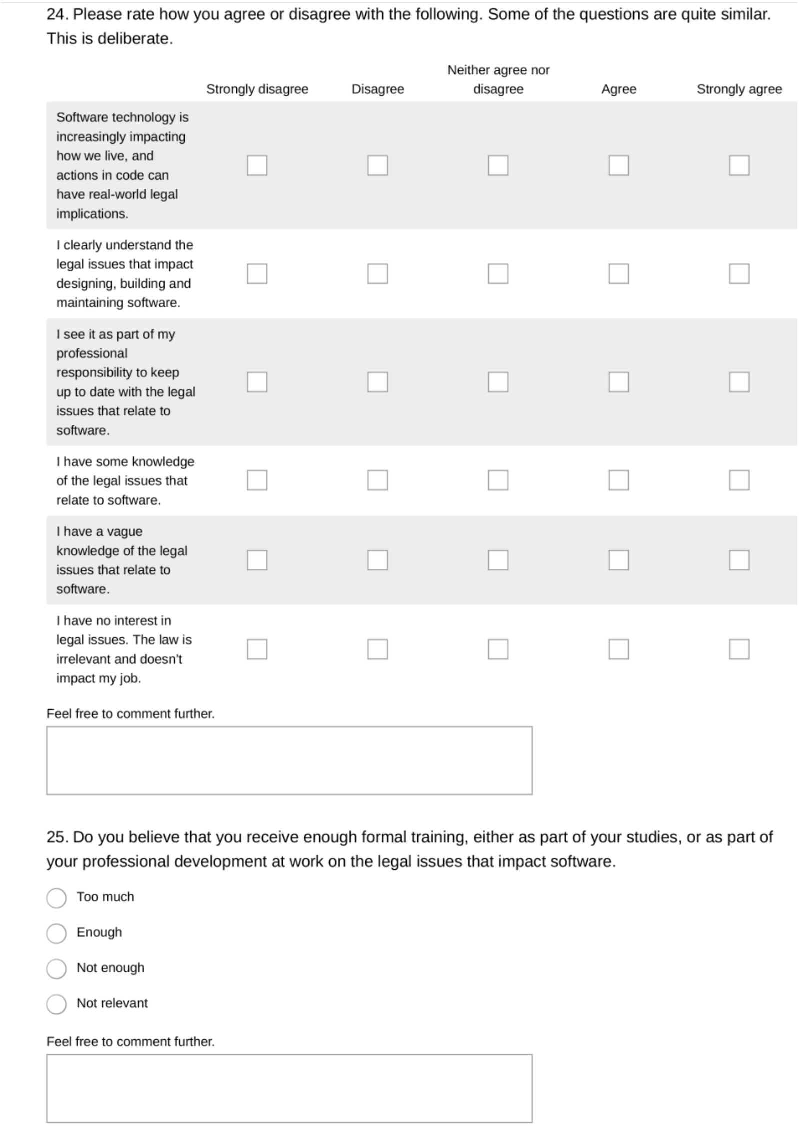
□ Never

23. My organization employs/uses experts who help developers understand the legal implications of software development.

○ Yes

○ No

○ Don't know



24. Please rate how you agree or disagree with the following. Some of the questions are quite similar. This is deliberate.

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Software technology is increasingly impacting how we live, and actions in code can have real-world legal implications.	□	□	□	□	□
I clearly understand the legal issues that impact designing, building and maintaining software.	□	□	□	□	□
I see it as part of my professional responsibility to keep up to date with the legal issues that relate to software.	□	□	□	□	□
I have some knowledge of the legal issues that relate to software.	□	□	□	□	□
I have a vague knowledge of the legal issues that relate to software.	□	□	□	□	□
I have no interest in legal issues. The law is irrelevant and doesn't impact my job.	□	□	□	□	□

Feel free to comment further.

25. Do you believe that you receive enough formal training, either as part of your studies, or as part of your professional development at work on the legal issues that impact software.

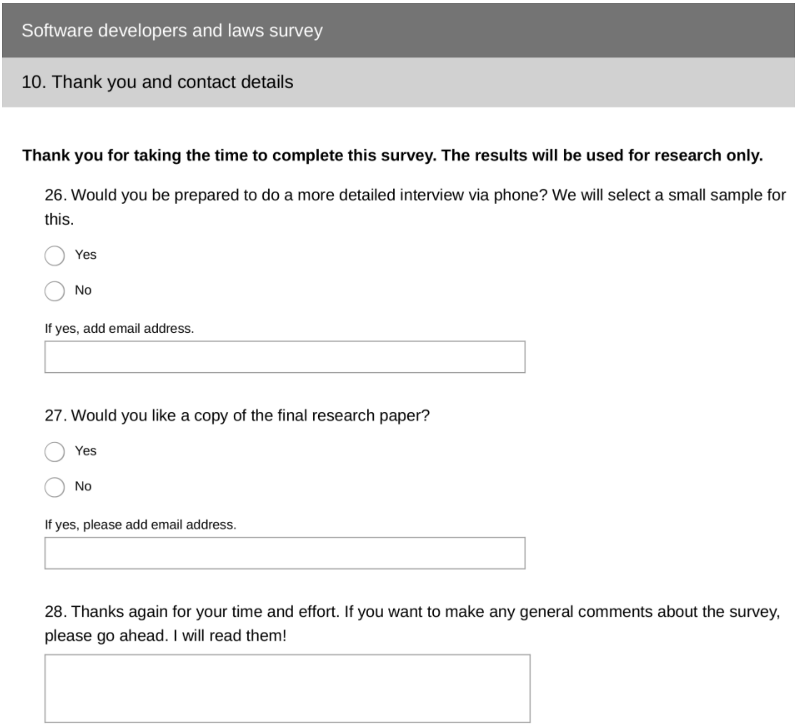
○ Too much

○ Enough

○ Not enough

○ Not relevant

Feel free to comment further.



Software developers and laws survey

10. Thank you and contact details

Thank you for taking the time to complete this survey. The results will be used for research only.

26. Would you be prepared to do a more detailed interview via phone? We will select a small sample for this.

○ Yes

○ No

If yes, add email address.

27. Would you like a copy of the final research paper?

○ Yes

○ No

If yes, please add email address.

28. Thanks again for your time and effort. If you want to make any general comments about the survey, please go ahead. I will read them!

SCHRIFTEN DES ZENTRUMS FÜR ANGEWANDTE RECHTSWISSENSCHAFT

Karlsruher Institut für Technologie (KIT) | ISSN 1860-8744

Herausgeber:
Prof. Dr. Thomas Dreier M.C.J.

Band 1 THOMAS DREIER | ELLEN EULER (Hrsg.)
Kulturelles Gedächtnis im 21. Jahrhundert. Tagungsband des internationalen Symposiums, 23. April 2005, Karlsruhe. 2005
ISBN 3-937300-56-2

Band 2 CHRISTOPH SORGE
Softwareagenten. Vertragsschluss, Vertragsstrafe, Reugeld. 2006
ISBN 3-937300-91-0

Band 3 JOSÉ LUIS CÁRDENAS T.
Rolle, Kriterien und Methodik der kartellrechtlichen Marktabgrenzung. Eine juristische und ökonomische Analyse. 2005
ISBN 3-937300-93-7

Band 4 WOLFGANG W. GÖPFERT
Die Strafbarkeit von Markenverletzungen. 2006
ISBN 3-937300-97-X

Band 5 CHRISTIAN KAU
Vertrauensschutzmechanismen im Internet, insbesondere im E-Commerce. 2006
ISBN 3-86644-036-7

Band 6 ALEXANDER MOHR
Internetspezifische Wettbewerbsverstöße. 2006
ISBN 3-86644-047-2

Band 7 FABIAN SCHÄFER
Der virale Effekt. Entwicklungsrisiken im Umfeld von Open Source Software. 2007
ISBN 978-3-86644-141-5

Die Bände sind unter www.ksp.kit.edu als PDF frei verfügbar oder als Druckausgabe bestellbar.

Band 8 RETO MANTZ
Rechtsfragen offener Netze: Rechtliche Gestaltung und Haftung
des Access Providers in zugangsoffenen (Funk-)Netzen. 2008
ISBN 978-3-86644-222-1

Band 9 STEFAN BOLAY
Mehrwertgebührenpflichtige Telefon- und SMS-Gewinnspiele:
Eine rechtliche Einordnung am Beispiel aktueller Erscheinungsformen
des Rundfunks. 2008
ISBN 978-3-86644-259-7

Band 10 OLIVER MEYER
Aktuelle vertrags- und urheberrechtliche Aspekte der Erstellung,
des Vertriebs und der Nutzung von Software. 2008
ISBN 978-3-86644-280-1

Band 11 SASCHA THEISSEN
Risiken informations- und kommunikationstechnischer (IKT-) Implantate
im Hinblick auf Datenschutz und Datensicherheit. 2009
ISBN 978-3-86644-343-3

Band 12 CHRISTIAN FUNK
Allgemeine Geschäftsbedingungen in Peer-to-Peer-Märkten. 2010
ISBN 978-3-86644-504-8

Band 13 ANNE VAN RAAY
Gewinnabschöpfung als Präventionsinstrument im Lauterkeitsrecht: Möglichkeiten und Grenzen effektiver Verhaltenssteuerung durch den Verbandsanspruch nach § 10 UWG; Untersuchung unter vergleichender Heranziehung insbesondere der Verletzergewinnhaftung im Rahmen der dreifachen Schadensberechnung nach Immaterialgutsverletzungen. 2012
ISBN 978-3-86644-811-7

Band 14 NADINE SCHÜTTEL
Streitbeilegung im Internet – Zukunft oder Irrweg? 2014
ISBN 978-3-7315-0300-2

Band 15 THOMAS DREIER | INDRA SPIECKER GEN. DÖHMANN (Hrsg.)
Informationsrecht@KIT –
15 Jahre Zentrum für Angewandte Rechtswissenschaft. 2015
ISBN 978-3-7315-0367-5

Band 16 STEFFEN ALBRECHT
Verwaiste Werke – Vom rechtlichen Problem zur rechtspraktischen
Herausforderung bei der Nutzung vorbestehender Inhalte. 2017
ISBN 978-3-7315-0687-4

Die Bände sind unter www.ksp.kit.edu als PDF frei verfügbar oder als Druckausgabe bestellbar.

Band 17 MIEKE LORENZ
Optimierung von Verfahren zur Lösung rechtsrelevanter
Wissensprobleme in kritischen Infrastrukturen:
Befunde im Smart Grid und technikrechtliche Empfehlungen. 2017
ISBN 978-3-7315-0716-1

Band 18 THOMAS OTTER
Externalities and Enterprise Software:
Helping and Hindering Legal Compliance. 2019
ISBN 978-3-7315-0937-0

Die Bände sind unter www.ksp.kit.edu als PDF frei verfügbar oder als Druckausgabe bestellbar.

ZAR

KARLSRUHER INSTITUT FÜR TECHNOLOGIE (KIT)
INSTITUT FÜR INFORMATIONS- UND WIRTSCHAFTSRECHT

Enterprise software plays a key role in helping organizations comply with a variety of laws and regulations, yet software itself creates negative externalities that can undermine rights and laws. Software developers are an important regulatory force, yet many know little about IT law, and how law and software interact. This work examines enterprise software developer understanding and perception of legal concepts and explores four examples of the software code and law relationship: payroll, the Sarbanes Oxley Act (SOX), web accessibility, and data protection law. It provides suggestions on how regulators, software vendors and educators might work more effectively to reduce the negative externalities that enterprise software directly or indirectly creates.

ISSN 1860-8744 | ISBN 978-3-7315-0937-0

ISBN 978-3-7315-0937-0
9 783731 509370 >

Gedruckt auf FSC-zertifiziertem Papier