***Eva-Maria Schomakers / Chantal Lidynia / Dirk Müllmann / Roman Matzutt / Klaus Wehrle / Indra Spiecker gen. Döhmann / Martina Ziefle***

# Insights on Data Sensitivity from the Technical, Legal and the Users' Perspectives

## Practical suggestions on how to raise more awareness for the assumed exercise of informational self-determination

*Social media, cloud computing, and the Internet of Things connect people around the globe, offering manifold benefits. However, the technological advances and increased user participation generate novel challenges for users' privacy. From the users' perspective, the consequences of data disclosure depend on the perceived sensitivity of that data. But in light of the new technological opportunities to process and combine data, it is questionable whether users can adequately evaluate risks of data disclosures. As mediating authority, data protection laws such as the European General Data Protection Regulation try to protect user data, granting enhanced protection to "special categories" of data. This article assesses the legal, technological, and users' perspectives on information sensitivity and their interplay. Technologically, all data can be referred to as "potentially sensitive." The legal and users' perspective on information sensitivity deviate from this standpoint, as some data types are granted special protection by law but are not perceived as very sensitive by users and vice versa. The key findings here suggest the GDPR adequately protecting users' privacy but for small adjustments.*

## I. Introduction

1 Technological advances have increased user participation online and generate large amounts of user data, which concerns users, who nevertheless disclose a lot of personal information.[1] Users' decisions for disclosing data are highly influenced by its perceived sensitivity, i.e., how risky they individually perceive particular information to be.[2] At the same time, data collection and processing has evolved over time so that increasingly more information can be combined, deanonymized, and used to profile individuals – consequently, users may be unaware of novel threats stemming from recent technological advances. As a mediating authority, laws like the European General Data Protection Regulation (GDPR) or the new Canadian Bill C-11[3] govern the use of personal data by companies, thereby distinguishing categories of information sensitivity and granting different levels of protection correspondingly.

However, with the ever-improving potential for data analysis, 2
the question arises whether the regulation (legal perspective) captures what data can potentially become sensitive (technological perspective) and also what data users perceive to be sensitive (users' perspective). This article examines sensitivity of information in a multidisciplinary approach comparing these three perspectives and discussing the findings with regard to the interests of online users and implications for future politics.

## II. Information Sensitivity from a Technological Perspective

The early 2000's shift of online services toward the Web 2.0 3
paradigm constituted a revolution of online services: user participation became an elementary ingredient of modern online

1 *Gerber, N./Gerber, P./Volkamer M.*: Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior, Computers & Security 2018, p. 226.

2 *Mothersbaugh, D. L./Foxx II", W.K./Beatty, S. E./Wang, S.*, Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information. Journal of Service Research 2012, p. 76 (90).

3 For an overview see *Beardwood, John*: The New Canadian Consumer Privacy Protection Act: A Compliance Briefing for Privacy Officers. CRi 2021, 1 (in this issue).

services.[4] The level of user interaction culminated in the rise of global social networks, such as Twitter and Facebook, which was enabled by shifting to the cloud computing paradigm.[5] In addition to its increased scalability and lowered entry bar for service providers, the cloud's ubiquity also enabled users to outsource their data to simplify sharing or maintaining online backups. Ultimately, cloud computing motivated the advent of smartphones and the Internet of Things (IoT). Cloud storage enabled synchronizing numerous devices easily and the cloud's scalable processing power allows service providers to remotely process the data sensed by their users' IoT devices.[6] As a consequence, systems based on distributed ledgers, most notably blockchains, recently gained traction to break up this level of centralization: While initial blockchain systems, such as Bitcoin[7] or Ethereum[8], focused on achieving decentralized financial services in partially distrusted environments, distributed ledgers are now being explored for, e.g., tamper-proof file storage[9] or managing access control to user data.[10] Distributed ledgers are experiencing this popularity because their immutability establishes technical accountability among otherwise mutually distrusting parties.

4 In short, new technologies have always simplified the deployment of online services centered around user participation or even enabled novel services over the Internet. However, those opportunities do not come without additional (privacy) challenges, as will be detailed in the following.

## 1. Web 2.0

5 The shift toward a strong focus on user participation within the Web 2.0 paradigm inherently led to the collection of more user data – and to new insights gained from service personalization, user tracking, and data breaches. Online services are routinely personalized to increase the user experience, e.g., provide better-fitting search results. While personalized services can benefit the user, the collected data is potentially highly sensitive. Not only is it possible to de-anonymize users solely based on search queries,[11] it is further possible to disclose sensitive user data even from properly anonymized data sets.[12] Web tracking maximizes this form of data collection by monitoring users' browsing behavior across services,[13] which potentially discloses a much more fine-grained view on users and was oftentimes opaque to the user prior to the GDPR's enactment. Even privacy-aware users, who actively protect their privacy by deleting cookies or using private browsing, have been shown to be susceptible to web tracking due to their distinct behavior.[14] A major threat also lies in the potential of data breaches, which disclose login credentials and other metadata for users' accounts on a regular basis.

## 2. Social Media

6 Especially the rise of social media revolutionized users' online behavior as users can now rapidly share personal moments and thoughts with both their friends and a general audience – leading to unprecedented privacy issues due to sensitive data disclosure. Users can directly share clearly sensitive data with the public (e.g., credit card information) or release it via metadata such as GPS locations stored in uploaded images.[15] These incidents showcase the need for education regarding potential threats of sharing sensitive data on the Internet. Furthermore, the data users share online can be combined and subsequently collectively be exploited as shown by the Cambridge Analytica scandal.[16] Hence, users can be profiled based on their shared data and the increased potential stemming from new analysis methods to exploit such data can cause data to effectively become sensitive.

## 3. Cloud Computing, Smartphones and IoT

Due to the cloud's multitenancy, single cloud providers could 7
gain access to data of all customers.[17] Moreover, a cloud can span multiple data centers. In this case, users lose control over where their data are being stored, which can violate both individual and even legal requirements.[18] Hence, the increased complexity of data management complicates users' risk evaluations.

The ubiquity of sensing devices also creates new challenges for 8
user privacy.[19] Third parties can potentially extract very fine-grained information from a user's sensor data via appropriate analysis technologies (e.g., location trajectories[20]). Furthermore, the often-insufficient security of IoT devices for smart homes can potentially leak sensitive information directly from the user's house to the Internet.[21] This potential threat is further

4 *O'Reilly*, *Tim*: What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software, Communication & Strategies First Quarter 2007, pp. 17–37.

5 *Armbrust*, *Michael et al.*: A View of Cloud Computing, Commun. ACM 53/4 2010, pp. 50–58.

6 *Henze*, *Martin et al.*: Maintaining User Control While Storing and Processing Sensor Data in the Cloud, International Journal of Grid and High Performance Computing 5/4 2013, pp. 97–112.

7 *Nakamoto*, *Satoshi*: Bitcoin: A Peer-to-Peer Electronic Cash System, White paper 2008.

8 *Wood*, *Gavin*: Ethereum: A Secure Decentralised Generalised Transaction Ledger, White paper 2016.

9 *Kopp et al.*: Design of a Privacy- Preserving Decentralized File Storage with Financial Incentives in: IEEE EuroS&PW, 2017, pp. 14–22.

10 *Zyskind*, *Guy et al.*: Decentralizing Privacy: Using Blockchain to Protect Personal Data, in: IEEE S&PW, 2015, pp. 180–184.

11 *Barbaro et al.*, A Face Is Exposed for AOL Searcher No. 4417749, https://www.nytimes.com/2006/08/09/technology/09aol.html (accessed 2021-01-19).

12 *Narayanan*, *Arvind* and *Shmatikov*, *Vitaly*: Robust De-anonymization of Large Sparse Datasets, in: IEEE S&P, 2008, pp. 111–125.

13 *Mayer*, *Jonathan R.* and *Mitchell*, *John C.*: Third-Party Web Tracking: Policy and Technology, in IEEE S&P, 2012, pp. 413–427.

14 *Yen*, *Ting-Fang et al.*: Host Fingerprinting and Tracking on the Web: Privacy and Security Implications, in NDSS, 2012.

15 *Smith*, *Matthew et al.*: Big Data Privacy Issues in Public Social Media, in IEEE DEST, 2012.

16 *Rosenberg et al.*, How Trump Consultants Exploited the Facebook Data of Millions, https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html (accessed 2021-01-19).

17 *Henze*, *Martin et al.*: A Trust Point-based Security Architecture for Sensor Data in the Cloud, in Krcmar/Reissner/Rumpe, Trusted Cloud Computing, 2014, pp. 77–106.

18 *Henze*, *Martin et al.*: The Cloud Needs Cross-Layer Data Handling Annotations, in IEEE S&PW, 2013, pp. 18–22.

19 *Ziegeldorf*, *Jan Henrik et al.*: Privacy in the Internet of Things: threats and challenges, Security and Communication Networks 7/12, 2014, pp. 2728–2742.

20 *Ziegeldorf*, *Jan Henrik et al.*: TraceMixer: Privacy- Preserving Crowd-Sensing sans Trusted Third Party, in IEEE/IFIP WONS, 2017, pp. 17–24.

21 *Serror*, *Martin et al.*: Towards In-Network Security for Smart Homes, in IoT-SECFOR, 2018.

exemplified by recent advances in deep learning.[22] Thus, users must be further aware of the potential privacy implications of third parties analyzing their sensed data.

### 4. Distributed Ledgers

9 While privacy-preserving platforms based on distributed ledgers aim to mitigate public data disclosure,[23] sensitive data on such ledgers can have especially devastating consequences due to their oftentimes public nature and immutability by design. For one, the initial promise of blockchains to provide financial privacy has been falsified.[24] Secondly, arbitrary data can be stored directly on blockchains, i.e., there is potential for the malicious disclosure of sensitive data of another user.[25] These initial observations indicate that users once again will be facing increasing complexity in the technologies providing their online services in the future.

10 In conclusion, emerging new technologies can cause intuitively non-sensitive data to become sensitive due to the potentially unwanted impact seizing this data can have. Despite whole research areas being dedicated to protecting sensitive data from being disclosed to unauthorized parties, there is no general solution to technical data protection. As mainstream technology becomes more complex and diverse, and thus harder for users to keep track of regarding potential privacy threats, it can be expected that this effect may be further exacerbated in the future.

## III. Information Sensitivity from a Legal Perspective

11 Since May 2018, data protection law in the Member States of the European Union is predominantly determined by the European General Data Protection Regulation (GDPR), leaving only a very limited scope of application to distinct national data protection legislation.[26] Depending on the content of the data, the European data protection law distinguishes three different categories: personal, special categories of personal and non-personal data all of which are granted different levels of protection.

12 Art. 4 No. 1 GDPR defines personal data as any information relating to an identified or identifiable natural person. When a person is considered identifiable is disputed.[27] However, it has to be at least assumed when the responsible body disposes of resources allowing the identification which it or another person will probably use.[28] Special categories of personal data consist of personal data referring to particularly sensitive information concerning a natural person. Under Art. 9 sec. 1 GDPR these include data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or union membership. Furthermore, genetic, biometric, and health data, as well as data concerning a person's sex life or sexual orientation, are part of this category. Every piece of information not falling under the definition of personal data, however, has to be considered non-personal data under data protection law.[29]

13 The group of personal data summarized under the notion of "special categories" consists of types of personal data which can be described as sensitive personal attributes. They have in common that they concern very personal beliefs or states which bear a special risk of being a leverage point for discrimination[30] and are closely connected to the exercise of fundamental rights.[31] The processing of these data can result in a severe violation of a person's privacy as well as significant risks to the fundamental rights and freedoms.[32] The legal protection for special categories of personal data, therefore, has to be even stronger compared to common personal data. Following the principle of "ban with reservation to permit",[33] Art. 9 GDPR restricts the processing of special categories of personal data to less, more specific, and more essential situations compared to mere personal data. Furthermore, only under very strict conditions may personal data of the special categories even be used for decision-making based solely on automated processing, including profiling (Art. 22 GDPR). If special categories of personal data are processed, this always leads to the necessity for the processor to keep records of his processing activities (Art. 30 GDPR). If handling this kind of data in a larger scale, the processor has to conduct a data protection impact assessment (Art. 35 sec. 3 lit. b) GDPR) and is obliged to appoint a data protection officer (Art. 37 sec. 1 lit. c) GDPR). The rigidity of the separation of these different levels of protection was already much debated at the time of its introduction by the Data Protection Directive.[34]

14 As non-personal data does not fall under the scope of the fundamental rights which establish data protection, it is, hence, neither protected under the GDPR nor any national data protection laws. Non-personal data, however, may be protected by other laws under different legal means, e.g., business secrets which are protected by the national civil law.[35] The GDPR as well as the national data protection legislations differentiate between data protection and data security. While data protection

22 *LeCun, Yann et al.*: Deep learning, Nature 521, 2015, pp. 436–444.

23 *Zyskind et al.*, in: IEEE S&PW, 2015, p. 180 (184).

24 *Meiklejohn, Sarah et al.*: A Fistful of Bitcoins: Characterizing Payments among Men with No Names, in ACM IMC, 2013, pp. 127–140.

25 *Matzutt, Roman et al.*: A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin, in Meiklejohn/Sato, IFCA FC, Berlin/Heidelberg 2018, pp. 420–438.

26 For an overview see *Pohle*: Data Privacy Legislation in EU Member States. CRi 2018, 97 and *Pohle*: Data Privacy Legislation in EU Member States – Part Two of the Practical Overview. CRi 2018, 133; *Wolff/Brink* in Wolff/Brink (Eds.), Beck'scher Onlinekommentar Datenschutzrecht, 34. Ed., 1.11.2019, Einleitung zur DS-GVO, par. 19.

27 Cf. *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann (Eds.), Datenschutzrecht, 2019, Baden-Baden, Art. 4 Nr. 1 DSGVO, par. 58 et seqq.

28 ECJ, 10.10.2016 - C-582/14 (Breyer), NVwZ 2017, 213; *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann (Eds.), Datenschutzrecht, Art. 4 Nr. 1 DSGVO, par. 60 et seqq.; *Kühling/ Klar*, Speicherung von IP-Adressen beim Besuch einer Internetseite, ZD 2017, 24, 28.

29 Cf. Art. 3 No. 1 Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, COM (2017) 495 final.

30 *Albers/Veit* in Wolff/Brink (Eds.), Beck'scher Onlinekommentar, Art. 9, par. 17 et. seq.; *Weichert* in Kühling/Buchner (Eds.), DS-GVO – BDSG Kommentar, 3. Ed., Munich 2020, Art. 9, par. 2.

31 Recital 51, cl. 1 GDPR; *Albers/Veit* in Wolff/Brink (Eds.), Beck'scher Onlinekommentar, Art. 9, par. 17 et. seq.; *Franzen*, in: Franzen/Gallner/Oetker (Eds.), Kommentar zum europäischen Arbeitsrecht, 3. Ed., Munich 2020, Art. 9 DSGVO, par. 1; *Weichert*, *Thilo*, 'Sensitive Daten' revisited, DuD 2017, 538, 538 ff.

32 Recital 51 cl. 1 GDPR; *Franzen* in Franzen/Gallner/Oetker (Eds.), Kommentar zum europäischen Arbeitsrecht, Art. 9 DSGVO, par. 1.

33 *Albers/Veit* in Wolff/Brink (Eds.), Beck'scher Onlinekommentar, Art. 9, par. 1; *Veil*, *Winfried*, Die Datenschutz-Grundverordnung: des Kaisers neue Kleider, NVwZ 2018, 686, 693.

34 *Albers/Veit* in Wolff/Brink (Eds.), Beck'scher Onlinekommentar, Art. 9, par. 16; *Simitis*, *Spiros*, Die EU-Datenschutzrichtlinie, NJW 1997, 281, 283.

35 *Müllmann*, *Dirk*, Auswirkungen der Industrie 4.0 auf den Schutz von Betriebs- und Geschäftsgeheimnissen, WRP 2018, 1177, 1178, 1180.

aims to protect personal data against the dangers of their processing, data security embraces all measures to preserve data from misuse and interference of risks from outside of the process of processing.[36] A justified use of personal data always requires adequate safety and security measures. An appropriate security level considers the technical state-of-the-art, the costs of the implementation of the security measures, the probability of occurrence of security risks, nature, scope, context, and purposes of the processing as well as the risks for the rights and freedoms of the natural persons which might especially arise from the accidental or unlawful destruction, loss, or unauthorized disclosure.[37] The processing of particularly sensitive data may, hence, only lead to more data security. However, the processing of common personal data does not mean the absence of security measures.

## IV. Information Sensitivity from the User Perspective

15 From the user perspective, the perception of how sensitive information is, influences how concerned users are about the data provision and how willingly this information is provided.[38] Thereby, the perception of sensitivity is related to the perceived risks when disclosing information[39] and, thus, related to the vulnerability and potential losses that are anticipated. Users are concerned about unauthorized use, misuse (e.g., fraud, identity theft, hackers), and improper access.[40] However, they also feel that the collection of information itself, targeted advertising, and profiling are violations of their privacy.[41] Thus, they seem not to differentiate between data privacy and data security. Moreover, the more personally identifying information is, the more it is perceived as sensitive,[42] which is in line with the GDPR covering personally identifying information. Improving data analysis technologies enable ever-deeper insights about users. Most users may not be aware of what is legally and technically possible and how, presumably non-identifiable or insensitive, data can be linked and used.

16 Besides limited knowledge about IT and law, there is another aspect that complicates the sensitivity evaluation for the users: Privacy perceptions depend on context and audience.[43] We learn from early childhood on how to manage our privacy in an offline world. But online, data is persistently available over space and time, confusing the context in which we disclose information and those in which it can be accessed and by whom.[44] Thus, users do not only have to include the present audience and context to evaluate the risk of disclosure and sensitivity of information but also potential access of information in the future by different entities and in different contexts. And the technological possibilities to combine data across services also need to be considered.

17 The Empirical Approach: To see not only which factors influence the perception of sensitivity, but how sensitive European Internet users perceive specific types of information, an empirical online study was conducted. In an online questionnaire, the participants evaluated 40 data types (cf. Fig. 1) on a 6-point scale from "not sensitive at all" (1) to "very sensitive" (6) (for more details on the empirical methods see Schomakers et al.[45]). The sample includes 601 participants aged between 15 and 69 years (M = 38.8, SD = 20.2). 59.1% were women.

18 The perceived sensitivity for all 40 data types is depicted in Fig. 1. Passwords are perceived as most delicate followed by financial account numbers, with both being rated "very sensitive" (M > 5.5). Personal identifiers like passport number and fingerprint, location and medical history are perceived as "sensitive." Browsing history, medication, and sexual preferences are evaluated as "rather sensitive." "Rather not sensitive" are, e.g., political affiliation, weight, and zip code. The only two information types from this list that are perceived as "not sensitive" are hair color and name of pet. Nothing was, on average, felt to be "not sensitive at all" (M < 1.5).

## V. Comparison between Legal, Technical, and User Perspective

*Fig. 1* depicts the legal and the user perspective on sensitivity. It 19
shows that users' perception of sensitivity is for some data types in line with the legal categorization but also deviates strongly for others. The data types that are perceived as most sensitive by the users (passwords, financial account numbers) are legally classified as possibly special category and no special category. This assessment by users indicates they might not differentiate between data privacy and data security. Rather, the sensitivity evaluation is based on a risk assessment, and users are concerned about unauthorized access and illicit data misuse as well as about data collection, targeted advertising, and profiling. The legal use of personal data, however, under Art. 32 GDPR always requires adequate data security measures proportionate to the risks of data processing. Hence, service operators implement established technical protection measures. However, even despite huge efforts to technically protect user data, data breaches are frequently experienced.[46]

36 *Heibey* in Rossnagel (Ed.), Handbuch des Datenschutzrechts, 1. Ed., Munich 2003, 570 et. seqq.; *Wolff/Brink* in Wolff/Brink (Eds.), Beck'scher Onlinekommentar Datenschutzrecht, Einleitung zur DS-GVO, par. 2 et seqq.

37 Cf. Art. 32 sec. 1, 2 GDPR.

38 *Mothersbaugh*, Journal of Service Research 2012, p. 76 (90).

39 Ibid, p. 90.

40 *Smith, H./Milberg, S./Burke, S.* Information privacy: Measuring individuals'concerns about organizational practices. MIS Quarterly 1996, 167 (172).

41 *Schomakers, Eva-Maria/Lidynia, Chantal/Ziefle, Martina*: Hidden within a Group of People – Mental Models of Privacy Protection. in: BDIOT 2018, 2018, p. 85 (89).

42 *Malheiros, M./Preibusch, S./Sasse, M.* "Fairly Truthful": The Impact of Perceived Effort, Fairness, Relevance, and Sensitivity on Personal Data Disclosure. in: Huth, M./Asokan, N./Capkun, S./Flechais, I./Coles-Kemp, L (Eds.), TRUST 2013, LNCS 7904, 2013, p. 250 (259).

43 *Nissenbaum, H*: Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford 2010, p. 231.

44 *Taddicken, M.*: The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance of Different Forms of Self-Disclosure. Journal of Computer-Mediated Communication, 2014, p. 248 (250).

45 *Schomakers, Eva-Maria/Lidynia, Chantal/Müllmann, Dirk/Matzutt, Roman/Wehrle, Klaus/Spiecker gen. Döhmann, Indra/Ziefle, Martina*. Putting Privacy into Perspective – Comparing Technical, Legal, and Users' View of Information Sensitivity, in: Reussner, Ralf H./Koziolek, Anne/Heinrich, Robert (Eds.) 50. Jahrestagung der Gesellschaft für Informatik INFORMATIK 2020, Back tot he Future, Bonn: Gesellschaft für Informatik, p. 847.

46 *Hunt, T.*: Have I Been Pwned?, https://haveibeenpwned.com (accessed 2020-06-29).

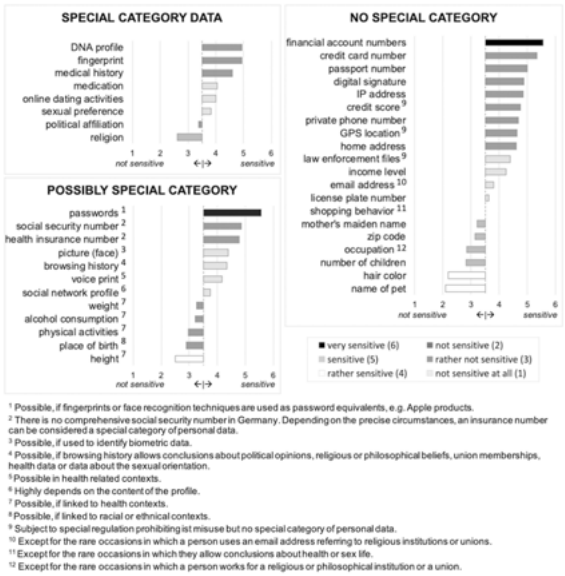


*Figure 1. Users' evaluation of the sensitivity of 40 data types (n = 601) categorized into the legal classification.*

## 1. Leverage Points for Discrimination

20 Data protection starts earlier, though, and already tries to minimize occasions and purposes in which personal data is collected and processed. While users' estimate of information sensitivity might anticipate the uncontrolled release and accept the necessity of the processing in other contexts, data protection law operates with wider categories and has internalized context dependency. Hence, from a legal point of view, the additional protection of special categories of personal data aims at categories whose general acquisition, irrespective of its legality, might bear severe risks and consequences. Thus, the legislator even restricted the contexts of legal uses compared to regular personal data.

21 Political affiliation and religion are classified as special category and particularly deserving of protection by the GDPR but are assessed as 'rather not sensitive' on average by the participants of the survey. The German view on data protection is, among other factors, highly influenced by the country's historical experience of two dictatorships cementing their power through surveillance and control and the potential as well as the risks of modern electronic data processing.[47] This affected the development of the European data protection law.[48] The legal point of view on special categories of personal data, as the most sensitive pieces of information in data protection law, mainly concern issues that can be used as leverage points for discrimination, such as religious believes, political opinions, or sexual orientation, and are closely connected to the exercise of fundamental rights, e.g., union memberships. Therefore, they need the particular protection of the democratic society and its laws. This aspect does not have the same importance for common users and the deviation between law and user evaluation can be explained by the methodological approach to report the mean user evaluation: For many users who have mainstream political views or a religion that are not discriminated against, these information types may not seem sensitive. The minority of users who may be discriminated against on these grounds do not have much weight within the average evaluation but still need protection from discrimination. Short-term financial losses and other acute consequences of released data are more relevant to the user, while the legislator has to consider long-term implications for the individual and the democratic society as a whole.

## 2. The Privacy Calculus

Voluntary sharing of personal information in social media can 22
make users vulnerable and create possibilities for harm. Users see these risks to some extent and state that they are concerned, but nevertheless, disclose this information.[49] One explanation for this privacy paradox in user behavior is provided by the theory of the privacy calculus which assumes that users weigh perceived benefits and perceived privacy risks against each other.[50] Thus, they disclose information when the benefits outweigh the risks. Correspondingly, the evaluation of risks is only one side of the coin. Self-disclosure on social network sites brings many benefits to the individual including self-representation, relationship development, and social control.[51] These may outweigh the perceived concerns. Granting consent allows users this self-determination with regard to their data. At the same time, however, it poses considerable practical problems as to the aspects of being voluntary and informed.

A topical example for trade-offs between privacy risks and self- 23
disclosure and anticipated benefits could be observed for the contact tracing apps for COVID-19 pandemic. Citizens can choose whether to use a contact tracing app with the varying privacy risks and information disclosure needs the different apps entail internationally[52] thereby helping to protect their own, dear ones' and the public's health and lives. The varying success in the dissemination of different contact tracing apps could, furthermore, allow conclusions to be drawn about how users weigh up the disclosure of even sensitive data and their privacy. The German Corona warning app is considered particularly secure in terms of data protection. The anonymity of users is maintained throughout and contact data is stored in a decentralized manner,[53] a fact that has also been publicly communicated by trustworthy authorities[54]. For this reason, it is of-

47 *Bull, Hans Peter*, Informationelle Selbstbestimmung, 1. Ed, Tübingen 2011, p.9 et seqq.; *Masing, Johannes*, Herausforderungen des Datenschutzes, NJW 2012, 2305.

48 *Reding, Viviane*, Sieben Grundbausteine der europäischen Datenschutzreform, ZD 2012, 195.

49 *Gerber/Gerber/Volkamer*, Computers & Security, 2018, p. 226.

50 *Dinev, T./Hart, P.*: An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research, 2006, p. 61.

51 *Lee, H./Park, H./Kim, J.* Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefits and risk. International Journal of Human-Computer Studies, 2013, p. 862.

52 Ahmd, Nadem/Michelin, Regio A./Xue, Wanli/Ruj, Sushmita/Malaney, Robert/Kanhere, Salil S./Seneviratne, Aruna/Hu, Wen/Janicke, Helge/Jha, Sanjay K. A Survey of COVID-19 Contact Tracing Apps. IEEE Access 2020, p. 134577.

53 *Kühling, Jürgen/Schildbach, Roman*, Corona-Apps – Daten- und Grundrechtsschutz in Krisenzeiten, NJW 2020, 1545, 1546, 1548 ff.

54 Cf. Rzepka, Chaos Computer Club lobt deutsche Corona-App, 16.06.2020, https://www.zdf.de/nachrichten/politik/corona-app-launch-100.html (accessed 2021-01-21); Anke Domscheit-Berg in a Interview with ZDF heute journal, 14.06.2020, https://www.zdf.de/nachrichten/politik/coronavirus-domscheit-berg-corona-warn-app-100.html. (accessed 2021-01-21).

ten – wrongly[55] – blamed for being ineffective.[56] However, with 25.2 million downloads,[57] it is very widespread. The French version, on the other hand, relied on central data storage, was considered critical of data protection, and was downloaded only 2.6 million times.[58] Even if other aspects and cultural differences may also play a significant role in societal acceptance of intensive collection of sensitive data, the comparison against the background of the present study allows, at least, the assumption that a high level of data protection could strengthen among users the acceptance of sensitive data being processed and increase the likelihood of users pondering the pros and cons of disclosing data under these circumstances.

24 Additionally, users do not make purely rational decisions. Rather, decision-making is affected by cognitive biases and heuristics. For example, optimism bias leads individuals to perceive themselves as less vulnerable than others[59] and affect heuristics influence the risk assessment in a way that users tend to underestimate risks when it is associated with things they like.[60] These psychological means will always influence users' decision making to some extent. Here, the aim of data legislation and privacy preserving technologies should be to guarantee users an online environment in which they can freely decide what to share, following the principle of informational self-determination. This also includes data protection via technical and legal means so that users are protected to the largest extent possible.

## 3. Classification of Location Data

25 Another deviation between users' and legal evaluation is the categorization of location information. GPS data can comprise distinct locations or even whole trajectories and users believe it to be sensitive, but location is not among the special categories of data in Art. 9 GDPR. Nevertheless, there is European legislation providing special rules for its processing. Directive 2002/58/EC, which was enacted to complement the former European Data Protection Directive 95/46/EC, defines it as any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communication service, Art. 2 lit. c) Directive 2002/58/EC. Art. 9 sec. 1 Directive 2002/58/EC allows the processing of this data only after its anonymization or with the consent of the users to the extent and for the duration necessary to provide an additional service. The scope of this provision, however, is limited to the regulation of data processing in the context of providing publicly available electronic communications networks,[61] e.g., by phone companies.[62] For every other purpose and processing, the rules of the GDPR apply subsidiarly, treating location data connected to person as regular personal data. Hence only in a very limited number of use cases relevant today, location data enjoy further protection by the law. Considering the possibility of creating movement profiles of users through the analysis of location data and the threats to a person's freedom and rights such profiles bear, the protection granted by law seems insufficient. One reason for this situation is the ongoing reform process of the European data protection law. The Directive 2002/58/EC relevant at hand will be renewed and transferred into a regulation in the future.[63] Hence, the current legal state does not, yet, meet today's technical challenges. Despite the oncoming reform, the classification of location data as common personal data within the GDPR should be reconsidered and a higher level of protection for location data should be created.

The contrast between the European law and examples like the 26
Chinese Social Credit System[64] shows that, due to sufficient legal regulations in Europe, users are protected against harmful aggregation of data, although this would be technically possible. The collection of license plate numbers to create a governmental "obedience score" is not conceivable, as the European fundamental rights exclude, e.g., the comprehensive assessment of a person's behavior and actions. Therefore, European users do not need to be concerned about possible consequences which could result from the collection of such data. The low sensitivity evaluation of license plate number by the German sample shows that users indeed do not see many risks connected to that information. Reliance on the current data protection law can be one reason for the low sensitivity evaluation of the license plate number by the German sample compared to other cultures.[65] This would indicate that users are aware of the legal protection granted to their data. The other hypothesis – users not being aware of potential risks – could also hold true and is important to consider regarding users' perception of privacy risks in general. Looking at data disclosure decisions through a privacy calculus lens, users need to evaluate the risks of data disclosure. To do that adequately, they need to be aware of these risks. However, they are not always privy to the legal protection and technical means.[66]

It is argued here that the main objective should not be informa- 27
tional heteronomy imposed by law over the users but informational self-determination. But this requires that users are aware and able to evaluate the risks of data disclosures. To empower

55 *Kelber, Ulrich*, Weniger Datenschutzhilft auch nicht gegen Covid-19, 23.11.2020, https://www.spiegel.de/netzwelt/netzpolitik/corona-warn-app-weniger-datenschutz-hilft-auch-nicht-gegen-covid-19-a-a3a31c6b-e876-44cb-bb84-baf95681b53f. (accessed 2021-01-21).

56 Cf. *Nida-Rümelin, Julian/Hilgendorf, Eric*: Unser Datenschutz verhindert eine wirksame Corona-Warn-App, 20.01.2021, https://www.welt.de/debatte/kommentare/plus224695267/Grundrechte-Unser-Datenschutz-verhindert-eine-wirksame-Corona-Warn-App.html. (accessed.2021-01-21).

57 RKI, status from 21.01.2021, https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Archiv_Kennzahlen/Kennzahlen_22012021.pdf?__blob=publicationFile (accessed 2021-01-21).

58 *Karp*, Nach Kritik – Frankreich startet neue Corona-Warn-App, 22.10.2020, https://www.zdf.de/nachrichten/politik/coronavirus-warnapp-frankreich-100.html (accessed 2021-01-21).

59 *Cho, H./Lee, J.-S./Chung, S.* Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. Computers in Human Behavior, 2010, p. 987.

60 *Wakefield, R.* The influence of user affect in online information disclosure. The Journal of Strategic Information Systems, 2013, p. 157.

61 Cf. Art. 3 sec. 1 dir. 2002/58/EC.

62 *Lünenbürger/Stamm* in Scheuerle/Mayen (Eds.), Telekommunikationsgesetz, 3. Ed., Munich 2018, § 3, par. 40.

63 Cf. Proposal for as Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EG, COM 2017/010final-2017/03(COD).

64 *Meissner, Mirjam*, China's Social Credit System, 24.05.2017, https://www.chinafile.com/library/reports/chinas-social-credit-system-big-data-enabled-approach-market-regulation-broad (accessed 2021-01-20).

65 *Schomakers, Eva-Maria/Lidynia, Chantal/Müllmann, Dirk/Ziefle, Martina*, Internet Users' Perseptions of Information Sensitivity, IJIM 2019, 142 et. seqq.

66 *European Commission*. Special Eurobarometer 431 "Data Protection". European Union 2015.

users here, they need to be well informed. But educational measures at school are limited, especially because of the ever-evolving technical means. Thus, education and information must be available from a trusted source for all citizens, e.g., from a governmental website. Also, qualified media coverage and easy to understand consent forms are required. Finally, technological means to prevent unauthorized access to user data or the derivation of additional information from such data need to be further improved.

## 4. Result

28 In summary, the comparison of the different perspectives on information sensitivity shows that users', technical, and legal views deviate to some degree. For example, the law grants protection to data categories as "special" categories that not all users perceive as especially sensitive. This can be seen as unproblematic as users are still able to freely disclose data, thereby giving their explicit consent to process these data. Other data categories, e.g., GPS data, are not given special privacy protection by the GDPR, but they are perceived as sensitive by the users and are, from a technological perspective, very revealing about the individual user. Here, the law nevertheless requires adequate data security measures for data processing, thus still providing protection. Rather, it is a problem that users, by allowing the processing of their data on the basis of consent without being fully aware of possible consequences, often thwart the safeguards of data protection laws which generally tries to limit the amount of processed data and the admissible purposes of its processing. For the premise of informational self-determination, it is of utmost importance to raise users' awareness about possible risks of data disclosure and the legal protection they are entitled to. As long as users decide to give their free, specific, informed, and unambiguous consent to the processing of their data as demanded by Art. 7 sec. 1, 4 No. 11 GDPR, the processing is in accordance with the law. It is, therefore, a manifestation of the users' informational self-determination which would, otherwise, turn into informational heteronomy. Finally, technological means must seek to unburden the users, i.e., provide the best data protection possible while not overly restricting the users' freedom of educated self-expression. In the current state, admittedly, perception of the importance between the three perspectives differs. However, the categories of data seen as sensitive by users and computer science are adequately protected by law, although it grants other categories, which are not rated as particularly sensitive by users, more protection for the aforementioned reasons. The comparison of the three perspectives has shown how advanced the GDPR is in protecting users' privacy but for small adjustments. The effort of the GDPR to support the privacy interests of customers – structurally inferior compared to many companies and their economic interests – balances inequalities of social forces and strengthens the pluralism and democracy in digital societies.

***Eva-Maria Schomakers***

PhD student and research assistant at the Chair of Communication Science and Human-Computer Interaction Center at RWTH Aachen University

Users' perceptions and acceptance of information technologies, privacy perceptions health and mobility context

schomakers@comm.rwth-aachen.de

***Chantal Lidynia***

Research assistant at the Chair of Communication Sciences and the Human-Computer Interaction Center at RWTH Aachen University

User perception and acceptance of innovative technologies in health and mobility contexts

lidynia@comm.rwth-aachen.de

***Dirk Müllmann***

PhD student and Senior Researcher Assistant at the Competence Center for Applied Security Technology at Karlsruhe Institute of Technology and Data Protection Center at Goethe-University Frankfurt/Main

Public Law, Data Protection Law, IT-Security Law

muellmann@jur.uni-frankfurt.de

***Roman Matzutt***

Researcher at the Chair of Communication and Distributed Systems (COMSYS) at RWTH Aachen University

Challenges and opportunities of accountable and distributed data ledgers, blockchain technology, users' privacy demands against Internet services

roman.matzutt@comsys.rwth-aachen.de

***Klaus Wehrle***

Full professor of Computer Science and Head of the Chair of Communication and Distributed Systems (COMSYS) at RWTH Aachen University

Engineering of networking protocols, (formal) methods for protocol engineering and network analysis, reliable communication software, all operating system issues of networking

wehrle@comsys.rwth-aachen.de

### *Indra Spiecker gen. Döhmann*

Full professor and chair of Public Law, Information Law, Environmental Law and Legal Theory at Goethe-University Frankfurt/Main

Public Law, Data Protection Law, IT-Security Law, Environmental Law, Legal Theory

spiecker@jur.uni-frankfurt.de



### *Martina Ziefle*

Psychologist, full professor and chair of Communication Science at RWTH Aachen University

Human interaction and communication of humans with technology in different technology types and using contexts

ziefle@comm.rwth-aachen.de