Human-Centered Design for Data-Sparse Tailored Privacy Information Provision

Mandy Goram, Tobias Dehling, Felix Morsbach, and Ali Sunyaev

1 Motivation

In the age of information with its diverse data-driven business models [9], consumers provide and share much information about themselves and others. To prevent abuse of consumer information, data protection laws have become more restrictive and require informed consent for many uses of consumer data [41]. Hence, it should be inevitable for consumers to cut their way through the privacy notices jungle to get information on privacy practices [17]. However, an uninhabitable jungle would have to be conquered; privacy notices are just confusing and impractical for consumers [28].

The intended purpose of privacy notices is to inform consumers by providing information about the privacy practices of companies and the information systems they provide [30]. Consumers face two problems: first, the sheer volume of privacy notices [22] that need to be provided for each visited website and every other type of online or offline information system, and second, the extensive texts, which are usually difficult to understand and often formulated in a complicated manner [39].

M. Goram (✉)
Karlsruhe Institute of Technology, Institute of Applied Informatics and Formal Description Methods, Karlsruhe, Germany
e-mail: mandy.goram@kit.edu

T. Dehling · A. Sunyaev
Karlsruhe Institute of Technology, Institute of Applied Informatics and Formal Description Methods, Karlsruhe, Germany

KASTEL Security Research Labs, Karlsruhe, Germany
e-mail: dehling@kit.edu; sunyaev@kit.edu

F. Morsbach
KASTEL Security Research Labs, Karlsruhe, Germany
e-mail: felix.morsbach@kit.edu

N. Gerber et al. (eds.), *Human Factors in Privacy Research*,
https://doi.org/10.1007/978-3-031-28643-8_14

This results in consumers not taking notice of privacy notices at all and often giving broad consent to data processing and sharing without knowing what they consent to [3]. This is often to the disadvantage of consumers—yet it happens with their consent [29].

Different approaches have been developed to support consumers. Privacy-enhancing technologies (PETs) support consumers, for instance, with privacy-preserving configurations of applications [18] or disguising their identity [14]. The more focused transparency-enhancing technologies (TETs), a subclass of PETs, provide information on consequences of data disclosure and information system use [26] through different forms of privacy information provision, such as, visualization concepts [36], just-in-time notifications [36], privacy seals [35], and text summaries of privacy notices [43]. Supporting consumers in making decisions on application use and data disclosure with TETs requires more than just a technique or visualization concept [36] because privacy decision-making is context-dependent: "The rules people follow for managing privacy vary by situation, are learned over time, and are based on cultural, motivational, and purely situational criteria" [2, p. 511]. Hence, privacy decisions made in one context may not be applicable in another. Privacy information provision requires knowledge about the context in which decisions are made by consumers to provide information about privacy practices that really matter to consumers in their specific situation [36]. People will, for example, have quite different privacy concerns when being asked to share health information while talking to a physician during treatment—or during a job interview.

How to account for context in privacy information provision is a pressing issue for supporting consumers with TETs. Personalization strategies are required to give consumers seamless access to context-specific information on privacy practices. This requires flexible information systems that can detect and adapt to consumer preferences, for instance, based on consumer behavior, system interactions, or previous decisions. The remainder of this chapter will shed light on how to accomplish this.

This chapter is structured as follows, we start with an overview of extant TETs, their functionalities, and potentials for tailoring. We go on with outlining a solution space for tailored privacy information provision while protecting sensitive privacy preference information. After that, we describe TET solution archetypes for tailored privacy information provision by explaining what tailoring approaches are suitable and how feasible local and remote processing is.

2 Overview of Extant Transparency-Enhancing Technologies

Various TETs have emerged in research and practice. These can be divided into six different types in terms of their functionality and purpose: privacy practice scoring, privacy practice description, privacy practice monitoring, privacy risk assessment, privacy practice history, and privacy practice comparison TETs. See Table 1 for an overview.

Table 1 Overview of the TET types, their functionalities, and examples

TET type	Abstract functionality	Examples
Practice scoring	Calculate a single score which represents how good/bad (appropriate) privacy practices are based on information from privacy notices, system functionality, or system behavior	*PrivacyMonitoring* [33]: creates a score for a website and explains how the score was calculated; *PrivacyScore* [24]: compares websites and allows consumers to rate websites on a range of security and privacy features; *Privacy Rating* [4]: based on predefined privacy aspects, the tool calculates an overall score of a website
Practice description	Describe privacy practices in an information system or of a provider and how consumer data might be used	*Layered privacy notices* [36]: present consumers with a brief notice with high-level information and allows consumers to expand each section to access more detailed information; *PrivacyCheck* [43]: text summarization tool that analyzes privacy notices through a browser plug-in; *Just-in-time notifications* [36]: appear when consumers have to make privacy decisions and present information that may be relevant for the decision
Practice monitoring	Monitor information use or other privacy practices of an information system and may alert consumers if actual divert from intended/expected practices	*Privacy Cleaner* [32]: scans, tracks, and controls access to information about a consumer, *Privacy Evaluation* [10]: evaluates popular educational applications based on a wide range of legal requirements and best practices for data protection
Risk assessment	Calculate a risk assessment for consumers based on system interactions, information shared, or privacy settings	*Cover your tracks* [11]: shows the unique and identifying features of a browser that trackers can use for identification; *Privacy Analyzer* [34]: allows consumers to see what data their browser exposes
Practice history	Lists changes in privacy notices or practices in a chronological order	*Change history summary* [8]: summarizes changes between different versions of privacy notices; *Privacy notice differences* [13, 40]: displays all changes between a document and its previous version
Practice comparison	Compares privacy practices and other characteristics between information systems	*Privacy Matters* [37]: compares popular messenger apps; *Browser Comparison Tool* [6]: compares web browsers; *Privacy Risk Index* [7]: compares mHealth apps and its privacy practices

As illustrated by the overview in Table 1, TETs come in many flavors. Yet, an all-to-common denominator is the provision of standardized information. Adaptivity to consumers' context-specific privacy preferences is a facet of TETs that offers much room for improvement. In the following sections, we will explore this untapped potential of TET with respect to stronger adaptivity to consumers' privacy preferences while protecting the confidentiality of sensitive preference information.

2.1 Tailoring Potential of Transparency-Enhancing Technologies

The TET types included in Table 2 yield different rooms for improvement by tailoring privacy information provision. Some could, for instance, be more interactive to better adapt to context-specific consumer preferences. Others overload consumers with too much information and require a more focused design. Overall, there is a lack of tailored, privacy need-based information provision. Instead of offering standardized sets of information, tailored TETs can take consumers' individual privacy preferences into account. For the tailoring, it is necessary to have information about the consumer to tailor TETs accordingly. This information can be provided by the consumer or detected automatically. Potential for tailoring information on privacy practices depends on the TET type. An overview of tailoring potentials of the different TET types is presented in Table 2.

Table 2 shows that the TET types yield room for improvement by tailoring privacy information provision to consumer privacy preferences. However, this requires access to preference information and other consumer information (Fig. 1), which poses privacy risks that should be addressed. Figure 1 shows categories of necessary consumer data for tailored information provision on privacy practices. The specific data required for tailoring depends on the TET, for example, the data required for tailored privacy practice descriptions could be a consumer's interest on data sharing practices. The privacy risks can be addressed by protecting the confidentiality of the additional information required for tailoring. To do so, technical privacy-preserving mechanisms can be used. Once information about the context-dependent preferences of consumers is available and confidentiality of that information is protected through technical privacy-preserving mechanisms, tailored privacy information provision becomes possible without introducing additional privacy risks.

3 Solution Space for Tailoring Challenges

The solution space for tailored privacy information provision requires access to privacy preferences and confidentiality protection of preference information so that tailored TETs can be made available to consumers.

Table 2 Overview of what can be tailored in the TET types

TET type	Practice scoring	Practice description	Practice monitoring	Risk assessment	Practice history	Practice comparison
Analysis features	Privacy practices considered in score	N/A	Privacy practices to be monitored	Risks to be assessed; consumer practices and device characteristics to be analyzed	Privacy practices of interest	Systems to be compared; privacy practices of interest
Analysis weights	Weights for privacy practice relevance	N/A	Relevance of monitored privacy practices	Relevance of privacy risks	N/A	N/A
Displayed information	N/A	Privacy practices on which information is displayed	N/A	N/A	N/A	Representation of monitored privacy practices
Aggregation level	Granularity of explanations for calculated score	Granularity of information presented on privacy practices	N/A	Granularity of explanations for determined risks	Level of detail on which changes should be tracked	Level of detail on which differences should be reported
Notification	N/A	N/A	Means to inform the consumer about deviations from intended privacy practices	N/A	N/A	N/A
Visualization	score (e.g., categorical)	privacy practices (e.g., icons)	monitored privacy practices	assessment outcomes	changes over time	differences between privacy practices

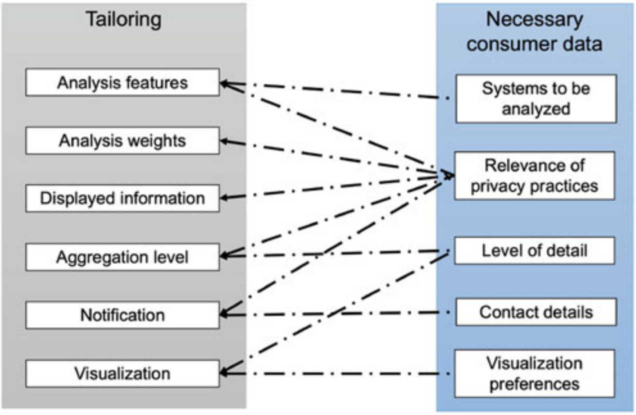

Fig. 1 Mapping of necessary consumer data for tailoring approaches

3.1 Privacy Preferences

For tailored privacy information provision, information about privacy preferences is required to tailor information provision to consumers' privacy needs. Consumer preferences can be elicited via three general approaches: (1) standardized preferences, (2) consumer-specified preferences, and (3) automatic detection of preferences.

Standardized preferences are specified by software designers or the software developer when the consumer interface is designed and cannot be changed by consumers. Preferences are represented statically in the design, for instance, what information is made available [22], how a privacy score is calculated [4], or what consumer archetypes are predefined [12]. Provision of information on privacy practices may be based in part on consumer studies investigating which privacy practices are important and should be considered when providing and preparing information on privacy practices [17]. However, the results of consumer studies do not capture the diverse situation-specific factors and circumstances that will be present when a consumer is actually using the TET [27]. Hence, standardized preferences are likely to not match the actual privacy preferences in real use contexts [25].

Consumer-specified preferences are more likely to match actual privacy preferences in real use contexts. Preference information is stored in consumer profiles [38] or collected as part of a session (e.g., through search queries and filters). Preference profiles can be created with various explicit preference elicitation approaches and require consumers to manually set their preferences [23], for example, through situation-specific questionnaires, preference menus, search queries, search filters, or ratings. Explicit preference elicitation approaches burden consumers with additional effort to decrease the gap between captured and real preferences [20]. Thus, they bear the risk to overwhelm consumers by being overly complex. On the other hand, simple explicit approaches may not offer sufficient degrees of freedom to close the gap far enough, so that outcomes may not improve much over preference standardization [20].

Automatic detection of preferences avoids this trade-off. Here, preferences are derived from consumer interactions with the system to better match real use contexts without requiring additional consumer effort [38]. Automatic detection approaches detect various consumer characteristics through observation of system interactions (e.g., mouse movements, content clicked, reading time, or location) or may leverage data collected beyond the application boundary (e.g., physical reactions, facial expressions, or eye movements) [44]. Based on the collected data, consumer preferences can be derived in a more context-specific manner. However, this requires complex technical procedures and extensive data collection [38]. In addition, consumers may find the subliminal data collection inappropriate and there is always the risk of false classification. We will discuss PETs suitable for tailored TETs in the next section.

3.2 Technical Privacy-Preserving Mechanisms

In a classic information system architecture, the necessary data required for tailored information provision is collected on consumer devices (e.g., a mobile phone or laptop) and transmitted to a server operated by the information system provider. The provider processes the data to generate tailored privacy information and sends this back to the consumer device. In this architecture, the information system provider has full access to the necessary data required for tailored privacy information provision, information that is in itself sensitive [38]. This poses a privacy risk for consumers. While the information system provider may have limited data use to prespecified purposes and may have consent according to the General Data Protection Regulation (GDPR) [15], recent data breaches and scandals have shown that these practices do not guarantee the protection of consumer data against misuse [19].

An alternative approach is to not collect or process the raw data on a central server in the first place. The possibility of misuse is significantly reduced when data is not collected by a third party. The raw data stays with the consumer and the tailoring of information provision can happen in such a way that the system provider has no direct access to consumer data. The privacy-enhancing technologies community [31] developed multiple approaches and techniques that can be used to mitigate these privacy risks by protecting the confidentiality of privacy preferences. In the following paragraphs, we will briefly describe and outline the potential use of local computation, homomorphic encryption (HE), and secure multiparty computation (SMPC)—three common options for privacy-preserving computing [21].

Local computing restricts processing of consumer preferences and tailoring of privacy information to the consumer device itself. For some use cases and applications, it is not necessary to process the data on a third-party server. For example, the weighting of privacy practice score criteria is not a complicated or resource-intensive operation and can easily be done on a mobile device. Therefore, whenever possible, the tailoring of privacy information should happen only on the consumer device. However, some data processing may either require too much data to be done on mobile devices, for example, data about privacy practices of multiple information systems, or require access to some central component that cannot be stored on consumer devices, for example, to protect intellectual property. In this case, there are technical methods for privacy-preserving computation that allow for processing of data while protecting confidentiality of consumer data.

Homomorphic encryption (HE) [1] allows to perform calculations on encrypted data. The input data is encrypted and the operation is executed on the cipher text. The result of this blindfolded operation will be decrypted and will then match the output of the operation as if it had been performed directly on plain data. HE can be used in TETs to compute operations on confidential data. A consumer can, for example, encrypt their private data locally on their device using local encryption keys and send the encrypted data to an information system provider. The provider computes the desired operation, here, the tailored privacy information provision, on the encrypted data and sends the constantly encrypted results back to the consumer device. The consumer can then decrypt and use them using the local keys. In this way, the information system provider has no access to sensitive consumer data (neither input nor output of the tailoring operation) but can still perform its job, even if application of proprietary code is required. While HE allows for private computation on sensitive data, it comes with a high computation overhead on the information system providers' side, especially, with respect to memory consumption. This makes homomorphic-encrypted calculations very expensive and limits its attractiveness for ubiquitous application.

Secure multi-party computation (SMPC) is a collection of methods and algorithms in which a group of consumers wants to compute a joint function on their private data without revealing their private inputs. For example, in the millionaire's problem, two persons want to determine who of them is richer without revealing their own wealth to the other [42]. This setting is also a special case and called secure two-party computation (S2PC). S2PC is especially interesting due to its high relevance in many real-world scenarios such as private database queries. S2PC can be used to protect consumer preference data by computing an SMPC function, while consumer preferences are stored on the consumer devices and serve only as input to the shared SMPC function. This way, the inputs remain hidden from the information system provider. By also encrypting the result with a secret key only known to the consumer using the SMPC function, the tailored output would also remain hidden from the information system provider. While generally any function can be implemented in an SMPC fashion [16] and general-purpose compilers for doing so exist, the applicability of SMPC is often severely limited by its high communication bandwidth requirements. There exist multiple approaches to realize

SMPC, but approaches based on Yao's garbled circuits [5] are said to be the most widely applicable ones, in which the function to be evaluated is transformed into a Boolean circuit. In this approach the execution cost scales linearly with the size of the circuit. This makes SMPC often less suitable for scenarios with resource-constraint devices, such as mobile phones.

The exact overhead and resources requirements of HE and SMPC highly depend on the concrete implementation and the computations required. HE is generally said to be cheap for client devices but computationally expensive for the server side, especially in memory consumption. SMPC, however, is generally said to be computationally cheap but requires a high communication bandwidth between the participating parties.

4 Solution Archetypes for Tailored Privacy Information Provision

4.1 Suitability of Tailoring Approaches

To provide consumers with easy and quick access to privacy information, it is important to take their individual information needs into account. However, it is not always appropriate to apply consumer-specified or detected tailoring to all TET types. Table 3 shows which tailoring approaches are suitable for which TETs.

Privacy practice scoring TETs provide an overview and summary of privacy practices of an information system. A standardized privacy practice scoring TET uses evaluation criteria specified by TET providers. Standardization of privacy practice scoring is appropriate when consumers want to get a general or first impression of a system or its provider without having to make elaborate settings on their own (Type Practice Scoring TETs:standardized). If consumers want to include specific aspects in the app score or set their own weights, scoring TETs must allow for customizability, as is possible with consumer-specified approaches (Type Practice Scoring TETs:consumer-specified). Preference detection is not recommended

Table 3 Comparison of the usefulness and applicability of standardized approaches, consumer-specified approaches, and detection approaches for TET type tailoring. Legend: −− very unsuitable, − unsuitable, + suitable, ++ very suitable, *N/A* not applicable

	Standardized	Consumer-specified	Detected
Practice scoring	+	++	−
Practice description	−−	+	++
Practice monitoring	−−	++	+
Risk assessment	++	+	N/A
Practice history	−−	+	++
Practice comparison	+	++	+

because it is not transparent to the consumer how the rating was calculated and what preferences are included (Type Practice Scoring TETs:detected).

Privacy practice description TETs inform consumers about privacy practices. Standardization means that all information about privacy practices considered relevant by the standardization body is provided (Type Practice Description TETs:standardized), which may lead to mismatches between communicated information and consumers information needs [39]. To provide consumers with quick and easy access to relevant privacy practice information, it makes sense to tailor privacy information to consumers information needs. Consumer-specified preference information can be used to filter for relevant privacy information (Type Practice Description TETs:consumer-specified). But consumers may not know what to look for when they are faced with filters, key words, or other kinds of proxies because most of the consumers are not privacy experts. Preference detection is a better way to provide relevant privacy information. Consumers must not know specific search terms or filter criteria because preference detection makes the connection between their privacy preferences and the underlying privacy information without any explicit user engagement (Type Practice Description TETs:detected).

Privacy practice monitoring TETs provide consumers with an overview of activities of an information system. A standardized monitoring includes information defined by TET providers. Consumers get only information others find relevant but cannot tailor monitoring to their own information needs, which is why standardized privacy practice monitoring is not consumer-friendly (Type Practice Monitoring TETs:standardized). A consumer-specified view of the processed data helps consumers to find the relevant information faster and tailor the monitoring to their own needs (Type Practice Monitoring TETs:consumer-specified). Preference detection is suitable too and offers faster access to relevant information because no input is required from consumers. However, proper working privacy practice monitoring based on preference detection requires suitable data to infer privacy preferences, which is hard to come by for monitoring (Type Practice Monitoring TETs:detected).

Privacy risk assessment TETs aim to make consumers aware of privacy risks. Standardization of the information provided is therefore appropriate, as risks unknown to consumers are also considered (Type Risk Assessment TET:standardized). Consumer-specified preference information can, however, be used to focus the assessment (Type Risk Assessment TETs:consumer-specified). Instead of providing access to all browser, app, or device content, it should be possible to make a dedicated decision about access and the scope of the evaluation. Preference detection (Type Risk Assessment TET:detected) is far too complicated for such a specific TET, as it is far too indeterminate to infer preferences for risk assessment from interaction data.

Privacy practice history TETs indicate changes in privacy practices through brief summaries or a comparison between old and new privacy practices. Standardization of privacy practice histories cannot account for individual consumer preferences. Therefore, a standardized privacy practice history does not add value to privacy information provision (Type Practice History TETs:standardized). Consumers should be able to choose how and about what they are informed, which is possible through consumer-specified approaches (Type Practice History TETs:consumer-specified). Even better would be to communicate also information on novel privacy practices, which would be possible via preference detection without need for manual effort and additional knowledge by the consumer (Type Practice History TETs:detected).

Privacy practice comparison TETs allow consumers to compare privacy practices between different information systems. Standardization of comparison features supports consumers in getting an overview over privacy practices (Type Practice Comparison TETs:standardized). But consumers should at least choose by themselves which information systems to compare against each other. The consumer-specified approach has an advantage, since a targeted selection of criteria gives consumers quicker access to information that is of interest to them (Type Practice Comparison TETs:consumer-specified). Preference detection is suitable too because of the quicker facilitation of access to relevant information. However, preferences detection makes it harder for consumers to keep track of changes in comparison criteria (Type Practice Comparison TETs:detected).

4.2 Feasibility of Local and Remote Processing

After having had a look on what types of TET tailoring approaches are a suitable solution for better provision of privacy information, we now move on to possible implementation approaches that can be deployed either locally or remotely, with different confidentiality-protecting mechanisms. Table 4 shows an overview of possible implementation approaches and their applicability for tailored TETs.

For privacy practice scoring TETs, which provide an overview and summary of privacy practices of an information system, and privacy practice description TETs, which inform consumers about privacy practices, the standardized approach is best realized with remote processing, as no adjustments based on user data are made. Consumer-specified and detected preferences can be processed locally, as the necessary calculations are not too computationally intensive. Hence, remote processing using HE is preferable if remote processing is necessary.

Privacy practice monitoring TETs provide consumers with an overview of activities of an information system. They can use local and remote processing for the standardized approach. It is important to keep in mind that in a local setting, only the locally available data and activities are available for monitoring; the same applies to remote approaches, which can only monitor provider activities. For consumer-specified tailoring, HE is preferable to SMPC as the preferences will likely only change very infrequently and the encrypted preferences can be reused. With a detection approach, changes will be more frequent and diminish this advantage, resulting in more overhead. Thus, SMPC should be a more suitable choice.

Table 4 Comparison of the applicability of standardized approaches, consumer-specified approaches, and detection approaches for TET type tailoring in local and remote environments. Legend: −− very unsuitable, − unsuitable, 0 not useful, + suitable, ++ very suitable, *N/A* not applicable

		Local	Remote	Remote with HE	Remote with SMPC
Practice scoring	Standardized	−−	++	N/A	N/A
	Consumer-specified	+	−−	++	+
	Detected	+	−−	++	+
Practice description	Standardized	−−	++	N/A	N/A
	Consumer-specified	+	−−	++	+
	Detected	+	−−	++	+
Practice monitoring	Standardized	+	+	N/A	N/A
	Consumer-specified	+	−−	++	+
	Detected	++	−−	+	++
Risk assessment	Standardized	++	−−	0	0
	Consumer-specified	++	−−	0	0
	Detected	++	−−	0	0
Practice history	Standardized	−−	++	N/A	N/A
	Consumer-specified	++	-	+	+
	Detected	++	−−	+	++
Practice comparison	Standardized	−−	++	N/A	N/A
	Consumer-specified	+	−−	++	+
	Detected	+	−−	+	++

Privacy risk assessment TETs use consumer data to calculate an individual risk score. Tailoring can be used to specify the analysis activity more precisely. For the standardized, consumer-specified, and detected approach, the necessary analyses can take place locally on the consumer device. The use of remote approaches is therefore not justified. HE and SMPC could be applied but without any benefits and would, therefore, constitute a waste of resources.

Tailoring privacy practice history TETs, which indicate changes in privacy practices through brief summaries or a comparison of past and current privacy practices, is best realized remotely when using standardized preferences, as there is no need for every device to calculate the same tailoring. Tailoring using consumer-specified or detected preferences can be done best locally. If the processing has to be done by the TET provider, the data should be protected: HE should be used when using consumer-specified preferences, as they are unlikely to change often and SMPC is more appropriate to handle the frequent changes when detecting preferences.

Privacy practice comparison TETs require lots of data about different providers in order to allow consumers to compare privacy practices between different information systems. This makes local processing for the standardized approach difficult; instead, remote processing is the most suitable choice, as no data needs to be collected from the consumer. In case of consumer-specified and detected tailoring, processing can be done locally, but it needs access to many data sources, which provide content for the tailoring that must be stored locally. Hence, encrypted remote processing makes sense to avoid storing multiple redundant copies of the same data. In the case of consumer-specified tailoring, HE should be used because consumers are unlikely to change their preferences once specified for the comparison to be made. In the case of detection, preferences are adapted more frequently, so SMPC is most likely a better choice.

5 Conclusions

In the beginning of this chapter, we set out to find a way through the privacy notice jungle. The good news is that there is a way. Even if revelation of privacy preferences is a “No-Go!” for consumers, we can realize confidentiality of privacy preferences through information systems design and offer tailored privacy information provision with confidentiality of privacy preferences. However, depending on the concrete use case and implementation, there might be a significant computational overhead compared to designs that do not provably protect the confidentiality of privacy preferences. A long road lies ahead; it should be kept in mind that there are no out-of-the-box solutions for tailored privacy information provision, nor do all approaches work equally well. Implicit detection approaches need very comprehensive data to perform reliable preference detection, which is not always technically feasible (e.g., tracking diverse sensor data in every situation) or practical (e.g., collecting a high amount of data for simple tailoring approaches like applying a filter criteria). Explicit consumer-specified preferences also have a drawback. Consumers have to think about and decide for themselves which settings they want in which situations. This may lead to frustration and rejection among consumers when privacy settings have to be repeatedly configured. Therefore, a sophisticated approach for using privacy preferences across a variety of information systems and a mix of implicit and explicit approaches is needed to provide consumers with real value and a path through the privacy notice jungle. On a more abstract level, the key takeaway of this chapter is that we should put more thought into what we are building and using our systems for to allow for privacy through human-centered design instead of static, predefined solutions which do not meet consumer needs. Since consumer privacy preferences are context-dependent [36], TETs need to be context-sensitive. Making this possible requires, however, even more consumer data more consumer data, which may cue additional privacy concerns. Yet, this is not as bad as it seems. In this chapter, we have outlined the parameters that can be adjusted for TETs and how privacy-preserving approaches can be implemented. The new and further development of TETs is in the hands of privacy researchers and privacy practitioners.

Acknowledgments This work was partially funded by a research grant for the project PANDIA: platform for the analysis of privacy notices of interactive assistance systems in the health care domain—consumer-centered privacy communication (German Federal Ministry of Education and Research (BMBF), funding reference number: 16SV8398). This work was also supported by funding from the topic Engineering Secure Systems of the Helmholtz Association (HGF) and by KASTEL Security Research Labs.

References

1. Acar, A., Hidayet Aksu, A. U., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys, 51*(4), 1–79.
2. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514.
3. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology, 30*(4), 736–758.
4. Barth, S., Ionita, D., Jong, M. D., Hartel, P. H., & Junger, M. (2021). Privacy rating: A user-centered approach for visualizing data handling practices of online services. *IEEE Transactions on Professional Communication, 64*(4), 354–373.
5. Beaver, D., Micali, S., & Rogaway, P. (1990). The round complexity of secure protocols. In *Proceedings of the twenty-second annual ACM symposium on Theory of computing - STOC '90* (pp. 503–513). ACM Press.
6. Browser comparison tool | avoidthehack! https://avoidthehack.com/util/browser-comparison
7. Brüggemann, T., Hansen, J., Dehling, T., & Sunyaev, A. (2016). An information privacy risk index for mhealth apps. In *Proceedings of the 4th Annual Privacy Forum* (pp. 190–201). Springer.
8. Change history for Microsoft privacy statement–Microsoft privacy. https://privacy.microsoft.com/en-us/updates
9. Clemons, E. K. (2019). *New patterns of power and profit: A strategist's guide to competitive advantage in the age of digital transformation* (1st ed.). Palgrave Macmillan.
10. Common sense privacy evaluations. https://privacy.commonsense.org/evaluations/1
11. Cover your tracks. https://coveryourtracks.eff.org/
12. Dehling, T., Schmidt-Kraepelin, M., Demircan, M., Szefer, J., & Sunyaev, A. (2016). User archetypes for effective information privacy communication. In *Proceedings of the Pre-ICIS Workshop on Information Security and Privacy, AIS.*
13. Difference check tool. https://www.man7.org/linux/man-pages/man1/diff.1.html
14. Dingledine, R., Mathewson, N., & Syverson, P. (2004). *Tor: The second-generation onion router*. Naval Research Lab Washington DC.
15. General Data Protection Regulation (GDPR). (2016). https://gdprinfo.eu/
16. Goldreich, O., Micali, S., & Wigderson, A. (1987). How to play any mental game. In *Proceedings of the Nineteenth ACM Symp. on Theory of Computing, STOC* (pp. 218–229).
17. Habib, H., Zou, Y., Yao, Y., Acquisti, A., Cranor, L., Reidenberg, J., Sadeh, N., & Schaub, F. (2021). Toggles, dollar signs, and triangles: How to (in)effectively convey privacy choices with icons and link texts. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1–25). ACM.
18. Heurix, J., Zimmermann, P., Neubauer, T., & Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers & Security, 53*, 1–17.
19. Hu, M. (2020). Cambridge analytica's black box. *Big Data & Society, 7*(2), 205395172093809.
20. Jawaheer, G., Weller, P., & Kostkova, P. (2014). Modeling user preferences in recommender systems: A classification framework for explicit and implicit user feedback. *ACM Transactions on Interactive Intelligent Systems (TiiS), 4*, 2:1–26.

21. Kaaniche, N., Laurent, M., & Belguith, S. (2020). Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. *Journal of Network and Computer Applications, 171*, 102807.
22. Kelley, P. G., Cesca, L., Bresee, J., & Cranor, L. F. (2010). Standardizing privacy notices: An online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery.
23. Loepp, B., Hussein, T., & Ziegler, J. (2014). Choice-based preference elicitation for collaborative filtering recommender systems. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14), Association for Computing Machinery* (pp. 3085–3094).
24. Maass, M., Wichmann, P., Pridöhl, H., & Herrmann, D. (2017). Privacyscore: Improving privacy and security via crowd-sourced benchmarks of websites. arXiv:1705.05139 [cs].
25. Milne, G. R., Pettinico, G., Hajjat, F. M., & Markos, E. (2017). Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing. *Journal of Consumer Affairs, 51*(1), 133–161.
26. Murmann, P., & Fischer-Hubner, S. (2017). Tools for achieving usable ex post transparency: A survey. *IEEE Access, 5*, 22965–22991.
27. Nissenbaum, H. F. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books.
28. Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society, 23*(1), 128–147.
29. Peppet, S. R. (2011). Unraveling privacy: The personal prospectus and the threat of a full-disclosure future. *Northwestern University Law Review, 105*(3), 1153–1204.
30. Pollach, I. (2006). Privacy statements as a means of uncertainty reduction in www interactions. *Journal of Organizational and End User Computing, 18*(1), 23–49.
31. PoPETs/P.E.T.S. (2022). https://petsymposium.org/
32. Privacy cleaner. https://chrome.google.com/webstore/detail/privacy-cleaner/liiikhhbkpmpomjmdofandjmdgapiahi
33. Privacy Score Guide. Privacy monitor. https://www.privacymonitor.com/score/
34. Privacy test & analyzer: See what information websites know about you. https://privacy.net/analyzer/
35. Rodrigues, R., Wright, D., & Wadhwa, K. (2013). Developing a privacy seal scheme (that works). *International Data Privacy Law, 3*(2), 100–116.
36. Schaub, F., Balebako, R., Durity, A., & Cranor, L. (2015). A design space for effective privacy notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)* (pp. 1–17). USENIX Association.
37. Secure messaging apps comparison | privacy matters. https://www.securemessagingapps.com/
38. Shanmugarasa, Y., Paik, H.-y., Kanhere, S. S., & Zhu, L. (2022). Automated privacy preferences for smart home data sharing using personal data stores. *IEEE Security Privacy, 20*(1), 12–22.
39. Sunyaev, A., Dehling, T., Taylor, P. L., & Mandl, K. D. (2014). Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association, 22*(e1), 28–33.
40. Updates: Privacy policy—privacy & terms–Google. https://policies.google.com/privacy/archive?hl=en-US
41. Woods, D. W., & Böhme, R. (2022). The commodification of consent. *Computers & Security, 115*, 102605.
42. Yao, A. C. (1982). Protocols for secure computations. In *23rd Annual Symposium on Foundations of Computer Science* (pp. 160–164).
43. Zaeem, R. N., German, R. L., & Barber, K. (2018). Privacycheck: Automatic summarization of privacy policies using data mining. *ACM Transactions on Internet Technology, 18*(4), 1–18.
44. Zhang, S., Feng, Y., Bauer, L., Cranor, L. F., Das, A., & Sadeh, N. (2021). "Did you know this camera tracks your mood?" Understanding privacy expectations and preferences in the age of video analytics. In *Proceedings on Privacy Enhancing Technologies 2021* (Vol. 2, pp. 282–304).