


A Need for Privacy-Assistive Technology in Notice and Consent Paradigm in IoT

Shukun Tokas ^[0000-0001-9893-6613] and Gencer Erdogan^[0000-0001-9407-5748]

Sustainable Communications Technologies, SINTEF Digital, Oslo, Norway
{shukun.tokas, gencer.erdogan}@sintef.no

Abstract. A privacy notice is a document/notification that is addressed to consumers, describing how their personal information will be handled. While browsing the Internet, installing an app on smartphone, setting up a smart sensor or IoT devices in personal spaces, consumers are often asked to consent to privacy notices. Ideally, the consumer is expected to read and understand the notice and give an informed consent. These notices are often lengthy and complicated, containing legal-technical jargons and ambiguous statements describing commercial use of personal data. Most people reflexively choose “I consent”, unknowingly agreeing to unfair-deceptive practices. Given the ubiquity of IoT and thus ubiquity of (personal) data collection, the reliance on notice and consent is inappropriate. In this article, we present the challenges of the *notice and consent* paradigm, and explore the idea of privacy-assistive solutions to enhance consumer privacy awareness and control in IoT.

Keywords: Privacy, automated notice processing, informed consent, consumer control, privacy-assistive technology, privacy-enhancing technology.

1 Introduction

The Internet of Things (IoT) describes the network of physical objects embedded with sensors, software, and other technologies to exchange data with other devices and systems over the Internet. These objects deployed in public and private spaces enable use cases that enhance productivity and quality of life. There is a trend where companies offer cheap IoT devices in exchange for the data they collect from consumers using these devices. This trend is popularly known as *surveillance capitalism*, “it is an economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales” [46]. The data is used to “anticipate what you will do now, soon, and later ” [46]. It raises privacy concerns as an enormous amount of personal data is collected through IoT devices such as fitness trackers, home sensors, and connected vehicles. Several research studies and surveys reveal that privacy concerns are at an all-time high, as the collection and use of data in IoT are happening with very little or no control, and organizations collecting data are most of the time unknown to data subjects. For example, a Norwegian population survey [26] reveals that two out of three respondents feel uncomfortable

about commercial actors collecting information about them. Cisco’s value/trust paradox report [8] reveals the divide between IoT value and trust: 53% of participants feel IoT makes their life more convenient, while only 9% trust that their data collected and shared through IoT is secure. Despite the trust deficit and perceived risk, 42% say IoT is too integrated into their lives to disconnect from IoT services. This growing trend of lack of transparency and absence of support for data subjects to control the collection and processing of their data in IoT may heavily affect many areas of our lives and even constitute a long-term danger for democracy and voting [34]. In particular, the sensor data can be used in specific kind of marketing, i.e., election politics, where personalized marketing is used to target voters [34] by means of behavioral modification at scale [46]. It is evident that analysis of personal data had played a prominent role in Brexit campaign, and election campaigns in both the USA and France [27]. In response to the emerging privacy concerns, the European Parliament has approved the General Data Protection Regulation (GDPR) [14] to strengthen and impose data protection across the European Union (EU) and the European Economic Area (EEA). Several studies have investigated the impact of GDPR on consumers. For instance, a survey carried out by Cisco [9] confirms that 55% of respondents view GDPR very favorably, 84% respondents indicated that they care about privacy, and Of this group, 80% respondents said they are willing to act to protect it. Furthermore, an analysis from Godinho and Adjerid [19] found that only 6.2% of participants gave opt-in consent to the personal data collection (e.g., location data), in particular consumers to make deliberative choices and permit uses of data that directly benefit them and pose less risk. Overall, there is a positive view of GDPR among consumers, but there is a negative side to it, e.g., as per Cisco survey [9] 47% respondents expressed notification fatigue and said they receive far too many privacy notices as a result of GDPR. Moreover, Visa’s Consumer Empowerment Study found that 76% of people desire greater control or the choice to have more control over their personal information [6].

In this article, we focus on a crucial privacy concept, *consent*. According to the GDPR there are six lawful basis of processing personal data: contractual necessity, consent, legal obligation, vital interests, public interests and legitimate interests. The service providers of data-enabled technologies or smart infrastructure must carry out the processing of personal data within the limit of the applicable processing grounds. Consent is one of the most discussed basis of processing, and is also a core principle of data protection as “it relates to the exercise of fundamental rights of autonomy and self-determination” [29]. Consent is the lawful ground that reflects a data subject’s agreement and provides the data controller with permission to process a subject’s personal data for specific purposes. Arguably, consent is often the most exploited legal ground for processing personal data.

Most of us have had these experiences of giving consent in different situations where stakes can be low, e.g., small financial transactions, browsing news on Internet, or even where stakes can be high, e.g., medical procedures, legal transactions, continuous monitoring through wearable technology. Consumers accept

all the risks detailed in privacy notices, without even reading them. For example, an increasing number of consumers are using sophisticated fitness trackers, capable of sensing bodily states with precision, with very little awareness of privacy risks of collection and processing of fine-grained data. It appears that privacy notices primarily serve as a means of avoiding legal action for data controllers, rather than fulfilling their intended purpose of informing consumers about their data practices.

The paradigm of notice and consent, widely known as ‘notice and choice’, is based on a presupposition that consumers will adequately manage their privacy, if provided sufficient information about data collection and processing [31]. In fact, the GDPR resulted in more detailed and longer privacy notices. It is our experience since GDPR came into effect, we routinely encounter long and detailed notices.

Research [18,24] has shown that comprehending privacy notices imposes a high cognitive and time burden on data subjects [15]. In order to address this widespread issue of uninformed consent, research efforts are needed to advance the state-of-the-art in automatic processing of privacy notices (to extract relevant information) and use the extracted information to present the notices more intuitively to consumers so that these notices are more likely to be read and understood.

2 Background

Mark Weiser introduced the term ubiquitous computing in 1991 as “The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it” [42]. Internet of Things (IoT) [4] is meant to support this ubiquitous computing wave. The term IoT was coined by the British technology pioneer Kevin Ashton [3], who described it as a system of physical objects embedded with sensors and software, which are connected to the Internet. IoT devices are now ubiquitous in the very spaces (personal or public) the consumers move through, e.g., cars, wearables, healthcare devices, and electric systems. These connected devices create new types of unprecedented quantities of massive and nuanced datasets about consumer behavior [28]. All this information undoubtedly enhances productivity and quality of life. For example, a Fitbit activity tracker [38] allows consumers to track their daily physical activity, including the number of steps, amount of sleep, calories burned, heart rate, etc. Muse headband [22] can measure brain activity, brain health and performance, in real world environments to track the user’s ability to focus. Information from these connected devices can in combination measure consumers’ driving habits, behavioral patterns, and/or work productivity [28]. All these devices such as activity trackers, headbands, home sensors, baby monitors, and so on, continually generate personal data about the consumer. The GDPR is a intricate regulation that primarily focuses on data privacy, and regulates collection and processing of the personal data about EU citizens. Subsequently, we provide a foundational understanding of privacy

and data protection, and then give a concise overview of the privacy principles outlined in the GDPR.

2.1 Privacy and data protection

Privacy is considered a fundamental human right [13], giving the right to a private life and associated freedoms to its citizens. The significance of privacy is reflected by the fact that the documents that define human rights, such as the Universal Declaration of Human Rights (UDHR, Article 12), the European Convention on Human Rights (UCHR, Article 8), incorporate references to privacy and related concepts. Interpreted broadly, privacy has a rich history in law and philosophy, and many definitions attempt to define privacy considering one or more distinct perspectives on privacy [7]. There are several interpretations of privacy, encompassing different perspectives such as privacy of person, privacy of personal communication, informational privacy, privacy of association etc. In [36], Sieghart describes privacy in terms of ensuring that “the right data are used by the right people for the right purposes”. The *right data* requires the information to be accurate, complete, relevant and timely. The *right purpose* requires that the purposes are explicitly or implicitly agreed to by the data subject or are permitted by the law. The *right people* are the entities that will use the data for only the right purposes. Absence of these conditions may jeopardize critical rights, interests, and services [36]. To a great extent, this definition of privacy is still valid in current times, at least in the context of the GDPR.

The privacy literature introduced a term, namely *data protection*. Data protection can be defined as the law designed to protect personal data, and is recognized as a fundamental aspect of the right to privacy [30]. Data protection has been included as a standalone right under the Charter of Fundamental Rights [30] of the European Union (2012/C 326/02) under Article 8 [13], with emphasis on concepts such as lawfulness, fairness, and transparency, which are in line with GDPR’s privacy principles. Note that the literature uses the terms individual/user/consumer/data subject interchangeably. In order to understand the privacy principles, it is necessary to be familiar with the following GDPR specific terminology:

- *Personal data*: the concept of personal data is central to data protection and its definition in the GDPR is kept intentionally broad. Article 4(1) of the GDPR defines personal data as “any information relating to an identified or identifiable natural person” [14]. Example of personal data include date of birth, gender, marital status, citizenship, association with organizations, address, phone number, and identity verification information. This also includes information such as dynamic IP addresses and cookies, as this information can be used to track online activities and generate a user profile which can be linked to devices and in most cases, an individual [40].
- *Data subject*: it is defined parenthetically within the definition of personal data, as an identified or identifiable natural person as being a data subject. In particular, the data subject is the individual about whom or from whom the information is being collected and processed.

- *Data controller and processor*: a data controller is a natural person, organization, public authority, or agency, which collects information about data subjects, determines the purposes of processing personal information, and processes the information (including its storage, disclosure). A data processor is a natural person, organization, public authority, or agency, that processes personal data on behalf of the data controller, which essentially means that a data processor is simply a service provider for a data processor [40]. The data controllers are the ones that exercise the decisions about collection, disclosure, processing, retention and destruction of personal data. As a result, a data controller is responsible for most of the compliance requirements (Article 5(1)). Through Article 24 and Article 25 of the GDPR, the requirements of integrating necessary safeguards into processing of personal information are imposed on the data controller.

2.2 Privacy principles (GDPR)

The privacy profession offers established principles to guide information technology professionals in different stages of system engineering, for better and privacy-aware systems. The GDPR's processing principles [14] are set out in Article 5(1) and required to be followed by entities responsible for processing personal data. Data controllers are prescribed with the duty to demonstrate compliance (in Article 5(2)) with the privacy principles. The following points describe these principles.

1. *Lawfulness, fairness and transparency*: under the regulation, personal data shall be processed lawfully, fairly, and in a transparent manner. Fairness of the processing is linked to the idea that individuals must be aware of the fact that their personal data will be processed, including how the data will be collected, kept and used, to allow them to make an informed decision about whether they agree with such processing and enable them to exercise their data protection rights. Transparency is directly linked to fairness, and it means that the data controller must be open and clear towards data subjects when processing personal data. In summary, this principle requires honest usage and communication with the data subject about their personal data.
2. *Purpose limitation*: purpose limitation restricts the collection and processing of personal data for specific, explicit and legitimate purposes only, and requires that the data is not processed beyond such purposes. Secondary use of data, i.e., processing which does not fall within the boundaries of the purpose for which the personal data was collected, will be considered as incompatible and a separate legal ground will be required (such as consent) for processing secondary purposes. To determine if the personal data could be used for secondary purposes, the GDPR provides guidelines to assess the compatibility of the secondary purpose with the original purpose.
3. *Data minimization*: data minimization means that the data controllers must only collect and process personal data that is relevant, necessary, and adequate to accomplish the purposes for which it is processed. In other words, it

means the data controllers should collect only the personal data they really need. If a goal can be reached using anonymous data or methods that are less intrusive to privacy, those methods should be used instead of a strategy that involves collection and processing of all personal information without discrimination.

4. *Accuracy*: accuracy means that the data controllers must take reasonable measures to prevent inaccuracies and ensure that the data is accurate and up to date. It also includes taking necessary measures to respond to data subjects' request to correct inaccurate or incomplete information. For example, in a healthcare setting, the organization must ensure that the personal data it holds about each patient is accurate and up-to-date. This could include verifying the accuracy of the patient's name, address, medical history, and other relevant information. If the organization becomes aware that any of this information is incorrect, it must take steps to correct it as soon as possible.
5. *Storage limitation*: storage limitation means that personal data must not be kept for longer than necessary for the purposes for which it was collected for. Once the personal data is no longer needed, it must be securely deleted. However, there is a provision for data controllers to keep the personal data for unlimited period only when the data is irreversibly anonymized. In addition, data can be stored for longer periods for archiving purposes in public interest.
6. *Confidentiality and integrity*: confidentiality and integrity means that the controllers must take appropriate security measures to protect the data against unauthorized and unlawful processing, accidental loss, and so on. The regulation prompts the use of techniques such as pseudonymization and encryption, implementing information security framework, in order to protect the personal data throughout its lifecycle.
7. *Accountability*: the GDPR strengthens the six privacy principles by explicitly adding the accountability requirement (in Article 5(2)). It means that the data controller is responsible for complying with the aforementioned six principles, and they must be able to evidence their compliance. The principles are broadly interpreted, but their violators may incur large administrative fines (e.g., a financial penalty of 50 Million Euros against Google LLC [10]).

3 Notice and Consent

The *notice and consent* is a widely used regulatory approach for protecting privacy rights. It also encourages innovation and it appeals to individual choice [39]. It requires that individuals be informed and give their approval (informed consent) before any data regarding them is collected and processed. The aim of the notice and consent paradigm is to give individuals control over their personal information and to ensure that they are aware of how it will be used. In [44], OECD concludes that “consumer engagement – namely checking privacy policies and establishing one’s own privacy preferences – are crucial elements without which privacy-enhancing technologies are largely ineffective”.

3.1 Privacy policy and privacy notice

In general, there are two types of documents that communicate privacy practices: a privacy policy and a privacy notice. A *privacy policy* is an internal document addressed to employees accessing personal information, clearly stating how the personal information will be collected, stored and disclosed to meet the organizational/regulatory privacy needs. A *privacy notice* is an external document and a transparent notification that is addressed to consumers that describes how their personal information is being handled, including information on the legal basis of processing and specific legitimate interests pursued by the data controller. In particular, a privacy notice is a legally mandated document for the collection and processing of personal data. As per GDPR, the privacy policy must be formulated by taking into account the privacy principles. The privacy notices should be consistent with the privacy policies. A data controller is required to provide relevant data practices, such as basis of processing, purpose of processing, legitimate interests etc., in the privacy notice. In summary, aligning a controller's internal privacy policy with its external privacy notice is important to ensure that the controller is meeting its obligations under privacy regulations, and consumer data is being used in a responsible manner. However, it is debatable whether consumers really benefit from lengthy and technical privacy notices loaded with legal jargon. Some argue that notices are insufficient instruments for providing individual users with a deep enough understanding of the data practices [24,39].

3.2 Consent

Consent is frequently an essential instrument in data protection and privacy laws, which puts individuals in control of their personal data. GDPR strengthens 'consent' in relation to use of personal data as compared with the the 1995 Data Protection Directive. It is mentioned in the earlier section that the GDPR requires the data controllers to process personal data in a *lawful, fair and transparent* manner, meaning that there must be honest usage and communication with the data subject about their personal data. The three components here are linked with one another, and requires that the controllers are open and clear towards data subjects. The requirement of lawfulness means that personal data can only be processed if there is a legal basis for doing so. Article 6 of the GDPR outlines the legal bases of processing processing personal data:

1. *Consent*: the data subject has given consent to the processing of his or her personal data for one or more specific purposes. Consent requires a very clear and specific statement of consent. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.
2. *Contract necessity*: it is a commonly used option and it is applicable when processing is necessary for the performance of a contract to which the data

subject is party or in order to take steps at the request of the data subject prior to entering into a contract. For example, processing the address of the individual to deliver the products when a data subject makes online purchases.

3. *Legal obligation*: it is applicable when processing is necessary for compliance with a legal obligation to which the controller is subject. For example, disclosure of personal data to public authorities for the exercise of their official mission, such as tax and customs authorities, financial investigation units etc.
4. *Individual's vital interest*: it is applicable when processing is necessary in order to protect the vital interests of the data subject or of another natural person. It is applicable in scenarios such as, emergency medical care, monitoring epidemics etc.
5. *Public interest*: it is applicable when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. For example, processing data for archiving purposes in the public interest, historical research or statistical purposes, etc.
6. *Legitimate interest*: it is applicable when processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. In this case, processing is not required by law or for contract performance, but processing is of clear benefit to data subjects, for example, in fraud detection or for information security.

Legal bases such as performance of contract and legitimate interest often do not offer consumers with the same level of choice and control over their data, as offered by consent. For example, in the case of performance of contract, the processing of personal data is necessary in order to perform the contract, i.e., provide the necessary service or product. In the case legitimate interest, the data controller must balance their own interests in processing the personal data against the interests of the consumer. If the data controller's interests are deemed to outweigh consumer's interests, they may still process the personal data, as long as there is a clear justification for the impact on the consumer. Similarly, consumers do not have much choice and control over processing based on legal obligation, vital interest and public interest. Processing personal data under these legal bases is either required by law or necessary to protect the vital and public interests of the individual. Therefore, consent is the most suitable legal basis for processing personal data when the goal is to offer consumers choice and control over their data.

3.3 Discussion: Notice and Consent

While browsing the Internet, installing an app on our phone, or setting up a new IoT device, individuals are often asked to consent to privacy notices. This is

intended to provide individuals with a clear understanding of how their personal data will be used and enable them to make informed decisions. The paradigm of *notice and consent* is grounded on the assumption that consumers will take appropriate measures to safeguard their privacy if they receive adequate information about data collection and processing [31].

Such explicit notifications are necessary towards achieving the ideal scenario (Figure 1), where the individual recognize-read-understand the privacy notice, and once understood, gives informed consent. Actually, the GDPR led to the creation of lengthier and more detailed notices that contain a great deal of technical and legal terminology. Individuals do recognize the privacy notice, but due to longer, layered and complicated text it is hard to read and understand. Contrary to expectation, most people reflexively choose “I consent” or “I agree” [18]. They agree to unfair-deceptive practices with uninformed consent. Choosing “I consent” or “I agree” without reading and understanding the notices becomes increasingly problematic when it is about electronic devices used in everyday life in personal spaces, such as a fitness tracker constantly sensing our bodies, a voice assistant listening in. These devices collect a significant amount of data, including personal and sensitive data, and organizations use this data to understand user behavior and preferences. These insights are then used in marketing, (micro)targeted advertising, and creation of new products and services. However, some argue that the notice-and-consent may be exploited by commercial entities to extract more personal data from consumers than necessary, and that consumers may not fully understand what they are consenting to [18,26,39].

As computing becomes ubiquitous, the continued reliance on consumers to read several dozen such privacy notices and make informed decision is a practical problem. Comprehending privacy notices imposes a high cognitive and time burden on users [20]. Surveillance capitalism is the business model of the Internet [35] and Internet of Things. Surveillance capitalism’s core idea is that the data generated by the users of digital platforms is a valuable asset that can be extracted, analyzed, and traded with third parties in the data market. This business model has given rise to a variety of malpractices. For example, “dark patterns” to manipulate users into agreeing to intrusive terms and conditions, and “notification overload” to create confusion and ultimately undermine informed consent. Combined effect of surveillance capitalism and connected malpractices is that privacy notices fails its very purpose of protecting privacy. This leads to provocation of *paradoxical behavior* [5], i.e., despite being very concerned about their privacy, consumers do not take necessary actions to protect their personal data, and *privacy resignation* [16], i.e., data subjects give up managing their privacy settings. Acquisti et al. [1], in their analysis of surveys, field studies and experiments in privacy literature conclude that privacy management that rely purely on consumer responsabilization have failed.

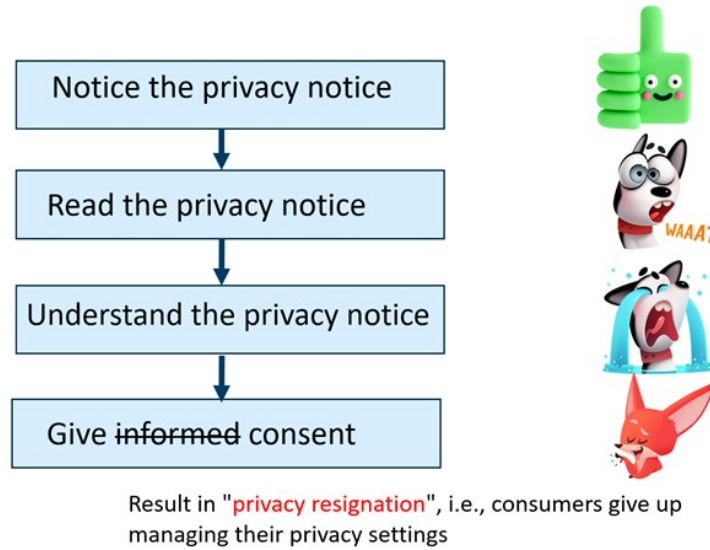


Fig. 1. GDPR's consent: expectation vs reality

4 Privacy-assistive technology

The notice-and-choice paradigm has been criticized in scientific literature [32,37,39], seeking to move beyond the current consent model. The World Economic Forum (WEF) has published a white paper [18] that discusses the current state of the notice and consent paradigm, and the paper concludes that the existing mechanisms for notice and consent fail to account for the complex nature of human psychology. "Existing approaches do not scale for either traditional digital user interfaces or the emergent world of screenless internet of things (IoT) devices, smart cities or other connected environments" [18]. In another white paper [6], the WEF highlights the need to empower individuals, and thoughtful consent mechanisms to strengthen trust and maximize data sharing for common good. Clearly, there is a need to reconceptualize notice and consent mechanism, that shifts the burden of protecting privacy to business entities processing personal data, rather than placing it squarely on consumers.

One way to solve the challenges outlined in Section 3 is by utilizing privacy-assistive technology. In this context, privacy-assistive technology (PAT) means software-based solutions that could assist consumers in comprehending privacy notices, making meaningful privacy decisions, and managing their privacy settings. PAT includes tools such as interactive interfaces, visualizations, and summary explanations that aim to enhance the accessibility comprehension of notices. In this section, we present existing research in the field of privacy assistive technologies for IoT.

Morel et al. [25] provide a Personal Data Custodian, an edge-based tool that informs data subjects about privacy notices specified in a policy language

endowed with formal semantics. Data practices (e.g., purpose, retention period, opt-out choice) are manually extracted from notices in this tool. Next in line are the research works which involves automation to process privacy notices. Amos et al. [2], analyzing the trend in privacy notices over the last 20 years, conclude that privacy notices show a disturbing lack of transparency: using third parties and tracking technologies is severely underreported. Sathyendra et al. [33] use a privacy corpus [43] to train models to automatically detect the provision of ‘opt-out choice’ in notices. Harkous et al. [21] provide a deep learning-based notice analysis tool, Polisis, which can automatically identify 122 data practices. Zhang et al. [45] developed a predictive model using clustering techniques to assist users in consenting to allow or deny personal data processing in video analytics deployments.

According to Lipman [23], “Consumers have the power to change the way companies handle their data. They just need to know about it first”. Awareness is the key to autonomy. When consumers have more awareness of ongoing data collection and data practices then they would prefer to exercise control (as is evident from findings in [11,19]). Now we briefly present the research works which enhances consumer’s privacy awareness and control. Wang et al. [41] present a privacy-aware IoT architecture comprising several components, including a software module privacy mediator. The mediator runs on an edge device and receives user privacy preferences through a smartphone app, i.e., IoT Assistant (IoTA). It applies the privacy preferences to a real-time video before the video is stored or made available for analytics. IoTA communicates the available notices and choices of registered IoT devices to users. Feng et al. [16] propose a design space for privacy choices based on a user-centered analysis of what makes privacy notices effective.

A newer version of the IoTA app leverages this design space to implement meaningful privacy choices. Fernandez et al. [17] provide a novel augmented reality privacy management interface, i.e., Privacy Augmented Reality Assistant (PARA), for smart home devices. When a smartphone points to a smart IoT device, the PARA interface shows the data collected and allows users to switch on or off data collection, offering real-time privacy control. The evaluation results show that PARA users become more aware of IoT devices and their disclosed data, improving their privacy perception and control. IoTA and PARA offer simple interfaces enhancing the user awareness of deployed IoT systems and their data practices, but they do not directly work with privacy notices. IoTA requires IoTA owners to register privacy settings in a predefined template, and PARA uses hypothetical privacy settings. Habib et al. [20] leverage icons and their descriptions to effectively communicate privacy choices to consumers. Their assessment reveals that it is hard to communicate privacy choices without text.

As digital technologies evolve, various privacy-assistive technologies will be developed. Based on an analysis of existing privacy-assistive solutions in IoT domain, it can be inferred that the solutions will more likely be based on (i) sophisticated machine learning based automatic processing of privacy notices, to automatically extract precise and nuanced information, and (ii) present the ex-

tracted information intuitively in ways that enhance consumers’ privacy awareness, understandability, and control without overburdening them with notice comprehension and privacy configurations. In particular, the success of privacy-assistive technology depends on two crucial elements, i.e., consumer awareness and participation in establishing their own privacy preferences.

Further research is needed for rethinking and redesigning the notice and consent paradigm in a way that better empowers individual and provides a level of regulatory certainty to businesses so that they can invest in innovation. Existing research may be utilized (e.g., [2,12,16,20,25,31,33]) to advance the state-of-the-art. According to WEF’s white paper [18], the aim is to have technology serve people, rather than the reverse. Our assessment of existing research also converge to a similar note that privacy-assistive technology has potential to address the challenges of notice and consent paradigm, and enhance consumers’ privacy awareness and control over personal data collected and processed by IoT systems.

5 Conclusion

In this article we looked at the notice and consent paradigm, from two sides: the regulatory (GDPR) expectation and the reality. We briefly discussed regulatory text and its interpretation. The notice and choice paradigm has been a cornerstone of personal data processing for many years. It is clear the objectives of the Notice and Consent paradigm are worthy. Nonetheless, it is apparent that the implementation of this paradigm is obsolete and falls short in obtaining meaningful consent. Its execution needs to be reassessed to empower consumers, and balance the information asymmetry between organizations and consumers.

With the growth in awareness of privacy concerns, privacy assistive technology is emerging as a critical tool to assist individuals. We suggest that one way to solve the challenges is by developing software-based privacy-assistive technology, which could assist consumers in comprehending privacy notices, making meaningful privacy decisions, and managing their privacy settings. Designing effective privacy assistive technology is not without its challenges. It requires a deep understanding of various fields, such as privacy risks, multi-stakeholder exchange of personal data, consumers’ privacy sensitivity and their cost-benefit assessment, user-friendly interfaces, human-technology interaction. We presented state-of-the-art in the field of privacy assistive technologies for IoT.

Overall, the design and development of privacy assistive technology relies on a diverse range of technologies. According to our assessment of existing research, it is probable that the solutions will rely on (i) advanced machine learning algorithms to automatically analyze privacy notices and accurately extract detailed information, and (ii) presentation of the extracted information in an intuitive manner that enhances consumers’ privacy awareness, understanding, and control without overwhelming them with complex privacy notices or configurations.

Funding

This work has been carried out as part of the CyberSec4Europe project (830929) and CyberKit4SME project (883188) funded by the European Union’s Horizon 2020 Research and Innovation Programme, as well as the CINELDI project (257626/E20) funded by the Research Council of Norway.

References

1. Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 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, 2020.
2. Ryan Amos, Gunes Acar, Eli Lucherini, Mihir Kshirsagar, Arvind Narayanan, and Jonathan Mayer. Privacy policies over time: Curation and analysis of a million-document dataset. In *Proceedings of the Web Conference 2021*, pages 2165–2176, 2021.
3. Kevin Ashton. That ‘Internet of Things’ thing. *RFiD Journal*, 22(7), 2011.
4. Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer Networks*, 54(15):2787–2805, 2010.
5. Susanne Barth and Menno DT De Jong. The privacy paradox—investigating discrepancies between expressed privacy concerns and actual online behavior—a systematic literature review. *Telematics and informatics*, 34(7):1038–1058, 2017.
6. Kimberly Bella, Christophe Carugati, Cathy Mulligan, and Marta Piekarska-Geater. Data for common purpose:leveraging consent to build trust. <https://www.weforum.org/whitepapers/data-for-common-purpose-leveraging-consent-to-build-trust/>, 2021.
7. Travis Breaux, Stuart Shapiro, Lujo Bauer, Chris Clifton, Lorrie Cranor, Simson Garfinkel, David Gordon, David Marcos, Aaron Massey, Florian Schaub, Manya Sleeper, and Blase Ur. *An Introduction to privacy for technology professionals*. IAPP Publication, 2020.
8. Cisco. The iot value/trust paradox: Building trust and value in the data exchange between people, things and providers. <https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2017/m12/cisco-survey-reveals-divide-between-iot-value-and-trust.html>, 2017. Accessed: 2021-12-21.
9. Cisco. Consumer privacy survey: The growing imperative of getting data privacy right. https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/cybersecurity-series-2019-cps.pdf, 2019. Accessed: 2022-01-06.
10. CNIL. The CNIL’s restricted committee imposes a financial penalty of 50 million euros against google llc, 2019. <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>.
11. Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. Privacy expectations and preferences in an iot world. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pages 399–412, 2017.
12. Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. Which privacy and security attributes most impact consumers’ risk perception and willingness to purchase iot devices? In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 1937–1954, 2021.

13. EP and CEU. Charter of Fundamental Rights of the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN>, 2012. Accessed: 2020-04-29.
14. EP and CEU. The General Data Protection Regulation (GDPR). <https://eur-lex.europa.eu/eli/reg/2016/679/oj>, 2016. Accessed: 2019-11-24.
15. Benjamin Fabian, Tatiana Ermakova, and Tino Lentz. Large-scale readability analysis of privacy policies. In *Proceedings of the international conference on web intelligence*, pages 18–25, 2017.
16. Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. A design space for privacy choices: Towards meaningful privacy control in the internet of things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–16, 2021.
17. Carlos Bermejo Fernandez, Lik Hang Lee, Petteri Nurmi, and Pan Hui. Para: Privacy management and control in emerging iot ecosystems using augmented reality. In *ACM International Conference on Multimodal Interaction*. Association for Computing Machinery (ACM), 2021.
18. Anne J Flanagan, Jen King, and Sheila Warren. Redesigning data privacy: Reimagining notice consent for human-technology interaction. https://www3.weforum.org/docs/WEF_Reducing_Data_Privacy_Report_2020.pdf, 2020.
19. Miguel Godinho de Matos and Idris Adjerid. Consumer consent and firm targeting after gdpr: The case of a large telecom provider. *Management Science*, 2021.
20. Hana Habib, Yixin Zou, Yaxing Yao, Alessandro Acquisti, Lorrie Cranor, Joel Reidenberg, Norman Sadeh, and Florian Schaub. 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*, pages 1–25, 2021.
21. Hamza Harkous, Kassem Fawaz, Rémi Lebret, Florian Schaub, Kang G Shin, and Karl Aberer. Polisis: Automated analysis and presentation of privacy policies using deep learning. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 531–548, 2018.
22. Olave E Krigolson, Mathew R Hammerstrom, Wande Abimbola, Robert Trska, Bruce W Wright, Kent G Hecker, and Gordon Binsted. Using muse: Rapid mobile assessment of brain performance. *Frontiers in Neuroscience*, 15, 2021.
23. Rebecca Lipman. Online privacy and the invisible market for our data. *Penn St. L. Rev.*, 120:777, 2015.
24. Alecia M McDonald and Lorrie Faith Cranor. The cost of reading privacy policies. *Isjlp*, 4:543, 2008.
25. Victor Morel, Mathieu Cunche, and Daniel Le Métayer. A generic information and consent framework for the iot. In *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (Trust-Com/BigDataSE)*, pages 366–373. IEEE, 2019.
26. Norwegian Consumer Council. Surveillance-based advertising: Consumer attitudes to surveillance-based advertising. <https://fil.forbrukerradet.no/wp-content/uploads/2021/06/consumer-attitudes-to-surveillance-based-advertising.pdf>, 2021. Accessed: 2021-12-21.
27. C. O’Brian. How nationbuilder’s platform steered macron’s en marche, trump, and brexit campaigns to victory, 2017. <https://venturebeat.com/business/how-nationbuilder-helped-emmanuel-macron-secure-a-landslide-in-frances-legislative-elections/> .

28. Scott R Peppet. Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent. *Tex. L. Rev.*, 93:85, 2014.
29. Privacy International. Grounds for processing of personal data. https://privacyinternational.org/sites/default/files/2018-09/Part%205%20-%20Grounds%20for%20Processing%20of%20Personal%20Data_0.pdf, 2018. Accessed: 2022-03-17.
30. Privacy International. A guide for policy engagement on data protection : Part 1 Data protection, explained. <https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf>, 2018. Accessed: 2021-12-22.
31. Abhilasha Ravichander, Alan W Black, Thomas Norton, Shomir Wilson, and Norman Sadeh. Breaking down walls of text: How can nlp benefit consumer privacy? In *Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing (Volume 1: Long Papers)*, pages 4125–4140, 2021.
32. Neil Richards and Woodrow Hartzog. The pathologies of digital consent. *Washington University Law Review*, 96:1461, 2018.
33. Kanthashree Mysore Sathyendra, Shomir Wilson, Florian Schaub, Sebastian Zimmeck, and Norman Sadeh. Identifying the provision of choices in privacy policy text. In *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing*, pages 2774–2779, 2017.
34. Bruce Schneier. *Data and Goliath: The hidden battles to collect your data and control your world*. WW Norton & Company, 2015.
35. Bruce Schneier. New Data Privacy Regulations. https://www.schneier.com/blog/archives/2018/06/new_data_privac.html, 2018. Accessed: 2022-12-18.
36. Paul Sieghart. Privacy and computers. 1976.
37. Daniel J. Solove. Murky consent: An approach to the fictions of consent in privacy law. *Social Science Research Network (SSRN)*, 2023.
38. Ruth Gaelle St Fleur, Sara Mijares St George, Rafael Leite, Marissa Kobayashi, Yaray Agosto, and Danielle E Jake-Schoffman. Use of fitbit devices in physical activity intervention studies across the life course: Narrative review. *JMIR mHealth and uHealth*, 9(5):e23411, 2021.
39. Daniel Susser. Notice after notice-and-consent: Why privacy disclosures are valuable even if consent frameworks aren't. *Journal of Information Policy*, 9:148–173, 2019.
40. Eduardo Ustaran. *European Data Protection: Law and Practice*. an IAPP Publication, International Association of Privacy Professionals, 2018.
41. Junjue Wang, Brandon Amos, Anupam Das, Padmanabhan Pillai, Norman Sadeh, and Mahadev Satyanarayanan. A scalable and privacy-aware iot service for live video analytics. In *Proceedings of the 8th ACM on Multimedia Systems Conference*, pages 38–49, 2017.
42. Mark Weiser. The computer for the 21st century. *Scientific American*, 265(3):94–104, 1991.
43. Shomir Wilson, Florian Schaub, Aswarth Abhilash Dara, Frederick Liu, Sushain Cherivirala, Pedro Giovanni Leon, Mads Schaarup Andersen, Sebastian Zimmeck, Kanthashree Mysore Sathyendra, N Cameron Russell, et al. The creation and analysis of a website privacy policy corpus. In *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 1330–1340, 2016.

44. Working Party on Information Security and Privacy. Inventory of privacy-enhancing technologies (pets). <https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?doclanguage=en&cote=dsti/iccp/reg%282001%291/final>, 2002.
45. Shikun Zhang, Yuanyuan Feng, Anupam Das, Lujio Bauer, Lorrie Faith Cranor, and Norman Sadeh. Understanding people's privacy attitudes towards video analytics technologies. *Proceedings of the FTC PrivacyCon*, pages 1–18, 2020.
46. Shoshana Zuboff. *The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019*. Profile books, 2019.