A Design Space for Effective Privacy Notices

Florian Schaub, Rebecca Balebako, Adam L. Durity, Lorrie Faith Cranor

June 2015
CMU-ISR-15-105

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

To appear in the Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015) published by the USENIX Association.

Abstract

Notifying users about a system's data practices is supposed to enable users to make informed privacy decisions. Yet, current notice and choice mechanisms, such as privacy policies, are often ineffective because they are neither usable nor useful, and are therefore ignored by users. Constrained interfaces on mobile devices, wearables, and smart home devices connected in an Internet of Things exacerbate the issue. Much research has studied usability issues of privacy notices and many proposals for more usable privacy notices exist. Yet, there is little guidance for designers and developers on the design aspects that can impact the effectiveness of privacy notices. In this paper, we make multiple contributions to remedy this issue. We survey the existing literature on privacy notices and identify challenges, requirements, and best practices for privacy notice design. Further, we map out the design space for privacy notices by identifying relevant dimensions. This provides a taxonomy and consistent terminology of notice approaches to foster understanding and reasoning about notice options available in the context of specific systems. Our systemization of knowledge and the developed design space can help designers, developers, and researchers identify notice and choice requirements and develop a comprehensive notice concept for their system that addresses the needs of different audiences and considers the system's limitations and opportunities for providing notice.

This research was partially funded by NSF grants CNS-1012763 (Nudging Users Towards Privacy), CNS-1330596 (Towards Effective Web Privacy Notice & Choice: A Multi-Disciplinary Perspective), and DGE-0903659 (IGERT: Usable Privacy and Security), as well as by Facebook.

Keywords: Privacy, Notice & Choice, Privacy Notices, Interface Design, Design Space, Usability.

A Design Space for Effective Privacy Notices

Florian Schaub,[1] Rebecca Balebako,[2*] Adam L. Durity,[3*] Lorrie Faith Cranor[1]

[1]Carnegie Mellon University
Pittsburgh, PA, USA
{fschaub, lorrie}@cmu.edu

[2]RAND Corporation
Pittsburgh, PA, USA
balebako@rand.org

[3]Google
Mountain View, CA, USA
adurity@google.com

ABSTRACT

Notifying users about a system's data practices is supposed to enable users to make informed privacy decisions. Yet, current notice and choice mechanisms, such as privacy policies, are often ineffective because they are neither usable nor useful, and are therefore ignored by users. Constrained interfaces on mobile devices, wearables, and smart home devices connected in an Internet of Things exacerbate the issue. Much research has studied usability issues of privacy notices and many proposals for more usable privacy notices exist. Yet, there is little guidance for designers and developers on the design aspects that can impact the effectiveness of privacy notices. In this paper, we make multiple contributions to remedy this issue. We survey the existing literature on privacy notices and identify challenges, requirements, and best practices for privacy notice design. Further, we map out the design space for privacy notices by identifying relevant dimensions. This provides a taxonomy and consistent terminology of notice approaches to foster understanding and reasoning about notice options available in the context of specific systems. Our systemization of knowledge and the developed design space can help designers, developers, and researchers identify notice and choice requirements and develop a comprehensive notice concept for their system that addresses the needs of different audiences and considers the system's limitations and opportunities for providing notice.

1. INTRODUCTION

The purpose of a privacy notice is to make a system's users or a company's customers aware of data practices involving personal information. Internal practices with regard to the collection, processing, retention, and sharing of personal information should be transparent to users. The privacy notice acts as a public announcement of those practices. Privacy notices can take different shapes and leverage different channels, ranging from a privacy policy document posted on a website, or linked to from mobile app stores or mobile apps, to signs posted in public places to inform about CCTV cameras in operation. Even an LED indicating that a camera or microphone is active and recording constitutes a privacy notice, albeit one with limited information about the data practices associated with the recording. Providing notice about data practices is an essential aspect of data protection frameworks and regulation around the world [57]. While transparency has been emphasized as an important practice for decades, existing privacy notices often fail to help users make informed choices. They can be lengthy or overly complex, discouraging users from reading them.

Smartphones and mobile apps introduce additional privacy issues as they support recording of sensor and behavioral information that enables inference of behavior patterns and profiling of users. Yet, comparatively smaller screens and other device restrictions constrain how users can be given notice about and control over data practices.

The increasing adoption of wearable devices, such as smart watches or fitness trackers, as well as smart home devices, such as smart thermostats, connected light bulbs, or smart meters, represents a trend towards smaller devices that are even more constrained in terms of interaction capabilities, but are also highly connected with each other and the cloud. While providing notice and choice is still considered essential in the "Internet of Things" (IoT) [48, 74], finding appropriate and usable notice and choice mechanisms can be challenging.

The challenges of providing usable privacy notice have been recognized by regulators and researchers. For instance, FTC chairwoman Edith Ramirez [107] stated in the IoT context: "In my mind, the question is not whether consumers should be given a say over unexpected uses of their data; rather, the question is how to provide simplified notice and choice." An extensive body of research has studied usability issues of privacy notices (e.g., [14, 33, 64, 51]) and proposed improved notice interfaces (e.g., [34, 66, 67]), as well as technical means to support them (e.g., [75, 127, 131]). Multi-stakeholder processes have been initiated in the wake of the White House's proposed Consumer Bill of Rights [122] to tackle transparency and control issues of mobile privacy [92] and facial recognition [93]. While such efforts have resulted in guidance for notices in the context of particular systems, they have given little consideration to usability [14].

Existing frameworks and processes for building privacy-friendly systems, such as Privacy by Design [36] or privacy impact assessments [136], focus on the analysis of a system's data practices and less so on the design of notices. Even the OECD report on "making privacy notices simple" [94] basi-

*Rebecca Balebako and Adam Durity performed this work while at Carnegie Mellon University.

Symposium on Usable Privacy and Security (SOUPS) 2015, July 22–24, 2015, Ottawa, Canada.

cally states that one should design a simplified notice, conduct usability tests, and deploy it – the crucial point of *how* to design a simplified notice is not addressed. Common proposals to improve the usability of privacy notices are the use of multi-layered notices [9, 26] or just-in-time notices [47].

Despite the previous work on privacy notices, transparency tools, and privacy mechanisms, a system designer or developer has very little guidance on how to arrive at a privacy notice design suitable and appropriate for their specific system and its respective characteristics. Existing best practices are spread throughout the literature and have not previously been organized into a comprehensive design framework. As a result, privacy notices are often hastily bolted on rather than well-integrated into a system's interaction design. Designers may not be aware of the many alternatives for designing usable privacy notices and therefore do not systematically consider the options. Furthermore, designers and researchers do not yet have a standard vocabulary for describing privacy notice options.

In this paper, we make multiple contributions to ease the design of privacy notices and their integration into a system. The goal is to help developers embed privacy notices and choice options into their system design where relevant, with minimal disruption to the system's interaction flow. First, we identify challenges, requirements, and best practices for the design of privacy notices. Based on a survey of existing literature and privacy notice examples, we develop a design space of privacy notices. This design space and its dimensions provide a systemization of knowledge and a taxonomy to foster understanding and reasoning about opportunities for privacy notices and controls. We demonstrate the utility of our design space by discussing existing privacy notice approaches in different domains.

2. BACKGROUND

The concept of privacy notices is founded on the idea that users of services and systems that collect or process personal information should be informed about what information is collected about them and for which purposes, with whom it is shared, how long it is stored, and their options for controlling or preventing certain data practices [45, 95]. Given such transparency, users should be able to make informed privacy and consent decisions.

2.1 Roles of Privacy Notices

Privacy notices serve different roles depending on a stakeholder's perspective. Consumers, companies, and regulators see privacy notices in different ways.

For *companies*, privacy notices serve multiple purposes, including demonstrating legal compliance and building customer trust. Privacy notices are often primarily a necessity to ensure compliance with legal and regulatory requirements, rather than a tool to create transparency for users. For instance, the European Data Protection directives have strict notice requirements [41, 43]. In the U.S., not providing notice could be interpreted as a deceptive trade practice by the FTC [45] or violate federal, state, or sector-specific privacy legislation, such as CalOPPA [96] or HIPAA [27].

Yet, there are also intrinsic reasons why businesses and system designers should aim to provide privacy notices that are meaningful to users. Being upfront about data practices – especially about those that may be unexpected or could be misinterpreted – provides the opportunity to explain their purpose and intentions in order to gain user acceptance and avoid backlash. Furthermore, companies that provide privacy-friendly and secure systems can leverage privacy notices to make users aware of privacy-friendly data practices. Implementing and highlighting good security and privacy practices can further create a competitive advantage as users may perceive the system as more trustworthy.

Regulators, such as data protection authorities or the FTC, rely on companies' privacy notices – primarily their privacy policies – as an important tool to investigate and enforce regulatory compliance [31]. If a company violates its privacy policy, it provides regulators with a basis to take action; for example, the FTC may treat a violation as an unfair or deceptive trade practice [45, 116]. Further, data protection authorities in Europe and other countries may assess whether the described practices meet more stringent criteria, such as use limitation, proportionality of data practices, and user access options [41, 43].

2.2 Hurdles to Effective Privacy Notices

While privacy notices fulfill many roles for different stakeholders, in practice most privacy notices are ineffective at informing consumers [33, 83]. This ineffectiveness stems from hurdles that can be attributed not only to general shortcomings of the notice and choice concept [25, 33, 116], but also to the challenges in designing effective privacy notices.

Notice complexity. The different roles of privacy notices result in a conflation of requirements. Besides informing users about data practices and their choices, privacy notices serve to demonstrate compliance with (self-)regulation and limit the system provider's liability [23]. As a result, privacy notices often take the shape of long privacy policies or terms of service that are necessarily complex because the respective laws, regulations, and business practices are complex [25]. For instance, website privacy policies are typically long, complex documents laden with legal jargon. Indeed it has been estimated that to read the privacy policies for all the websites an American Internet user visits annually would take about 244 hours per year [83]. Privacy policies also read like contracts because regulators aim to enforce them like contracts [25]. Notices may further be purposefully vague to avoid limiting potential future uses of collected data [116]. The effect is that these notices are difficult for most people to understand [83, 111].

Lack of choices. Many privacy notices inform about data practices but do not offer real choices. Using a website, an app, a wearable device, or a smart home appliance is interpreted as consent to the data practices – regardless of the user having seen or read them. Even if notices are seen by users, they largely describe a system's data practices, with few choices to opt-out of certain practices, such as sharing data for marketing purposes. Thus, users are effectively left with a take-it-or-leave-it choice – give up your privacy or go elsewhere [116]. Users almost always grant consent if it is required to receive the service they want [25]. In the extreme case, privacy notices are turned into mere warnings that do not empower individuals to make informed choices [25] (e.g., "Warning: CCTV in use" signs). Yet, privacy notices can only be effective if they are actionable and offer meaningful choices [33]. Awareness of data practices can enable users to make informed privacy decisions, but privacy controls are needed in order to realize them [113].

Notice fatigue. Notice complexity and the lack of choices mean that most privacy notices are largely meaningless to consumers [25]. Users may feel it is pointless to read them, and most users don't. A recent White House report [106] stated, "Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent." Furthermore, businesses may change their data practices and notices at any time, which means any effort spent on understanding the notice may have been in vain [116]. Privacy notices and security warnings are often shown at inopportune times when they conflict with the user's primary task [63], therefore they are dismissed or accepted without scrutiny. Frequent exposure to seemingly irrelevant privacy notices results in habituation, i.e., notices are dismissed without even registering their content [6, 56]. Further, a notice's framing, distractions or time delays can reduce the notice's effectiveness [3].

Decoupled notices. Some systems decouple a privacy notice from the actual system or device, for example by providing it on a website or in a manual. Privacy notices are not only relevant for websites, mobile apps, or surveillance cameras, but for the whole gamut of systems and devices that process user information. Designing and providing appropriate notices for novel systems, such as smart home appliances or wearable devices, is challenging [48]. The straightforward approach is to decouple the privacy notice from the system. For example, many manufacturers of fitness tracking devices provide a privacy policy on their websites, while the actual device does not provide any privacy notices [103]. As a result, users are less likely to read the notice and may therefore be surprised when they realize that their mental models do not match the system's actual data practices [48].

These issues paint a somewhat dire picture of the state of privacy notices. However, just abandoning the concept of notice is not a viable option, as the transparency notices should provide is essential for users, businesses, and regulators alike [107]. We argue that many of these issues can be addressed by placing the emphasis on how privacy notices are designed. Instead of providing notice merely to fulfill legal and regulatory requirements, notices should effectively inform users about data practices and provide appropriate choices. Some proposed solutions point in that direction, such as multi-layered privacy notices [9], just-in-time notices [101], and notices focused on unexpected data practices [48, 107]. However, so far, there is little guidance on the actual design and integration of such notices into real-world systems. Next, we identify requirements and best practices for effective and usable privacy notice design.

3. REQUIREMENTS & BEST PRACTICES FOR PRIVACY NOTICE DESIGN

In order to make privacy notices effective and usable, they should not be tacked on after the system has been completed but instead be integrated into a system's design. Privacy notices and choice options can then be designed for specific audiences and their notice requirements, and take into account a system's opportunities and constraints.

In this section, we identify common requirements, necessary considerations, and best practices for privacy notice. These aspects are based on a survey of the usable privacy literature and an analysis of existing privacy design and assessment frameworks, such as Privacy by Design [36], privacy impact assessments [136], and proposals for layered notice design [9, 26, 94].

Together with the design space presented in the next section, the requirements and best practices discussed in this section provide guidelines and a toolbox for system designers and researchers that can aid them in the development of usable and more effective privacy notices for their systems.

3.1 Understand Privacy in the System

The first step in designing effective privacy notices is to understand a system's information flows and data practices in order to determine whether privacy notices are needed, who should be notified, and about what. Such an assessment can be conducted as part of a privacy impact assessment (PIA) [136], which further serves the purpose of identifying privacy risks associated with the system and making recommendations for privacy-friendly systems design. PIAs are becoming an essential – in some countries mandatory – aspect of systems design [134]. They serve the broader goal of ensuring a system's legal and regulatory compliance, as well as informing privacy by design and risk mitigation. A common approach in existing PIA frameworks [135, 136] is to first assess if the system collects or processes privacy-sensitive information to determine if a full PIA is required. The next step is to describe the system in detail, including its information flows and stakeholders. This description is the basis for analyzing the system's privacy implications and risks [36, 37]. A PIA produces a report detailing identified issues and recommendations on how to address them.

The resulting recommendations for privacy improvements may include changing collection practice, or identifying opportunities for data minimization. Data minimization reduces the risk of using data in ways that deviate from users' expectations as well as liability risks associated with data theft and unintended disclosure [48]. As an additional benefit, it also reduces the complexity of data practices that need to be communicated to users in privacy notices. If done early in a system's design process, this may also be an opportunity to consider and improve system constraints related to privacy. For example, recognizing that a video camera is collecting information, the device designers may decide to include a light or other signal indicating when the camera is on. The PIA report and data practices should be updated to reflect any privacy-friendly improvements. This process may involve multiple iterations.

Conducting a PIA informs notice design by helping to determine if notices are necessary in the first place, providing an overview of data practices for which notice should be given, potentially reducing the complexity of data practices, and determining the audiences that need to be considered in notice design. The outcome of a PIA is a deep understanding of a system's privacy characteristics, which can be codified in a comprehensive privacy policy.

A privacy policy describes a system's data practices including all relevant parameters, namely what data is being collected about users (and why), how this information is being used (and why), whether it is shared with third parties and for what purposes, how long information is retained, as well as available choice and access mechanisms [45]. This full privacy policy serves as the definitive (and legally binding) privacy notice. As such, it may be a long and complex document, which primarily serves the company to demonstrate transparency and regulatory compliance. It is there-

fore mainly relevant for businesses and regulators and less interesting or useful to users. However, a well-defined privacy policy can serve as the basis for designing concise, user-friendly privacy notices as it maps out the different data practices about which users may need to be informed.

3.2 Different Notices for Different Audiences

Privacy impact assessments and the creation of privacy policies are well-known and established concepts, but notice design often stops with the privacy policy. Whereas the full privacy policy may be sufficient for businesses and regulators, the key challenge is to design effective privacy notices for users. Therefore, one needs to understand which audiences have to be addressed by notices [23]. While determining a website's audience may be straightforward (typically the visitors of the website), mobile applications, wearables, smart cars, or smart home appliances expand the audiences and user groups that need to be considered. Such systems may have a primary user, but potentially also multiple users with different privacy preferences. For example, a home lock automation system may collect information about all family or household members, including guests [123]. Wearables, such as Google Glass, may incidentally collect information about bystanders. Social media and mobile applications enable users to share information with and about others, e.g., by tagging someone in a geo-referenced photo.

To determine the different audiences for privacy notices, the set of all data practices specified in the privacy policy needs to be analyzed to determine which data practices affect which audience. Typical audience groups are the *primary user* of a system; *secondary users*, such as household members, having potentially less control over the system; and *incidental users*, such as bystanders, who may not even be aware that information about them is collected by a system. Depending on the system, other or additional audience groups may need to be considered. There may also be regulatory requirements applying to specific audience groups, such as children [85], that have to be considered.

While some audience groups may be affected by the same data practices (e.g., data collection about the primary user and other household members by a smart home system), other groups may only be affected by very specific data practices (e.g., while all of a wearable's data practices affect the primary user, bystanders are only effected if they're incidentally recorded by the device, for instance, when the primary user takes a photo or video with a wearable device).

3.3 Relevant and Actionable Information

To be effective and draw the user's attention, privacy notices must contain relevant information. For each audience, one should identify those data practices that are likely unexpected for this audience in the prevalent transaction or context. Those practices are relevant because they cross contextual boundaries [82] and thus violate contextual integrity [15, 91]. Providing notice and choice for such practices should be prioritized. The FTC notes with respect to the IoT that not every data collection requires choice, but that users should have control over unexpected data practices, such as data sharing with third parties [48]. FTC chairwoman Ramirez explains this rationale as follows [107]: "Consumers know, for instance, that a smart thermostat is gathering information about their heating habits, and that a fitness band is collecting data about their physical activity. But would they expect this information to be shared with data brokers or marketing firms? Probably not." In these cases, users need clear privacy notices.

If possible, one should not only rely on estimations of what may be expected or unexpected. User surveys and experiments can reveal actual privacy expectations. Creating personas [90] that represent different members of a specific audience group can help ensure that less obvious concerns are appropriately considered.

For each data practice, all parameters relevant for creating a notice should be gathered. For instance, for a data collection practice this may include by whom information is collected, why, how it is used, for how long it is retained, and if and how it is eventually deleted. For third-party sharing practices, it is relevant with whom information is shared, why, and whether and how usage is restricted or limited in time. Data protection regulation may also provide specific notice requirements (e.g., [41, 42, 43]).

Regardless of regulatory requirements, additional information should be compiled about data practices – especially unexpected ones – to ensure the effectiveness of notices provided to users. The notice should help the recipient make informed privacy decisions. This can be achieved by identifying reasons or benefits for the practice with regard to a specific audience, determining implications and risks for the respective audience, and identifying remedies or choices available to the respective audience. Providing reasons offers the opportunity to explain the purpose of a potentially unexpected, yet benign data practice [85]. Communicating risks [16], for instance with examples [59], supports an individual's assessment of privacy implications, especially when data practices are complex or abstract. Offering specific choices makes the information actionable.

3.4 System Constraints and Opportunities

A specific system may impose constraints on privacy notices that need to be considered in their design. In general, aspects to consider are the different interfaces provided by a system, including their input and output modalities, as well as their relation to specific audience groups. Specific interfaces may have further constraints, such as limited screen real estate. For instance, the FTC [48] notes that providing notice and choice in the context of the IoT can be challenging due to the ubiquity of devices, persistence of collection, and practical obstacles for providing information if devices lack displays or explicit user interfaces. Similar issues have already been recognized in the context of ubiquitous computing [74]. Designing notices for specific audiences may further be limited by how the respective audience can be reached or how they can communicate their privacy choices [103].

Systems may also provide opportunities that can be leveraged to provide a layered and contextualized notice concept for each audience, and potentially even integrate privacy notices and controls into a user's primary activity [113]. By recognizing the constraints, designers may be able to find creative and perhaps novel ways for giving notice. For instance, the lack of explicit user interfaces on a device can be compensated with privacy dashboards, video tutorials, privacy icons or barcodes on the device, and offering choices at the point of sale or in setup wizards [48]. Identified constraints may also be addressed by considering notice mechanisms as part of the system design, i.e., adjusting system features to accommodate notices and controls.

3.5 Layered and Contextualized Notices

While it may be essential to be transparent about many aspects of a system's data practices, showing everything at once in a single notice is rarely effective. Instead, all but the most simple notices should consist of multiple layers. Multi-layered notices constitute a set of complementary privacy notices that are tailored to the respective audience and the prevalent contexts in which they are presented. The granularity of information provided in a specific notice layer must be appropriate for the respective context. For example, a full privacy policy can be complemented by short and condensed notices summarizing the key data practices [9, 85]. Just-in-time or transactional notices provide notice about a specific data practice when it becomes relevant for the user [47], for example, informing about how contact information is used or whether it is shared with third parties when a user registers on a website.

A multi-layered notice concept combines notices shown at different times, using different modalities and interfaces, and varying in terms of content and granularity in a structured approach. For example, some data practices may not require an immediate notice, particularly those that are consistent with users' expectations [46]. It can be expected that a fitness tracker collects information about the user's physical activities – this is the main purpose of the device – thus this collection does not necessarily require prior notice. Automatically uploading a user's activity data to a server or sharing it with other apps may be less expected, thus appropriate notice and choice should be given [85].

Any specific notice should include only the information and control options most relevant and meaningful to a specific audience at that time. Following the details-on-demand pattern [118], initial notices can either point towards additional information and controls or be complemented with alternative user interfaces to review data practices or privacy settings. Deciding what information to include in an initial short notice is a crucial aspect at this stage, because users are more likely to provide consent to the short notice than click through to a more detailed privacy notice. Thus, if such a short notice does not capture all relevant information it may hide information and impair transparency [84]. This is especially an issue for unexpected data practices. Therefore, the notice concept should structure notice layers hierarchically in such a way that the smallest notice either already captures the main aspects of the data practice or draws attention to more expressive notices. Subsequent layers may add additional characteristics.

Designers further need to be aware of not overwhelming users with privacy notices. While many data practices may warrant a notice, providing too many or repetitive privacy notices can result in habituation – users click notices away without considering their content. After a few repetitions, the content of a warning literally does not register anymore in the user's brain [5, 6]. Finding the appropriate number of notices may require user testing. Polymorphic messages [5] or forcing interaction with the notice [21, 22] can reduce habituation effects. A good practice is to prioritize what and when notices are shown based on privacy risks associated with the respective data practice [49].

An example for multi-layered design is the Microsoft Kinect sensor. This device uses video, depth-cameras, and audio to enable users to interact with games through motion and speech. The Kinect has two LEDs that indicate whether motion detection is active or whether video and audio are being recorded and potentially sent to a server. Users can further access a full privacy notice through the screen to which the Xbox is connected, as well as on the Xbox website [137]. Unfortunately, the LED indicators alone cannot make users aware of what information is being collected or shared for what purposes, whereas the policy will likely be ignored by most users. Thus, additional notice layers could enhance awareness and obtain informed consent from users.

In Section 4 we introduce a design space for privacy notices that supports the development of a layered and contextualized notice concept by exposing the relevant dimensions that can be leveraged in the design of individual notices, namely the *timing*, *channel*, and *modality* of notices, as well as the *control* options a notice may provide.

3.6 User-centered Design and Evaluation

Once a notice concept has been developed for each audience, individual notices can be designed and evaluated in a user-centered design process, or by engaging users in participatory design [130]. When conceptual notices for different audiences overlap in terms of timing, channel, modality and content, they can potentially be combined into a single notice serving multiple audiences, as long as the resulting notice meets the requirements of each audience group.

User testing and usability evaluation of notices can be integrated into a system's overall evaluation and quality assurance processes. One should evaluate the individual notices, as well as their combination and the overall notice concept. Notices should be evaluated in the context of the actual system or system prototypes to ensure that they integrate well into the system's interaction design. The effectiveness of notices and warnings can be evaluated along multiple dimensions, such as user attention, comprehension, and recall [8, 12]. It is also important to evaluate whether notices help users make informed choices, both about using a particular service and about exercising choice options [40, 66, 67].

Typically, notices should be evaluated in rigorous user studies. However, budget and time constraints may not always allow for extensive evaluation. In such cases, expert evaluation with usability heuristics [89] can provide at least some indication of the notices' effectiveness. Crowdsourcing platforms also offer an opportunity for conducting quick and inexpensive evaluations of privacy notice design [14].

The outlined best practices support the development of a comprehensive set of privacy notices tailored to a system's different audiences. In the next section, we describe the design space of privacy notices in detail to effectively support the design of individual notices as well as audience-specific notice concepts.

4. DESIGN SPACE OF PRIVACY NOTICES

The design practices outlined in the previous section help to integrate notice design into a system's development process. The purpose of the design space described in this section is to aid the design of specific notices by supporting system designers and privacy engineers in considering the design dimensions of privacy notices. The design space also provides a taxonomy and vocabulary to compare, categorize, and communicate about different notice designs – within a product team as well as with other involved stakeholders, such as the legal department, responsible for drafting the privacy policy, and management. The design space approach

has also been used in other privacy and security research, for example, for the creation of a taxonomy of social network data [112], the investigation of web browser Privacy Enhancing Technologies (PETs) [138], and the examination of interfaces for anti-phishing systems [28].

We constructed our design space according to design science principles [102, 126]. Following Peffers et al.'s research methodology [102], we developed and refined the design space in an iterative process, starting with an extensive literature review and the collection and assessment of multiple existing information systems and their privacy notices. This resulted in an initial privacy notice taxonomy, for which we collected feedback in informal discussions with about 20 privacy experts and professionals in summer 2014 at the Symposium on Usable Privacy and Security [120] and at the Workshop on the Future of Privacy Notice and Choice [30]. In further iterations, we refined the design space by taking the expert feedback into consideration and assessing the applicability and expressiveness of the design space in the context of several scenarios grounded in existing privacy notices.

Figure 1 provides an overview of the design space. Its main dimensions are a notice's *timing* (when it is provided), *channel* (how it is delivered), *modality* (what interaction modes are used), and *control* (how are choices provided). In the following, we describe each dimension in detail. Note, that it often makes sense to consider these dimensions in parallel rather than in sequence, as different dimensions can impact each other. Furthermore, the options for each dimension presented here are not meant to be exclusive. The design space can be extended to accommodate novel systems and interaction methods.

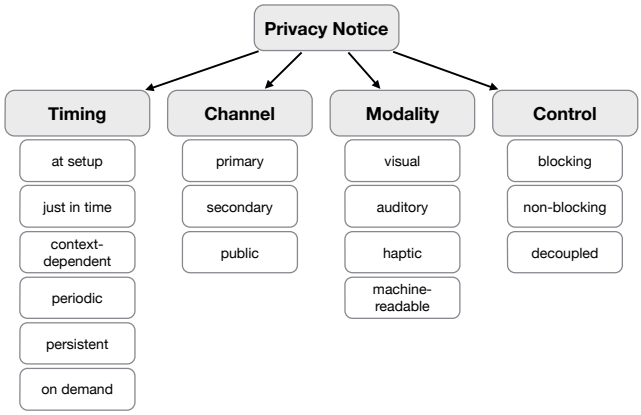

Figure 1: The privacy notice design space.

4.1 Timing

Timing has been shown to have a significant impact on the effectiveness of notices [12, 40, 56, 100]. Showing a notice at an inopportune time may result in users ignoring the notice rather than shifting their attention to it [132]. Delays between seeing a notice and making a privacy decision (e.g., caused by distractions) can change the user's perception of the notice [98] and even cancel out a notice's effect [3]. Thus, users may make different decisions at different points in time, depending on what primary task they are engaged in, information provided in a notice, and other contextual factors [2]. A comprehensive notice concept should provide notices at different times tailored to a user's needs in that context. We describe six possible timing opportunities here.

4.1.1 At setup

Notice can be provided when a system is used for the first time [85]. For instance, as part of a software installation process users are shown and have to accept the system's terms of use. Receiving and acknowledging a HIPAA privacy notice [125] when checking into a doctor's office in the U.S. can also be considered a setup notice – even if provided on paper. Typically, privacy notices shown at setup time are complemented by a persistently available privacy policy that can be accessed retrospectively by users on demand.

An advantage of providing notices at setup time is that users can inspect a system's data practices before using or purchasing it. The system developer may also prefer to provide information about data practices before use for liability and transparency reasons. Setup notices can be used to make affirmative privacy statements to gain user trust. For example, a form to sign up for an email newsletter may contain a concise statement that email addresses are not shared with third parties [24]. Setup notices also provide the opportunity to explain unexpected data practices that may have a benign purpose in the context of the system [85]. Such explanations can be integrated into the system's setup wizard or video tutorials. Showing privacy information before a website is visited can even impact purchase decisions. Egelman et al. found that participants were more likely to pay a premium at a privacy-protective website when they saw privacy information in search results, as opposed to on the website after selecting a search result [40].

However, privacy notices at setup also have multiple shortcomings. Users have become largely habituated to install-time notices, such as end-user license agreements, and ignore them [19]. At setup time, users may have difficulty making informed decisions because they have not used the system yet and cannot fully assess its utility or weigh privacy trade-offs. Furthermore, users may be focused on the primary task, namely completing the setup process to be able to use the system, and fail to pay attention to notices [56]. Therefore, privacy notices provided at setup time should be concise and focus on data practices immediately relevant to the primary user rather than presenting extensive terms of service [85]. Integrating privacy information into other materials that explain the functionality of the system may further increase the chance that users do not ignore it.

4.1.2 Just in time

A privacy notice can be shown when a data practice is active, for example when information is being collected, used, or shared. Such notices are referred to as "contextualized" or "just-in-time" notices [13, 68, 85]. Patrick and Kenny [101] first proposed just-in-time click through agreements in order to provide notice and obtain consent with a concise dialog specific to a certain data practice or transactional context. An example of notices triggered by data collection are cookie consent notices shown on websites in Europe [43]. Just-in-time notices can complement or replace setup notices.

Just-in-time notices and obtaining express consent are particularly relevant for data practices considered sensitive or unexpected [48, 85]. For instance, in the case of mobile apps, access to sensitive information such as the user's location, contacts, photos, calendars, or the ability to record audio and video should be accompanied by just-in-time no-

tices [47]. Another example are cars with automatic headlamps that continually sense ambient light conditions; providing notice about this type of data collection might not be necessary. However, privacy expectations may be violated when this information is shared with an insurance company to determine how often the car is driven at night. In such cases, privacy notice as well as choices should be provided. While just-in-time notices enhance transparency and enable users to make privacy decisions in context, users have also been shown to more freely share information if they are given relevant explanations at the time of data collection [68].

Typically, just-in-time notices are shown before data are collected, used, or shared if express user consent is required. On websites, information about how collected data will be used can be presented near input fields in online forms [68]. Just-in-time summary dialogs [7] can show summarized transaction data before it is sent to a service provider. This approach is often used before applications send error or crash reports. Small delays to avoid interrupting the user's primary task may be acceptable [100, 98].

4.1.3 Context-dependent

The user's and system's context can also be considered to show additional notices or controls if deemed necessary [113]. Relevant context may be determined by a change of location, additional users included in or receiving the data, and other situational parameters. Some locations may be particularly sensitive, therefore users may appreciate being reminded that they are sharing their location when they are in a new place, or when they are sharing other information that may be sensitive in a specific context. For example, Wang et al. [129] proposed a notice that provides cues to Facebook users about the audience of their future post to help avoid oversharing. Facebook introduced a privacy checkup message in 2014 that is displayed under certain conditions before posting publicly. It acts as a "nudge" [1, 29] to make users aware that the post will be public and to help them manage who can see their posts (see Figure 2). In sensor-equipped environments, such as smart homes, new users or visitors should also be made aware of what information is being collected and how it is used [74]. Privacy-preserving proximity testing could help determine when the user is near a sensor [10, 75].

Challenges in providing context-dependent notices are detecting relevant situations and context changes. Furthermore, determining whether a context is relevant to an individual's privacy concerns could in itself require access to that person's sensitive data and privacy preferences [113]. However, providing context-specific support may help users make privacy decisions that are more aligned with their desired level of privacy in the respective situation and thus foster trust in the system.

4.1.4 Periodic

Notices can be shown once, the first couple of times a data practice occurs, or every time. The sensitivity of the data practice may determine the appropriate frequency. Additionally, if the notice includes a consent or control option, it may be appropriate to obtain consent on different occasions, depending on the context, user action, or data being collected. However, showing a notice more than once can be overbearing and can lead to notice fatigue [18] and habituation [6, 22]. Thus, repeating notices need to be designed carefully [5] and their frequency needs to be balanced with user needs. Data practices that are reasonably expected as part of the system may require only a single notice, whereas practices falling outside the expected context of use may warrant repeated notices. In general, it is also advisable to show a notice anew if a data practice has changed.

Periodic reminders of data practices can further help users maintain awareness of privacy-sensitive information flows. Reminders are especially appropriate if data practices are largely invisible [10]. For example, in the health domain, patient monitoring devices in the home may remind users on a weekly basis that data is being collected. Those messages make the user aware of the on-going practice and can provide control options. Almuhimedi et al. [4] find that periodic reminders of how often a user's location and other information has been accessed by mobile apps caused participants to adjust and refine their privacy settings. Another example of periodic reminders are the annual privacy notices U.S. financial institutions must provide to customers [35].

A challenge with periodic notices is that they must be relevant to users in order to be not perceived as annoying. Reminders should not be shown too frequently and should focus on data practices about which users may not be aware. If a system has too many data practices requiring reminders, data practices can be prioritized based on their potential privacy impact or a combined notice can remind about multiple data practices. Individual reminders can also be integrated into an overall notification schedule to ensure that users are not overwhelmed. Rotating warnings or changing their look can further reduce habituation effects [5, 132].

4.1.5 Persistent

Persistent notices can provide awareness of ongoing data practices in a less obtrusive manner. A persistent indicator is typically non-blocking and may be shown whenever a data practices is active, for instance when information is being collected continuously or when information is being transmitted [34, 47]. When inactive or not shown, persistent notices also indicate that the respective data practice is currently not active. For instance, Android and iOS display a small icon in the status bar whenever an application accesses the user's location, if the icon is not shown the user's location is not being accessed. Privacy browser plugins, such as Privacy Bird [34] or Ghostery [54], place an icon in the browser's toolbar to inform users about the data practices or third party trackers of the website visited. Recording lights are examples of persistent notices that indicate when a sensor is active. Camcorders, webcams, the Kinect sensor, Google Glass, and other devices feature such indicators.

An issue with such ambient indicators is that they often go unnoticed [105] and that most systems can only accommodate such indicators for a small number of data practices. A system should only provide a small set of persistent indicators to indicate activity of especially critical data practices. Furthermore, persistent indicators should be designed to be noticeable when they are active.

4.1.6 On demand

All previous timing options pertain to the system actively providing notices to users. Users may also actively seek privacy information and request a privacy notice. Therefore, systems should expose opportunities to access privacy notices on demand [85]. A typical example is posting a pri-

vacy policy at a persistent location [74] and providing links to it from a website, app, or other privacy notices in the system. A better option are privacy settings interfaces or privacy dashboards within the system that provide information about data practices; controls to manage consent; summary reports of what information has been collected, used, and shared by the system; as well as options to manage or delete collected information. Contact information for a privacy office should be provided to enable users to make written requests.

4.2 Channel

Privacy notices can be delivered through different channels. We distinguish *primary*, *secondary*, and *public* channels. A system may leverage multiple channels to provide different types of notices.

4.2.1 Primary

When a privacy notice is provided on the same platform or device a user interacts with, a primary channel is used for delivering the notice. One example is a privacy notice shown on the user's smartphone that is either provided by the app in use or the operating system. Another example are privacy notices shown on websites. The defining characteristic of a primary channel is that the notice is provided within the user's interaction with the system, i.e., the user is not required to change contexts. Thus, a browser plugin that provides privacy information about a website (e.g., Privacy Bird [34]) would also be considered a primary channel as the notice is provided within the browsing context.

Using a primary channel is typically preferable, because the notice is presented within the context of the system, which supports users in evaluating privacy implications and their privacy preferences [97, 113]. The primary channel is particularly suitable to provide notice to primary users, but can also be used to provide notices to secondary users. For instance, other household members can also be addressed by a smart home appliance's privacy indicators.

4.2.2 Secondary

Some systems may have no or only limited primary channels that can be leveraged for privacy notices and obtaining consent [10]. Wearables, smart home appliances, and IoT devices are examples of systems with constrained interaction capabilities. Such devices may have very small or no displays, which makes it difficult to display notices in an informative way [103]. For instance, privacy policies are more difficult to read on mobile devices [119]. LEDs and other output features could serve as persistent privacy indicators but are often insufficient to communicate relevant aspects of data practices, such as for what purposes data is being collected or with whom it is being shared. Moreover, IoT devices may be installed in remote or less accessible locations. The user may not be near the sensor device when a notice is generated. The user's context may further constrain the use of primary channels for privacy notices. For instance, car owners cannot read detailed privacy notices while driving; users of Internet-connected gym equipment may only want basic information about data sharing while they exercise, but may be interested in learning more about privacy implications when at home.

In such cases, privacy notices can be provided via secondary channels, i.e., outside the respective system or context. A secondary channel leverages out-of-band communication to notify primary and secondary users. For instance, secondary channels can be used to provide setup notices. Rather than showing privacy information on the respective device, choices could be provided at the point of sale (e.g., opt-outs or opt-ins for specific data practices) or as part of video tutorials [48]. Just-in-time, context-dependent, and periodic notices can be delivered as text messages or emails, or any other available communication channel. This requires that the user agrees to receive such notices and provides respective contact information during setup [48]. For instance, the iOS update process gives the option to email oneself the terms of service instead of reading them on the phone.

On-demand notices can be made persistently available at a well-defined location [74], such as posting a (multi-layered) privacy policy on the system's website. Pointers to the privacy policy from the system or device (e.g., using visual markers [10, 48]) can ease access to that privacy notice layer.

An increasingly common approach is to make privacy notices and controls available on a companion device, e.g., on a paired smartphone rather than directly on the wearable or IoT device. Such companion devices provide larger displays and more input and output options to make notices more accessible. Companion devices can also act as privacy proxies [75] for a larger number of constrained devices and systems. Examples are centralized control centers for smart home and IoT devices [48], or privacy and permission managers on mobile devices [4, 47].

4.2.3 Public

Primary and secondary channels are targeted at specific users. However, some systems are not aware of the identity of their users, especially secondary and incidental users. In such cases, public channels can be leveraged to provide notice and potentially choices. Examples of public channel privacy notices are signs posted in public places to inform about video surveillance or a camera's recording indicator.

Public notices can also be supported by technology. IoT devices and other systems may broadcast data practice specifications wirelessly to other devices nearby [10] in so called privacy beacons [75]. For instance, a camera could inform about the purpose of its recordings, how long recordings are retained and who may access them. Such beacons can also inform about available privacy controls [69].

Public channels can also be leveraged by users to communicate their privacy preferences. Markers can be placed on physical objects to control object or face recognition [109]. A privacy beaconing approach can be used to broadcast preferences to others nearby, for instance transmitting the wish to not be photographed to camera phones nearby [70].

4.3 Modality

Different modalities can be used to communicate privacy notices to users. Which modality should be selected depends on what the specific notice strives to achieve, the user's likely attention level, and the system's opportunities and constraints. According to the C-HIP model [32, 132], users process warning messages by switching their attention to them, extracting relevant information from the warning, and comprehending the information; a user's attitudes and beliefs determine if the user acts on the warning. Privacy notices can target each aspect of this process and the choice of modality can increase the effectiveness. For example, if

users are engaged in a task that requires visual attention (e.g., driving), using audio to convey privacy information may be more appropriate. Note that not all modalities may be consistently available or effective. Accessibility issues due to physical or visual impairments need to be considered in notice design [128]. Users may also not hear or see a notice due to distractions, blocked line of site, or headphone use. Thus, it is important to evaluate the saliency of different modalities used in notice design [132].

We first discuss visual notices, including text and icons, as they are most common. Auditory and haptic signals can also be used to communicate privacy information. However, they have a lower capacity for conveying information compared to visual notices, which may result in a user preference for visual or textual notices [28]. Quite often, modalities are combined; for example, an audio signal may be used to draw attention to a visual notice displayed on a screen. Finally, machine-readable privacy notices enable the use of different modalities and representations depending on context.

4.3.1 Visual

Visual notices can be provided as text, images, icons, or a combination thereof. Presentation and layout are important aspects in the design of visual notices [132], including colors, fonts, and white space, all of which can impact users' attention and comprehension of the notice [28, 29].

Textual notices can convey complex ideas to users. However, linguistic properties have been shown to influence the perception of warning messages [58]; a notice's framing affects sharing decisions [3]. Specialized terms and jargon may lead to low understanding or the inability to make appropriate privacy decisions [14, 77]. Thus, designers should pay attention to a notice's wording [132], including user testing [14].

While today's website privacy policies are often lengthy [64, 83], privacy notices do not have to be. Relevant information can often be expressed more concisely than in prose. For instance, short notices for smartphone apps have been proposed that convey useful privacy information in the form of risk or expectation scores [53, 79, 80, 88]. Privacy tables and privacy nutrition labels have also been proposed to summarize websites' data practices [66, 84, 87]. Some privacy notice formats have also been standardized by industry or regulators, e.g., financial privacy notices in the U.S. [52]. Standardized notices offer a familiar interface for users, and ease comparison of products [66].

The effectiveness of notices can be increased by personalizing them to the specific user; for instance by including the user's name in the notice [133] or leveraging other user characteristics, such as their demographics or familiarity with a system [132]. An aspect related to personalization is the translation of textual privacy notices into the user's language. Failing to translate may leave international users uninformed about the privacy policy or unable to exercise control over their privacy settings [124].

Images, icons, and LEDs are further options for conveying privacy information visually. Icons can quickly convey privacy settings or currently active data practices. They can be combined with a control switch to activate or deactivate the data practice [48]. However, due to privacy's often abstract nature, images or icons depicting privacy concepts can be difficult to develop. A number of icon sets have been proposed to represent various privacy concepts, both in industry [38, 78, 104, 108] and in research projects [29, 34, 55, 61], with varying levels of success. For example, the AdChoices icon used by the online advertising industry and placed on web ads has been shown to have low user comprehension [78]. Physical indicators, such as LEDs, may use light to visually indicate data practices. LEDs do not have to be binary (on or off) but could leverage colors and blinking patterns to convey different information [60]. Google Glass' display is a transparent glass block that is visibly illuminated if the device is in use, which gives bystanders an indication of whether the device is active.

The meaning of abstract indicators, such as icons or LEDs, often needs to be learned, thus requiring user education. Users may also not notice them [105]. However, when done well pictorial symbols increase the salience and likelihood of a warning being noticed [132], thus, combining icons with textual explanations in privacy notices may improve the effectiveness of the notice, yet, does not require that users learn the exact meaning of the icon.

Visceral notices take an experiential rather than descriptive approach [23]. For example, eyes appearing and growing on a smartphone's home screen relative to how often the user's location has been accessed [114] can leverage strong reactions to anthropomorphic design [23] to provide an ambient sense of exposure.

4.3.2 Auditory

Auditory notices can take at least two forms: spoken word and sounds. Spoken word may be the form of an announcement, pre-recorded or otherwise. One familiar example is the announcement when calling a hotline that the call might be recorded before being connected to a representative.

Sounds can be specialized for the device, or based on well-known sounds in that culture. Calo discusses several examples of visceral notices in which audio signals can "leverage a consumer's familiarity with an old technology" [23]. One example are digital cameras; although some digital cameras and smartphones do not have a physical shutter, they are often configured to emit a shutter sound to make secondary users (i.e., the subjects of the picture) and passersby (incidental users) aware that the device is collecting data by taking a picture. A bill was proposed in the US Congress in 2009 to make such camera shutter sounds mandatory [23]. The bill was not passed, however, some Asian countries have had such requirements for many years.

Auditory warnings can also draw attention to data practices or other notices [132]. For example, the P3P browser plugin Privacy Bird emitted different bird chirping sounds depending on whether the website's privacy policy matched the user's specified privacy preferences [34]. Balebako et al. [13] used sounds to draw attention to occasions when game apps accessed the user's location and other data during game play. Auditory notices face similar challenges as icons – unless familiar [23], their meanings need to be learned. However, they can draw attention to ongoing data practices or privacy notices requiring user attention, especially for systems and devices with constrained interaction capabilities.

4.3.3 Haptic and other

While not widely used for privacy notices yet, haptic feedback provides a potential modality to communicate privacy information. For instance, Balebako et al. [13] combined sound and vibration to notify users about data sharing on

smartphones. Similar approaches could be used in wearable devices without displays.

Other modalities taking advantage of human senses, such as smell, wind, ambient lighting, or even taste [71], could be potentially leveraged for privacy notices as well. For instance, olfactory displays [72] could use chemical compounds to generate a pleasant or disgusting smell depending on whether a system or app is privacy-friendly or invasive. Such approaches may warrant further exploration.

4.3.4 Machine-readable

The previous modalities directly engage the user's senses. An additional modality offered by technical systems is to encode data practices in a machine-readable format and communicate them to other systems or devices where the information is rendered into a privacy notice. This way, the origin system only needs to specify the data practices and can leave it to the recipient how the information is presented to the user, leveraging that system's input and output capabilities. This also provides the opportunity to present notices in different formats on different devices, or differently for specific audiences. However, there is also a risk that machine-readable data practices are misinterpreted or misrepresented by a device. Transparent documentation, certification, or established guidelines on how the machine-readable format should be interpreted may alleviate this issue [110].

Maganis et al. equipped devices with small displays that show active QR codes, which encode recent data collection history and the device's privacy policy [81]. Privacy beacons [75] have already been mentioned as an approach to transmit machine-readable data practices to other devices.

The Platform for Privacy Preferences (P3P) is a standard machine-readable format for expressing data practices. Websites provide a P3P policy that P3P user agents, such as Privacy Bird [34] or Internet Explorer, can obtain and render. While P3P failed to reach widespread adoption [33], communicating data practices in a machine-readable format may gain acceptance in the IoT context [10, 113]. Smartphone apps or centralized command centers could aggregate privacy information from multiple constrained devices and offer a unified notice format and privacy controls.

4.4 Control

Whenever possible, privacy notices should not only provide information about data practices but also include privacy choices or control options. Choices make the information in privacy notices actionable and enable users to express their consent and their privacy preferences.

The typical choice models are *opt-in*, i.e., the user must explicitly agree to a data practice, and *opt-out*, i.e., the user may advise the system provider to stop a specific practice. However, choices need not be binary. Instead users can be provided with controls to refine purposes for which collected information can be used, specify recipients of information sharing, or vary the granularity of information collected or shared. The goal should be to provide means for users to express preferences globally and selectively [74] instead of a take-it-or-leave-it approach. Controls need to be designed well in order to not overwhelm the user with choices [115].

Furthermore, offering elaborate privacy controls can lead to oversharing over time, either because users feel in control and thus share more [20], or just because of the usability cost of managing the settings [65]. Therefore, default settings need to be carefully considered [85], as they may be kept unchanged out of convenience or because they are interpreted as implicit recommendations [2]. Notice can also give explicit recommendations, for example, as nudges that highlight beneficial choices [1, 4], or with social navigation cues that inform about others' privacy choices [17, 99].

Controls can be directly integrated into the notice, in which case they may be blocking or non-blocking, or they can be decoupled to be used on demand by users. This may be desirable if the control panel is complex or if the notice provides only limited opportunities for integrating control.

4.4.1 Blocking

Setup, just-in-time, context-dependent, and periodic notices may include blocking controls. A blocking notice requires the user to make a choice or provide consent based on the information provided in the notice. Until the user provides a choice he or she cannot continue and the respective data practice is blocked. Blocking notices typically constitute opt-in consent, e.g., when terms of service must be accepted in order to use the service, but ideally should provide more meaningful choices. For example, if a smartphone privacy notice states that the camera app can access the device's location, users should be able to selectively allow or deny this access while still being able to use the app.

An issue with such clickthrough agreements [101] is that users may click without reading the provided information. Moving away from just presenting yes and no buttons can increase engagement with the dialog. For instance, Fischer-Hübner et al. propose using a map metaphor on which the user has to drag and drop data onto areas corresponding to their sharing preference [50]. Bravo-Lillo et al. found that forcing users to interact with relevant information in the notice, e.g., by having to move the mouse cursor over a specific text, can effectively address habituation [21, 22].

4.4.2 Non-blocking

Blocking controls require engagement, which can be obtrusive. Non-blocking controls can provide control options without forcing user interaction. For instance, Facebook and Google+ provide integrated sharing controls when users create a post. Users who do not interact with these controls have their posts shared according to the same settings as their previous posts. The same dialog can also inform about a post's audience [129]. Privacy notices can also link to a system's privacy settings to ease access to privacy controls without blocking the interaction flow.

4.4.3 Decoupled

Some notices may not provide any integrated privacy controls due to system or device constraints. They can be complemented by privacy controls that are decoupled from the specific privacy notice. For instance privacy dashboards and privacy managers enable users to review and change privacy settings when needed [47, 48]. Online companies, like Google, offer such privacy dashboards to control privacy settings across multiple of their services; advertising associations provide websites to allow web users to opt out of targeted advertising for all partners. Apple's iOS provides a settings menu to control privacy settings for installed apps.

Decoupled privacy controls may also take a more holistic approach by attempting to learn users' privacy preferences from their control choices. Those learned preferences could

then be applied to other systems, for example, when a new device is connected to the user's smart home system [48].

5. USE CASES

The description of the privacy notice design space highlights the variety of potential privacy notice designs. In this section, we discuss privacy notice approaches in three different domains, how they map onto our design space, and identify potential design alternatives.

5.1 Website & Social Media Privacy Policies

The prevalent approach for providing notice on websites is to post the website's privacy policy on a dedicated page. Audiences of a website's privacy policy are primary and secondary users, as well as regulators. Websites typically provide notices on demand (*timing*), i.e., users need to seek and access the privacy policy if they want to learn about a website's data practices. Website notices typically use the *primary channel*, because websites are not tied to a specific hardware or screen size, and are largely visual (*modality*). Privacy controls are often decoupled from a privacy notice (*control*), i.e., the privacy policy may point to a settings page that allows users to manage privacy, typically by opting-out of certain practices, such as data sharing with advertisers.

The status quo of website privacy notices is a major reason why notice and choice is considered ineffective [25, 33, 116]. However, some websites have developed more effective notice concepts. For instance, Microsoft [86], Facebook [44], and others have implemented multi-layered privacy policies that are also interactive. Explanations are integrated into the privacy page and details are provided on demand rather than showing a long privacy policy. But improving the presentation of the privacy policy is not sufficient if users do not access it. Users require notices integrated into the website in addition to a privacy policy.

One approach is to leverage different timing options, such as just-in-time and contextual notices. Notices can be shown when a data practice occurs for the first time or when the user uses a specific feature for the first time. Notices can be integrated into online forms to make users aware of how their provided data is used and with whom it may be shared. Browsers also provide just-in-time notices for resource access, e.g., when a website wants to use the user's location. Contextual notices can be used to warn about potentially unintended settings. For instance, Facebook introduced a privacy checkup warning when posting publicly, see Figure 2. This blocking notice explains the potential issue and offers integrated privacy controls. The same notice could be realized with non-blocking controls, e.g., as a banner below the post entry field; by blocking the publishing of the post, users are forced to validate their settings. Also note that the dialog does not contain an "OK" button; the user needs to make a specific choice.

Varying a notice's channel is not meaningful for most websites, because the primary channel is well accessible. However, secondary channels, such as email, SMS, and mobile app notifications, are being used by social media sites to provide privacy-relevant notifications, for instance, when one has been tagged in a photo or receives a friend request.

Most privacy controls on websites are decoupled from specific notices. But account registration forms may require users to provide opt-in consent for certain data practices before the account can be created. Cookie consent notices as required by European data protection regulation have been implemented as blocking notices, as well as non-blocking notices, e.g., a banner shown at the top of a page that does not impair use of the website.

Figure 2: Facebook's privacy checkup notice warns the user before posting publicly.

5.2 Smartphone app permissions

In contrast to websites' privacy policies, privacy and permission management on smartphones employs a more interactive approach. Whereas websites manage privacy on their own, mobile platforms regulate who installed apps access sensors and user resources (e.g., contacts and text messages). Currently, the two major platforms, Android and iOS, take different approaches in terms of how they provide privacy notices and controls to users concerning apps' access to resources. In the following, we discuss how their approaches utilize different parts of the design space. We focus on the current versions of those platforms (iOS 8.x and Android 5.x).

For both iOS and Android the smartphone itself is the *primary channel*. Both systems show privacy notices mainly on the device. Apps can also be installed via a *secondary channel*, namely a Web store for Android and the iTunes application for iOS. While this secondary channel is available via a computer, the notice design is almost identical to app installation directly on the device.

In terms of *modality*, both systems primarily use *visual notices*. Android further requires apps to declare requested permissions in a manifest (*machine-readable*), while iOS apps may specify usage descriptions for access of restricted resources (e.g., location or contacts).

In their app stores, both platforms provide links to an app's privacy policy, which users may access *on demand*. Android further integrates privacy notices into an app's installation process (*at setup*). The user sees a screen that lists the requested app permissions, and the user must either accept all permissions (*blocking*) or not install the app. When an app update changes the requested permissions, a similar notice is shown (*periodic*).

The app installation process on iOS does not include any privacy notices. Instead, iOS shows notices when an app wants to access a resource for the first time, see Figure 3. These notices are *blocking* and ask the user to allow or deny the access request. The notice may contain a developer-specified explanation [121]. In addition, many iOS apps integrate explanations into the application flow before the access request is shown. As of iOS 8, the app developer can also choose to show the authorization notice in advance, but iOS enforces that a resource cannot be accessed without user authorization. In iOS 8, permission requests are not periodic and are only requested once [76]. However, iOS shows peri-

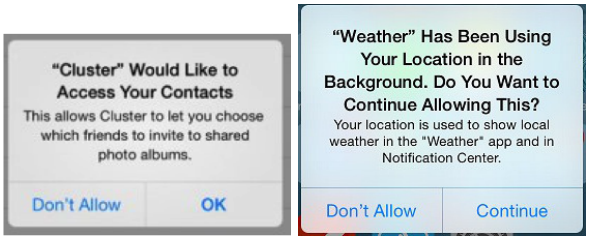

Figure 3: iOS's just-in-time notice with purpose explanation (*left*) and periodic reminder (*right*).

odic reminders for apps that have permission to access the user's location in the background, see Figure 3. Both iOS and Android also use a *persistent* location icon in the toolbar indicating that location information is being accessed.

On iOS, users can access a privacy settings menu that facilitates inspection and adjustment of privacy settings for specific resources, globally as well as for specific apps (*on demand, decoupled*). Android provided a similar option (AppOps) in a previous version, but the current version does not allow users to change an app's permissions. Users can inspect an app's permissions in the app store but the only option for privacy control is to uninstall the app.

Thus, the main difference between the platforms is the level of control afforded to the user. iOS users may choose to deny an app access to any specific resource requested, yet continue to use the app. In contrast, Android users must accept all of an app's permissions in order to use it. Android could make better use of different timing options for notices and offer more controls; iOS leverages the options in the privacy notice design space more comprehensively at the time of writing. However, Google announced in May 2015 that Android will also allow users to grant or revoke permissions selectively in the future [39].

5.3 Photo & Video Lifelogging

Lifelogging [117] aims to support memorization and retrieval of everyday events. A common aspect of lifelogging approaches is the recording of photos and videos at frequent intervals, e.g., with GoPro cameras or neck-worn cameras that automatically take a picture every few minutes. A major issue with those technologies is that they not only record the primary user but also bystanders (*incidental users*) [62]. Yet, privacy notices for lifelogging devices, such as the Autographer camera [11] or Google Glass, are mainly targeted at the primary user. They typically provide a privacy policy on the manufacturer's website, privacy settings in a mobile companion app, or a web portal to control sharing and access to the data stream (*secondary channel, on demand, decoupled*). Incidental users neither receive privacy notices nor have options to control being recorded, except for a recording indicator light or a shutter sound on some devices.

Based on the design space, we can consider alternatives to notify and give control to incidental users. Ideally, incidental users should be informed at the moment they are being recorded or soon afterwards (*just-in-time*) and should be given the opportunity to withdraw consent (*control*). Notices on the device (*primary channel*) are likely not effective, as they may not be salient. In order to leverage a secondary channel, e.g., send a notification to the bystander's smartphone, the bystander would need to be identified in order to determine whom to contact, which introduces additional privacy implications. Another option is to use a *public channel*, for instance by wirelessly broadcasting a *machine-readable* notice that a photo has been taken. The incidental user's device could render the notice visually and use sound or vibration to draw attention to the visual notice (*modalities*). A blocking control option does not make much sense in the context of taking photos and videos, as the primary user would have to wait until consent is collected from all bystanders, even though bystanders and the user may be in motion. Thus, incidental users could be given the *non-blocking* option to retroactively opt-out of being photographed. This choice would need to be relayed back to the primary user's device, which could then either delete the photo or detect and remove or blur the incidental user (which poses additional technical challenges that would need to be addressed). While this could provide a viable solution, it also requires bystanders to express their consent any time someone takes a photo nearby, which may become cumbersome in crowded places or at popular tourist spots. An incidental user's preferences could either be stored on their device, which then could automatically respond to such photo notifications, or the incidental user's photo preferences could be broadcast to photographers nearby [70].

6. CONCLUSIONS

We presented a design space that provides a structured approach and vocabulary to discuss and compare different privacy notice designs. This can support the design of privacy notices and controls. The design space should be leveraged as part of a comprehensive design process that focuses on audience-specific privacy notice requirements and considers a system's opportunities and constraints, in order to develop a notice and choice concept that is well integrated with the respective system, rather than bolted on. Notices should be evaluated in user studies.

A key aspect of effective notice design is the realization that a privacy policy, which may be necessary for regulatory compliance, is insufficient and often unsuitable for informing users. Privacy policies need to be accompanied by a notice concept that leverages the options provided in the notice design space to provide information relevant to the targeted audience and to make that information actionable by providing real choices. Actionability is important, because privacy notices without control may leave users feeling helpless [100]. Empowering users with privacy controls increases their trust and may result in increased use and disclosure [20].

Novel technologies and integrated devices, such as wearables or the Internet of Things, pose new challenges for the design of privacy notices and controls. Information collection is continuous and sharing paramount [73]. Public policy, legislation, and technological approaches need to work together to enable users to manage their privacy in such systems. The identified best practices and the proposed design space provide the means to reason about meaningful design options for notice and control in such systems. For instance, by leveraging alternative channels or modalities, and providing notices and control options at different times in the information lifecycle. A future challenge is to develop and provide tools to support the identification of notice requirements, system opportunities, and applicable options in the design space, and explore the (semi-)automated generation of notice and control interfaces.

Acknowledgments

This research was partially funded by NSF grants CNS-1012763, CNS-1330596, and DGE-0903659, as well as by Facebook. The authors would like to thank Aditya Marella and Maritza Johnson for initial contributions to this project; the privacy and usability experts who provided feedback on iterations of the design space; as well as Alessandro Acquisti, Sameer Patil, Yang Wang, our shepherd Andrew Patrick, and our reviewers for feedback on earlier drafts.

7. REFERENCES

[1] A. Acquisti. Nudging privacy: The behavioral economics of personal information. *IEEE Security Privacy*, 7(6):82–85, 2009.

[2] A. Acquisti, L. Brandimarte, and G. Loewenstein. Privacy and human behavior in the age of information. *Science*, 347(6221):509–514, 2015.

[3] I. Adjerid, A. Acquisti, L. Brandimarte, and G. Loewenstein. Sleights of privacy: Framing, disclosures, and the limits of transparency. In *Proc. SOUPS '13*, page 9. ACM, 2013.

[4] H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L. F. Cranor, and Y. Agarwal. Your location has been shared 5,398 times! a field study on mobile app privacy nudging. In *Proc. CHI '15*. ACM, 2015.

[5] B. Anderson, B. Kirwan, D. Eargle, S. Howard, and A. Vance. How polymorphic warnings reduce habituation in the brain – insights from an fMRI study. In *Proc. CHI '15*. ACM, 2015.

[6] B. Anderson, A. Vance, B. Kirwan, E. D., and S. Howard. Users aren't (necessarily) lazy: Using NeuroIS to explain habituation to security warnings. In *Proc. ICIS '14*, 2014.

[7] J. Angulo, S. Fischer-Hübner, T. Pulls, and U. König. HCI for Policy Display and Administration. In *Privacy and Identity Management for Life*, pages 261–277. Springer, 2011.

[8] J. J. Argo and K. J. Main. Meta-Analyses of the Effectiveness of Warning Labels. *Journal of Public Policy & Marketing*, 23(2):193–208, Oct. 2004.

[9] Article 29 Data Protection Working Party. Opinion 10/2004 on More Harmonised Information Provisions. WP 100, Nov. 2004.

[10] Article 29 Data Protection Working Party. Opinion 8/2014 on the Recent Developments on the Internet of Things. WP 223, Sept. 2014.

[11] Autographer. http://www.autographer.com, 2012. accessed: 2015-06-01.

[12] R. Balebako. *Mitigating the Risks of Smartphone Data Sharing: Identifying Opportunities and Evaluating Notice*. PhD thesis, Engineering and Public Policy, Carnegie Mellon University, 2014.

[13] R. Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen. Little brothers watching you: Raising awareness of data leaks on smartphones. In *Proc. SOUPS '13*. ACM, 2013.

[14] R. Balebako, R. Shay, and L. F. Cranor. Is your inseam a biometric? a case study on the role of usability studies in developing public policy. In *Proc. USEC '14*, 2014.

[15] L. Barkhuus. The Mismeasurement of Privacy: Using Contextual Integrity to Reconsider Privacy in HCI. In *Proc. CHI '12*. ACM, 2012.

[16] L. Bauer, C. Bravo-Lillo, L. F. Cranor, and E. Fragkaki. Warning design guidelines. Tech. report CMU-CyLab-13-002, CyLab, Carnegie Mellon University, 2013.

[17] A. Besmer, J. Watson, and H. R. Lipford. The impact of social navigation on privacy policy configuration. In *Proc. SOUPS '10*. ACM, 2010.

[18] R. Böhme and J. Grossklags. The security cost of cheap user interaction. In *Proc. Workshop on New Security Paradigms*. ACM, 2011.

[19] R. Böhme and S. Köpsell. Trained to accept?: A field experiment on consent dialogs. In *Proc. CHI '10*. ACM, 2010.

[20] L. Brandimarte, A. Acquisti, and G. Loewenstein. Misplaced confidences privacy and the control paradox. *Social Psychological and Personality Science*, 4(3):340–347, 2013.

[21] C. Bravo-Lillo, L. F. Cranor, S. Komanduri, S. Schechter, and M. Sleeper. Harder to ignore? Revisiting pop-up fatigue and approaches to prevent it. In *Proc. SOUPS '14*, 2014.

[22] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter. Your attention please: Designing security-decision uis to make genuine risks harder to ignore. In *Proc. SOUPS '13*. ACM, 2013.

[23] R. Calo. Against notice skepticism in privacy (and elsewhere). *Notre Dame Law Review*, 87(3):1027–1072, 2012.

[24] J. Cannon. *Privacy in Technology*. IAPP, 2014.

[25] F. Cate. The Limits of Notice and Choice. *IEEE Security Privacy*, 8(2):59–62, Mar. 2010.

[26] Center for Information Policy Leadership. Ten Steps to Develop a Multilayered Privacy Notice. White paper, Mar. 2007.

[27] Centers for Medicare & Medicaid Services. The Health Insurance Portability and Accountability Act of 1996 (HIPAA). http://www.cms.hhs.gov/hipaa/, 1996.

[28] Y. Chen, F. M. Zahedi, and A. Abbasi. Interface design elements for anti-phishing systems. In *Service-Oriented Perspectives in Design Science Research*, pages 253–265. Springer, 2011.

[29] E. Choe, J. Jung, B. Lee, and K. Fisher. Nudging people away from privacy-invasive mobile apps through visual framing. In *Proc. INTERACT '13*. Springer, 2013.

[30] CMU CyLab. Workshop on the future of privacy notice and choice. https://www.cylab.cmu.edu/news_events/events/fopnac/, June 27 2015.

[31] L. Cranor. Giving notice: Why privacy policies and security breach notifications aren't enough. *IEEE Communications Magazine*, 43(8):18–19, Aug. 2005.

[32] L. F. Cranor. A framework for reasoning about the human in the loop. In *Proc. UPSEC '08*. USENIX Assoc., 2008.

[33] L. F. Cranor. Necessary but not sufficient: Standardized mechanisms for privacy notice and

choice. *Journal on Telecommunications and High Technology Law*, 10:273, 2012.

[34] L. F. Cranor, P. Guduru, and M. Arjula. User interfaces for privacy agents. *ACM TOCHI*, 13(2):135–178, 2006.

[35] L. F. Cranor, K. Idouchi, P. G. Leon, M. Sleeper, and B. Ur. Are they actually any different? Comparing thousands of financial institutions' privacy practices. In *Proc. WEIS '13*, 2013.

[36] G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. Le Métayer, R. Tirtea, and S. Schiffner. Privacy and Data Protection by Design – from policy to engineering. report, ENISA, Dec. 2014.

[37] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*, 16(1):3–32, Nov. 2010.

[38] Disconnect.me. Privacy policies are too complicated: We've simplified them. https://disconnect.me/icons, Dec. 2014. accessed: 2015-06-01.

[39] J. Eason. Android M developer preview & tools. Android Developers Blog, May 28 2015. http://android-developers.blogspot.com/2015/05/android-m-developer-preview-tools.html, accessed: 2015-06-01.

[40] S. Egelman, J. Tsai, L. F. Cranor, and A. Acquisti. Timing is everything?: the effects of timing and placement of online privacy indicators. In *Proc. CHI '09*. ACM, 2009.

[41] European Parliament and Council. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities*, (L 281):31–50, 1995.

[42] European Parliament and Council. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). *Official Journal of the European Communities*, (L 201), 2002.

[43] European Parliament and Council. Directive 2009/136/EC. *Official Journal of the European Communities*, (L 337), 2009.

[44] Facebook. Data policy. https://www.facebook.com/privacy/explanation, 2015. accessed: 2015-06-01.

[45] Federal Trade Commission. Privacy online: a report to Congress. FTC report, 1998.

[46] Federal Trade Commission. Protecting consumer privacy in an era of rapid change. FTC report, 2012.

[47] Federal Trade Commission. Mobile privacy disclosures: Building trust through transparency. FTC staff report, Feb. 2013.

[48] Federal Trade Commission. Internet of things: Privacy & security in a connected world. FTC staff report, Jan. 2015.

[49] A. Felt, S. Egelman, M. Finifter, D. Akhawe, and D. Wagner. How to ask for permission. In *Proc. HOTSEC '12*, 2012.

[50] S. Fischer-Hübner, J. S. Pettersson, M. Bergmann, M. Hansen, S. Pearson, and M. C. Mont. HCI Designs for Privacy-Enhancing Identity Management. In *Digital Privacy: Theory, Technologies, and Practices*, pages 229–252. Auerbach Pub., 2008.

[51] H. Fu, Y. Yang, N. Shingte, J. Lindqvist, and M. Gruteser. A field study of run-time location access disclosures on android smartphones. In *Proc. USEC '14*, 2014.

[52] L. Garrison, M. Hastak, J. M. Hogarth, S. Kleimann, and A. S. Levy. Designing Evidence-based Disclosures: A Case Study of Financial Privacy Notices. *Journal of Consumer Affairs*, 46(2):204–234, June 2012.

[53] C. Gates, N. Li, H. Peng, B. Sarma, Y. Qi, R. Potharaju, C. Nita-Rotaru, and I. Molloy. Generating summary risk scores for mobile applications. *IEEE Trans. Dependable and Secure Computing*, 11(3):238–251, May 2014.

[54] Ghostery. https://www.ghostery.com. accessed: 2015-06-01.

[55] J. Gomez, T. Pinnick, and A. Soltani. KnowPrivacy. Final report, UC Berkeley, School of Information, 2009.

[56] N. S. Good, J. Grossklags, D. K. Mulligan, and J. A. Konstan. Noticing notice: a large-scale experiment on the timing of software license agreements. In *Proc. CHI '07*. ACM, 2007.

[57] G. Greenleaf. Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories. *Journal of Law, Information and Science*, 23(1):4–49, 2014.

[58] M. Harbach, S. Fahl, P. Yakovleva, and M. Smith. Sorry, I don't get it: An analysis of warning message texts. In *Proc. USEC '13*. Springer, 2013.

[59] M. Harbach, M. Hettig, S. Weber, and M. Smith. Using personal examples to improve risk communication for security & privacy decisions. In *Proc. CHI '14*. ACM, 2014.

[60] C. Harrison, J. Horstman, G. Hsieh, and S. Hudson. Unlocking the expressivity of point lights. In *Proc. CHI '12*. ACM, 2012.

[61] L.-E. Holtz, H. Zwingelberg, and M. Hansen. Privacy Policy Icons. In *Privacy and Identity Management for Life*, pages 279–285. Springer, 2011.

[62] G. Iachello, K. N. Truong, G. D. Abowd, G. R. Hayes, and M. Stevens. Prototyping and sampling experience to evaluate ubiquitous computing privacy in the real world. In *Proc. CHI '06*. ACM, 2006.

[63] P. G. Inglesant and M. A. Sasse. The True Cost of Unusable Password Policies: Password Use in the Wild. In *Proc. CHI '10*. ACM, 2010.

[64] C. Jensen and C. Potts. Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proc. CHI '04*. ACM, 2004.

[65] M. J. Keith, C. Maynes, P. B. Lowry, and J. Babb. Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure. In *Proc. ICIS '14*. SSRN, 2014.

[66] P. G. Kelley, L. Cesca, J. Bresee, and L. F. Cranor. Standardizing privacy notices: an online study of the nutrition label approach. In *Proc. CHI '10*. ACM,

2010.

[67] P. G. Kelley, L. F. Cranor, and N. Sadeh. Privacy as part of the app decision-making process. In *Proc. CHI '13*. ACM, 2013.

[68] A. Kobsa and M. Teltzrow. Contextualized communication of privacy practices and personalization benefits: Impacts on users' data sharing and purchase behavior. In *Proc. PETS '05*. Springer, 2005.

[69] B. Könings, F. Schaub, and M. Weber. PriFi beacons: piggybacking privacy implications on wifi beacons. In *Ubicomp '13 Adjunct Proceedings*. ACM, 2013.

[70] B. Könings, S. Thoma, F. Schaub, and M. Weber. Pripref broadcaster: Enabling users to broadcast privacy preferences in their physical proximity. In *Proc. MUM '14*. ACM, 2014.

[71] P. Kortum. *HCI beyond the GUI: Design for haptic, speech, olfactory, and other nontraditional interfaces*. Morgan Kaufmann, 2008.

[72] P. Kortum. *HCI beyond the GUI: Design for haptic, speech, olfactory, and other nontraditional interfaces*. Morgan Kaufmann, 2008.

[73] S. Landau. Control use of data to protect privacy. *Science*, 347(6221):504–506, Jan. 2015.

[74] M. Langheinrich. Privacy by design – principles of privacy-aware ubiquitous systems. In *Proc. UbiComp '01*. Springer, 2001.

[75] M. Langheinrich. A Privacy Awareness System for Ubiquitous Computing Environments. In *Proc. UbiComp '02*. Springer, 2002.

[76] M. Lazer-Walker. Core location in ios 8. http://nshipster.com/core-location-in-ios-8/, 2014. accessed: 2015-06-01.

[77] P. Leon, B. Ur, R. Shay, Y. Wang, R. Balebako, and L. Cranor. Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising. In *Proc. CHI '12*. ACM, 2012.

[78] P. G. Leon, J. Cranshaw, L. F. Cranor, J. Graves, M. Hastak, B. Ur, and G. Xu. What do online behavioral advertising privacy disclosures communicate to users? In *Proc. WPES '12*. ACM, 2012.

[79] I. Liccardi, J. Pato, D. J. Weitzner, H. Abelson, and D. De Roure. No technical understanding required: Helping users make informed choices about access to their personal data. In *Proc. MOBIQUITOUS '14*. ICST, 2014.

[80] J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proc. UbiComp '12*. ACM, 2012.

[81] G. Maganis, J. Jung, T. Kohno, A. Sheth, and D. Wetherall. Sensor tricorder: What does that sensor know about me? In *Proc. HotMobile '11*. ACM, 2011.

[82] G. Marx. Murky conceptual waters: The public and the private. *Ethics and Information technology*, pages 157–169, 2001.

[83] A. M. McDonald and L. F. Cranor. The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society*, 4(3):540–565, 2008.

[84] A. M. Mcdonald, R. W. Reeder, P. G. Kelley, and L. F. Cranor. A comparative study of online privacy policies and formats. In *Proc. PETS '09*. Springer, 2009.

[85] Microsoft. Privacy Guidelines for Developing Software Products and Services. Technical Report version 3.1, 2008.

[86] Microsoft. Microsoft.com privacy statement. https://www.microsoft.com/privacystatement/en-us/core/default.aspx, 2014. accessed: 2015-06-01.

[87] G. R. Milne, M. J. Culnan, and H. Greene. A longitudinal assessment of online privacy notice readability. *Journal of Public Policy & Marketing*, 25(2):238–249, 2006.

[88] A. Mylonas, M. Theoharidou, and D. Gritzalis. Assessing privacy risks in android: A user-centric approach. In *Workshop on Risk Assessment and Risk-Driven Testing*. Springer, 2014.

[89] J. Nielsen and R. Molich. Heuristic evaluation of user interfaces. In *Proc. CHI '90*. ACM, 1990.

[90] L. Nielsen. Personas. In *The Encyclopedia of Human-Computer Interaction*. The Interaction Design Foundation, 2nd ed. edition, 2014. https://www.interaction-design.org/encyclopedia/personas.html.

[91] H. Nissenbaum. A contextual approach to privacy online. *Daedalus*, 140(4):32–48, 2011.

[92] NTIA. Short form notice code of conduct to promote transparency in mobile app practices. Redline draft, July 2013. http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf.

[93] NTIA. Privacy multistakeholder process: Facial recognition technology, 2014. http://www.ntia.doc.gov/other-publication/2014/privacy-multistakeholder-process-facial-recognition-technology, accessed: 2015-06-01.

[94] OECD. Making Privacy Notices Simple. Digital Economy Papers 120, July 2006. http://www.oecd-ilibrary.org/science-and-technology/making-privacy-notices-simple_231428216052.

[95] OECD. The OECD Privacy Framework. Report, 2013. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[96] Official California Legislative Information. The Online Privacy Protection Act of 2003, 2003.

[97] L. Palen and P. Dourish. Unpacking "privacy" for a networked world. In *Proc. CHI '03*. ACM, 2003.

[98] S. Patil, R. Hoyle, R. Schlegel, A. Kapadia, and A. J. Lee. Interrupt now or inform later?: Comparing immediate and delayed privacy feedback. In *Proc. CHI '15*. ACM, 2015.

[99] S. Patil, X. Page, and A. Kobsa. With a little help from my friends: Can social navigation inform interpersonal privacy preferences? In *Proc. CSCW '11*. ACM, 2011.

[100] S. Patil, R. Schlegel, A. Kapadia, and A. J. Lee.

Reflection or action?: How feedback and control affect location sharing decisions. In *Proc. CHI '14*. ACM, 2014.

[101] A. Patrick and S. Kenny. From privacy legislation to interface design: Implementing information privacy in human-computer interactions. In *Proc. PET '03*. Springer, 2003.

[102] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee. A design science research methodology for information systems research. *Journal of management information systems*, 24(3):45–77, 2007.

[103] S. R. Peppet. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*, 93(85):85–176, 2014.

[104] T. Pinnick. Privacy short notice design. TRUSTe blog, Feb. 2011. http://www.truste.com/blog/2011/02/17/privacy-short-notice-design/, accessed: 2015-06-01.

[105] R. S. Portnoff, L. N. Lee, S. Egelman, P. Mishra, D. Leung, and D. Wagner. Somebody's watching me? assessing the effectiveness of webcam indicator lights. In *Proc. CHI '15*, 2015.

[106] President's Concil of Advisors on Science and Technology. Big data and privacy: A technological perspective. Report to the President, Executive Office of the President, May 2014.

[107] E. Ramirez. Privacy and the IoT: Navigating policy issues. CES Opening Remarks, 2015. FTC public statement.

[108] A. Raskin. Privacy icons: Alpha release. http://www.azarask.in/blog/post/privacy-icons/. accessed: 2015-06-01.

[109] N. Raval, A. Srivastava, K. Lebeck, L. Cox, and A. Machanavajjhala. Markit: Privacy markers for protecting visual secrets. In *UbiComp '14 Adjunct Proceedings*. ACM, 2014.

[110] J. Reidenberg and L. F. Cranor. Can User Agents Accurately Represent Privacy Policies? Available at SSRN: http://papers.ssrn.com/abstract=328860, 2002.

[111] J. R. Reidenberg, T. Breaux, L. F. Cranor, B. French, A. Grannis, J. T. Graves, F. Liu, A. M. McDonald, T. B. Norton, R. Ramanath, N. C. Russell, N. Sadeh, and F. Schaub. Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Technology Law Journal*, 30, 2015.

[112] C. Richthammer, M. Netter, M. Riesner, J. Sänger, and G. Pernul. Taxonomy of social network data types. *EURASIP Journal on Information Security*, 2014(1):1–17, 2014.

[113] F. Schaub, B. Könings, and M. Weber. Context-adaptive privacy: Leveraging context awareness to support privacy decision making. *IEEE Pervasive Computing*, 14(1):34–43, 2015.

[114] R. Schlegel, A. Kapadia, and A. J. Lee. Eyeing your exposure: Quantifying and controlling information sharing for improved privacy. In *Proc. SOUPS '11*. ACM, 2011.

[115] B. Schwartz. *The Paradox of Choice: Why More is Less*. HarperCollins Publishers, 2004.

[116] P. M. Schwartz and D. Solove. Notice & Choice. In *The Second NPLAN/BMSG Meeting on Digital Media and Marketing to Children*, 2009.

[117] A. J. Sellen and S. Whittaker. Beyond total capture: A constructive critique of lifelogging. *Commun. ACM*, 53(5):70–77, May 2010.

[118] B. Shneiderman. The eyes have it: A task by data type taxonomy for information visualizations. In *Proc. Symp. on Visual Languages*. IEEE, 1996.

[119] R. I. Singh, M. Sumeeth, and J. Miller. Evaluating the readability of privacy policies in mobile environments. *International Journal of Mobile Human Computer Interaction*, 3(1):55–78, 2011.

[120] SOUPS 2014 organizing committee. Tenth Symposium on Usable Privacy and Security. http://cups.cs.cmu.edu/soups/2014/, July 9–11 2014.

[121] J. Tan, K. Nguyen, M. Theodorides, H. Negrón-Arroyo, C. Thompson, S. Egelman, and D. Wagner. The effect of developer-specified explanations for permission requests on smartphone user behavior. In *Proc. CHI '14*. ACM, 2014.

[122] The White House. Consumer data privacy in a networked world. Technical report, Feb. 2012. http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[123] B. Ur, J. Jung, and S. Schechter. Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance. In *Proc. UbiComp '14*. ACM, 2014.

[124] B. Ur, M. Sleeper, and L. F. Cranor. Privacy policies in social media: Providing translated privacy notice. *I/S: A Journal of Law and Policy for the Information Society*, 9(2), 2013.

[125] U.S. Department of Health & Human Services. Notice of privacy practices for protected health information, April 2003.

[126] R. H. von Alan, S. T. March, J. Park, and S. Ram. Design science in information systems research. *MIS quarterly*, 28(1):75–105, 2004.

[127] W3C. Tracking protection working group. http://www.w3.org/2011/tracking-protection/. accessed: 2015-06-01.

[128] W3C. Web accessibility and usability working together. http://www.w3.org/WAI/intro/usable. accessed: 2015-06-01.

[129] Y. Wang, P. G. Leon, A. Acquisti, L. F. Cranor, A. Forget, and N. Sadeh. A field trial of privacy nudges on facebook. In *Proc. CHI '14*. ACM, 2014.

[130] S. Weber, M. Harbach, and M. Smith. Participatory Design for Security-Related User Interfaces. In *Proc. USEC '15*, 2015.

[131] R. Wenning, M. Schunter, L. Cranor, B. Dobbs, S. Egelman, G. Hogben, J. Humphrey, M. Langheinrich, M. Marchiori, M. Presler-Marshall, J. Reagle, and D. A. Stampley. The Platform for Privacy Preferences 1.1 (P3P 1.1) Specification. http://www.w3.org/TR/P3P11/, 2006. accessed: 2015-06-01.

[132] M. S. Wogalter, V. C. Conzola, and T. L. Smith-Jackson. Research-based guidelines for warning design and evaluation. *Applied Ergonomics*,

33(3):219–230, 2002.

[133] M. S. Wogalter, B. M. Racicot, M. J. Kalsher, and S. Noel Simpson. Personalization of warning signs: The role of perceived relevance on behavioral compliance. *International Journal of Industrial Ergonomics*, 14(3):233–242, Oct. 1994.

[134] D. Wright. Should privacy impact assessments be mandatory? *Communications of the ACM*, 54(8):121–131, Aug. 2011.

[135] D. Wright. Making Privacy Impact Assessment More Effective. *The Information Society*, 29(5):307–315, Oct. 2013.

[136] D. Wright, K. Wadhwa, P. D. Hert, D. Kloza, and D. G. Justice. A Privacy Impact Assessment Framework for data protection and privacy rights. Deliverable September, PIAF project, 2011.

[137] Xbox.com. Kinect and Xbox One privacy FAQ. http://www.xbox.com/en-US/kinect/privacyandonlinesafety.

[138] H. Xu, R. E. Crossler, and F. Bélanger. A value sensitive design investigation of privacy enhancing tools in web browsers. *Decision Support Systems*, 54(1):424–433, 2012.