Designing Effective Privacy Notices and Controls

Privacy notice and choice are essential aspects of privacy and data protection regulation worldwide. Yet, today's privacy notices and controls are surprisingly ineffective at informing users or allowing them to express choice. Here, the authors analyze why existing privacy notices fail to inform users and tend to leave them helpless, and discuss principles for designing more effective privacy notices and controls.

Florian Schaub
University of Michigan

Rebecca Balebako
RAND Corporation

Lorrie Faith Cranor
Carnegie Mellon University

Personal information is everywhere. Individuals share personal details on social media. Websites and mobile apps collect usage and purchasing habits. Advertisers and data brokers analyze behavioral data to deliver targeted advertising. Fitness wearables, smartwatches, and mobile apps – and their manufacturers – trace every step of their users and know about potential health issues before they do. Voice assistants, learning thermostats, and smart TVs provide companies with unprecedented access to people's homes.

The wide adoption of such potentially privacy-invasive technologies could indicate that many individuals don't care about privacy and are happy to surrender it for added comfort and convenience. However, privacy research suggests a more complex explanation. Surveys and experiments frequently show that many individuals are concerned about their privacy, but feel helpless and resigned when trying to balance privacy needs with other considerations.[1,2] While benefits of a new technology or service are often evident, privacy implications are rarely as clear. Opaque information flows involving multiple entities in the collection, processing, and sharing of personal data make it difficult to judge how data shared for one reason today may affect privacy in other contexts in the future. The progression toward the Internet of Things (IoT) exacerbates this issue as more devices gain extensive sensing capabilities and are highly connected with each other and the cloud.

To understand the privacy implications of using a system or device and make informed privacy decisions, users need to be aware of the system's data practices – for example, what personal information is collected, used, retained, and shared. Privacy laws and regulations around the world recognize this need for transparency – and the associated need for freedom to decide whether to entrust personal information to a certain entity.[3] Despite privacy notice and choice being considered essential aspects of privacy and data protection for decades, today's privacy notices are surprisingly ineffective at informing users.

Published by the IEEE Computer Society
1089-7801/17/$33.00 © 2017 IEEE

Why Today's Privacy Notices Are Ineffective

Today's most prevalent type of privacy notice are lengthy privacy policies that describe a company's data practices. Privacy notices have been studied extensively by the usable privacy and security research community. Researchers have found that typical privacy notices not only fail to help consumers make informed privacy decisions, but are largely ignored by them.[4-6] We highlight several factors as likely reasons for the ineffectiveness of today's privacy notices.

Conflating Requirements

Privacy notices serve different purposes for different stakeholders, resulting in a conflation of requirements (see Figure 1). Users might expect transparency about a company's data practices and privacy controls. For companies and service providers, however, privacy policies serve primarily to demonstrate compliance with legal and regulatory requirements, and to limit liability.[7] For them, privacy notices are often a necessity to ensure compliance with privacy notice requirements defined in laws and regulations, such as the California Online Privacy Protection Act (CalOPPA), the US Health Insurance Portability and Accountability Act (HIPAA), or Europe's General Data Protection Regulation (GDPR).

Regulators such as data protection authorities or the US Federal Trade Commission (FTC), on the other hand, leverage companies' privacy policies as one way to assess and enforce regulatory compliance. Furthermore, if a company is found in violation of its own privacy policy, it provides regulators with a basis to bring enforcement actions against the company.

In practice, this focus on legal and regulatory compliance results in privacy policies playing an essential role in the interaction between companies and regulators, while the users' need for transparency and control is neglected. Privacy notices often take the shape of long privacy policies or terms of service that require college-level reading skills.[8] Those policies are necessarily complex because the respective laws, regulations, and business practices are complex.[5] Further, privacy policies might be purposefully vague to avoid limiting potential future uses of collected data.[9] This conflation of requirements is particularly evident in the trend of large companies posting a single privacy policy for a diverse portfolio of services. Concentrating privacy-related information in a single document facilitates internal and external compliance assessment, but the described data practices are typically too broad for users to learn what information a specific service collects or how information provided to one service will be used by the company's other services. Privacy notices that are complex, abstract, or vague might meet the letter of the law, but they don't provide actual transparency to consumers.

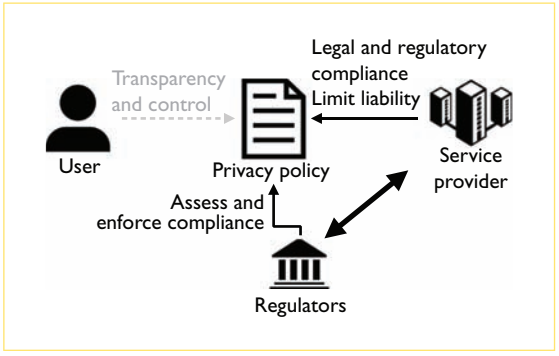

Figure 1. Privacy notices have different purposes for consumers, companies, and regulators. A predominant emphasis on legal and regulatory compliance by companies and regulators results in long and complex privacy policies and a neglect for the consumers' need for transparency and control.

Lacking Choices

Many privacy notices describe data practices but don't offer real choices. Using a website, app, or IoT device is interpreted as consent to the respective privacy policy and all its data practices — regardless of the user having seen or read them. Privacy policies typically contain only a few choices to opt out of individual practices, such as sharing data for marketing purposes. Users are effectively left with a take-it-or-leave-it choice — give up your data or go elsewhere. Users almost always grant consent if it's required, to receive the service they want.[5] Even when such notices create transparency about data practices, they don't afford consumers with the agency to act on the information in a meaningful way beyond completely forgoing interactions with a company.

High Burden, Low Utility

Reading privacy policies is extremely time consuming. In 2008, Aleecia McDonald and Lorrie Cranor estimated that reading the privacy policies for all the websites a person visits would take 244

hours per year.[10] With the increased adoption of mobile apps and smart devices, and the proliferation of data brokers, the number of privacy policies a person is subject to is likely much higher in 2017. Even if a user reads a privacy policy and deems it acceptable, most policies allow the company to change data practices and update their notices at any time. Furthermore, the neglect of usability concerns and the lack of choices mean that privacy notices are largely meaningless to consumers.[5] As a result, privacy policies are generally ignored and rarely read.

Decoupled Notices

Privacy notices are rarely integrated into a system. Instead, privacy policies are posted separately and thus decoupled from the user's interaction with the system. Websites only link to a privacy policy at the bottom of the page; mobile apps link to a privacy policy in the app store or in some app submenu; privacy policies for IoT devices are only available on the manufacturer's website. When privacy notices are decoupled from the system, users must seek them out proactively, which makes it even less likely that users read them.[11] Although sometimes the decoupling of privacy notices might be caused by technical constraints, it's also indicative of the split of responsibilities between designers and engineers who build the system, and lawyers and managers who are responsible for compliance and write the privacy policy.

Designing Effective Privacy Notices

These issues create an odd situation — in 2017, almost all services, apps, and devices have a privacy policy that describes data collection, use, and sharing practices, yet this information rarely guides users' decisions.

Rather than concluding that notice and choice has failed, we see the problem not in the quest for transparency and control but rather in how notice and choice is realized today. The need for more effective privacy notices and controls has been recognized by regulators and policy makers. Former FTC chairwoman Edith Ramirez notes that "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."[12] The Obama administration's proposed Consumer Privacy Bill of Rights[13] emphasizes the need for transparency and control, especially for data practices that are "not reasonable in light of context." The US National Privacy Research Strategy names transparency as one of the key challenges for privacy research.[14] Europe's GDPR, which will become effective in 2018, requires transparent and easily accessible notice and that requests for consent must be "clear, concise, and not unnecessarily disruptive."[15]

The challenge is to design privacy notices, controls, and consent mechanisms that are usable, useful, and yet unobtrusive. A first step toward addressing this challenge is realizing that privacy policies play an essential role for legal and regulatory compliance, but they're insufficient and unsuitable for informing users. An effective privacy notice or control mechanism must be as follows:

- *Relevant*. A privacy notice should provide information relevant to a user in the current transactional context to help them incorporate privacy considerations into their decision making.
- *Actionable*. Provided privacy information needs to be associated with options for user choice that are specific and explicit. Consent should be based on explicit expressions of choice and not be assumed based on use.
- *Understandable*. Privacy information and controls need to be understandable and easy to use. Privacy notices should engage users and inform their decision making, instead of overloading them with information.

Typical privacy policies don't meet those criteria. However, we argue that they don't have to. Rather than trying to make a document that's primarily intended for regulators and legal experts appealing to users, a clear distinction should be made between a privacy policy that serves to demonstrate legal and regulatory compliance, and privacy notices that are specifically designed for users and complement the privacy policy.

Understanding the System's Data Practices and Users

A prerequisite for effective notice design is an understanding of a system's data practices and information flows. Many organizations already conduct privacy impact assessments, risk assessments, and compliance checks as part of internal privacy or compliance programs. Such assessments

can provide a comprehensive overview of data collection, use, retention, and sharing practices involving personal and personally identifiable information. Such assessments should also surface notice requirements and the system's opportunities for providing notice and associated privacy choice options. The outcome of such analysis should be a comprehensive privacy policy, which can serve as the system's definitive (and legally binding) privacy notice, documenting regulatory compliance. A comprehensive privacy policy can further serve as the basis for designing additional user-centric privacy notices.

A key aspect in the analysis of information flows and data practices is to understand which user groups and audiences must be addressed by privacy notices.[7] While this might be trivial for websites, apps, or other systems used by individual users, wearables, smart cars, or smart home appliances might have multiple groups of users that must be considered. In addition to a primary user, such systems might have secondary users, who might be aware of a system but have limited control over it. Incidental users who might inadvertently and unwittingly become data subjects of a system's data collection should be considered as well. For example, a smart door lock might collect information about all family or household members, including guests;[16] cameras or drones might incidentally collect information about bystanders. Social media and mobile applications enable users to share information with and about others. In addition, specific regulatory requirements might apply to groups of protected users (such as children).

Providing Short, Specific Privacy Notices

Presenting information about all data practices of a company's services at once creates information overload and isn't an effective way to inform users. Instead, the privacy policy can be complemented with multiple short and specific privacy notices, as Figure 2 shows. Such privacy notices wouldn't be shown at the same time, but instead tailored to a specific transaction context, system feature, and audience, which means that each individual notice can focus on those data practices and choices that are relevant in the respective context, and can thus be much shorter and less disruptive. For example, a news website's practices regarding subscriber information — for example, whether contact information is shared — isn't relevant to a casual visitor until they decide to sign up for a subscription, at which point a short privacy notice can inform the visitor only about subscription-related data practices. Currently, casual visitors and (potential) subscribers have to sift through the same privacy policy and tease out the practices relevant to them.

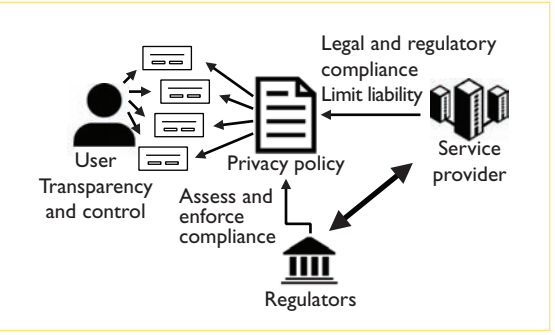

Figure 2. The privacy policy can be complemented with several short and specific privacy notices embedded well into a system's interaction flow. Such notices can combine relevant information with meaningful choices to make the notice actionable and obtain explicit and specific consent.

By focusing on data practices relevant in specific transaction contexts, privacy notices can not only be shortened, but can also integrate choice options relevant to those data practices, which makes the presented information actionable and user consent explicit.

Privacy notices that are short and specific require less interpretation and can be integrated into the user's interaction flow more easily without being overly disruptive. Individual users still receive information and choices for data practices that pertain to them, but through short and context-relevant notices rather than at once. They won't be confronted with data practices that are irrelevant for them, but still have the option to read the full privacy policy if they want. Creating and maintaining multiple privacy notices requires additional work, but the benefits are that users' privacy expectations can be better aligned with a system's data practices and that user consent is explicit, thus facilitating consumer trust by reducing opportunities for unexpected and surprising data practices.

Highlighting Unexpected Practices, Providing Details on Demand

Although short privacy notices can be more effective, there's a risk of overwhelming users with too many or repetitive privacy notices. This

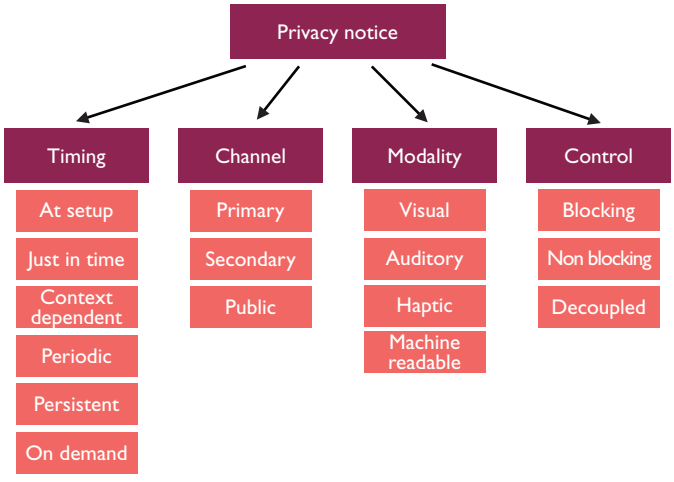

Figure 3. The design space for privacy notices[6] is defined by four main dimensions: when a notice is presented (timing), how the notice is delivered (channel), how information is conveyed (modality), and how choice options are integrated into the notice (control).

can result in habituation — users click notices away without considering them. After a few repetitions, the content of a warning literally doesn't register anymore in the user's brain.[17]

What to include in a privacy notice and when to show it can be prioritized based on associated privacy risks.[18] Data practices that are consistent with the transaction context and the users' expectations might not require immediate notice. However, practices that are likely unexpected or violate the transaction context should be highlighted.[11] For example, most people expect that a fitness tracker collects step and activity information — this is the device's main purpose. However, that collected activity data is automatically uploaded to the manufacturer's server and shared with other entities is less expected,[19] and users should be given appropriate notice and choice regarding those practices. User studies can help determine what practices are unexpected.

Short privacy notices can also provide companies with the opportunity to explain the purpose of unexpected data practices and build user trust. Short notices can further include links to additional information about described data practices, the full privacy policy, and additional privacy settings. By highlighting unexpected practices, a short notice can also get users to reflect on their privacy and point them toward more detailed explanations and settings. However, there's a risk of over-simplification. While long detailed policies aren't read, short notices might omit details important for certain users[20] and users might not continue on to more detailed notice versions.[21] Thus, it's crucial that the initial short notice constitutes an accurate reflection of the data practice.

Leveraging the Notice Design Space

Privacy notice design must consider a system's interaction opportunities and constraints. Aspects to consider are the system's interfaces, input and output modalities, and how different audiences can be reached or express privacy choices. Identifying such constraints and opportunities can facilitate creative interaction design for the notice and choice, when informed by an awareness of the main design dimensions of privacy notices and controls and existing solutions. In prior work,[6] we mapped the design space for privacy notices and identified four main dimensions each with multiple options (see Figure 3).

Timing. Timing, or when a privacy notice is shown, significantly impacts a notice's effectiveness. If shown at inopportune times, users will ignore or accept it without scrutiny. A notice should only be shown when the information is relevant to the transactional context, when the user is able to shift attention to it, and when the user isn't being loaded with other information and decisions.

Notice timing can support different purposes. Notices can be shown on initial use (at setup) or just in time to make users aware of a specific practice and obtain consent before it commences. Just-in-time notices are preferable, because they can be shown in the same transactional context as the data practice, which supports reasoning in the moment rather than providing information and choices before use. Just-in-time notices can also be more specific and shorter, because they pertain to a specific situation and don't have to leave room for diverse eventualities.

Other privacy notices aim to help users maintain awareness over time. Periodic notices remind users of an ongoing data practice in certain time intervals. They provide an opportunity to reaffirm user consent over time, especially when practices aren't visible. For example, iOS periodically reminds users of apps that access the phone's location in the background. Persistent privacy indicators are always shown when a data practice is active. Examples

are camera recording lights or location access indicators on smartphones.

Context-dependent and on-demand notices actively help users manage their privacy. Context-dependent notices can be triggered by certain aspects of the user's context, such as location (for example, when in proximity to a data-collecting sensor), who will have access to the information, or can warn about potentially unintended settings. Facebook, for example, warns users before accidentally posting publicly, depending on a user's posting habits. Users can seek out on-demand notices and controls anytime to learn about a system's data practices or manage privacy settings.

Channel. Privacy notices can be delivered through several channels. When the notice is shown on the same device that's collecting data, such as a smartphone or computer, this is the primary channel. When the notice is shown on a different device, such as when a fitness tracker's privacy notice is shown in its companion smartphone app or notices are delivered via email or text message, this is considered a secondary channel. Finally, a notice might require a public channel, such as a wall-mounted closed-circuit television (CCTV) camera notice, when users aren't known in advance. Although the primary channel is generally preferable for primary users, secondary or public channels might be more appropriate for secondary or incidental users, or when a device has limited output or input capabilities. Depending on the situation, the same device might serve as a primary, secondary, or public channel for different notices.

Modality. Most privacy notices are visual, occurring as text or icons. Many aspects of visual notices can affect their effectiveness, including color, font, white space, or combinations of icons and text. Privacy and data-sharing concepts can be difficult to represent as meaningful icons; therefore, combining icons with explanatory text is preferable. A device's LED lights can also be visual notices, for example, to indicate when a data practice is active.

Other modalities can also be leveraged for privacy notices. Sounds can serve as auditory notices. For example, camera shutter sounds are replicated on digital cameras to inform others when photos are being taken.[7] Haptic privacy notices, such as vibration, are also possible. Auditory and haptic notices face similar challenges as icons — if the sound or movement isn't familiar, the association with a data practice must be actively learned. However, they can serve to draw attention to a practice when visual attention isn't possible.

Machine-readable privacy notices and control APIs are a promising approach to aggregate privacy information and settings from multiple systems into a consistent view for the user. For instance, IoT devices that lack screens and input capabilities can broadcast their machine-readable privacy notices to smartphones of nearby users,[22] which then use other modalities for presentation to the user.

Control. An important aspect is the integration of user choices and consent into notices to make them actionable. Notice and choice need to be integrated, as delays between showing notice and users making choices can change the perception of the notice's content or even cancel its effect.[23]

A blocking notice forces users to interact with the notice. An example is a mobile permission request that blocks app use until the request has been allowed or denied. On the other hand, a nonblocking notice integrates choices without forcing interaction. For example, Facebook integrates controls for regulating a post's audience into the posting interface. The control is available but doesn't have to be used, and at the same time serves as a reminder of the user's current privacy settings. Decoupled notices don't integrate privacy controls into the user's interaction flow, but are available on demand. Examples include privacy dashboards that enable users to manage privacy settings in detail.

Privacy choice and settings must be specific to enable users to express their privacy preferences. Broad or coarse opt-outs could result in privacy settings that are either too open or too restrictive compared to the user's privacy preferences.

Evaluating Privacy Notices and Controls

Privacy notices and controls should be developed in a user-centered design process, which can be integrated into a system's overall interaction design and development.

If possible, privacy notices and controls should be evaluated in the context of the actual system. However, online and lab studies provide relatively inexpensive opportunities to evaluate

the usability of different notice and control variants. It's important to evaluate the individual notices and controls, as well as their combination and the system's overall privacy approach. The notices' effectiveness can be evaluated along multiple dimensions, such as user attention, comprehension, recall, and whether notices help users make informed choices.

The outlined design principles facilitate the development of privacy notices and controls tailored to the requirements, opportunities, and limitations of specific systems. Privacy notices and controls should become embedded in the user's interaction flow rather than being relegated to lengthy privacy policies and take-it-or-leave-it "choices." Many of the discussed design principles are well-established and have been studied extensively, yet we are still stuck in a world where companies' privacy transparency efforts often stop with posting a privacy policy.

A hurdle for the adoption of more effective privacy notice design is that companies seldom consider a system's privacy, engineering, and interaction design together. Often designers and engineers build the system or product, while the legal team is responsible for the privacy policy. While designers, engineers, executives, and other stakeholders might individually express an interest and willingness for protecting users' privacy better, they might struggle to integrate privacy into the overall product design and development process. Our hope is that our design space can ease interaction between different stakeholders by providing a joint taxonomy for the integration of privacy notices and controls. Establishing new interdisciplinary roles, such as privacy engineers, and creating interdisciplinary privacy teams within organizations can further help bridge such gaps.

However, facilitating such corporate changes on a wider scale also requires a further shift in public policy. The recognition by policy makers that privacy policies aren't effective needs to be turned into public efforts that encourage companies to embrace a more user-centric understanding of "providing notice." For instance, regulators should acknowledge the distinction between privacy policies for compliance and privacy notices and controls for users. Companies need guidance from regulators on how they can make privacy notices and controls more effective according to the described design principles, while remaining consistent with regulatory notice requirements. Otherwise uncertainty about legal and compliance implications of adopting innovative notice and control formats will continue to hinder their adoption. Furthermore, regulators should incentivize companies to evaluate the effectiveness of their privacy notices and controls. While larger companies, such as Apple, Facebook, or Google, are moving toward more user-friendly privacy notices and controls — often in response to consumer demand for better privacy protection — small- and medium-sized businesses might be reluctant to adopt novel concepts without further assurances and incentives.

Interestingly, privacy efforts by big companies are positively affecting how other companies approach privacy notice. For instance, both Apple and Google have moved to selective permission models in iOS and Android. Mobile apps have to request access to certain phone sensors and resources via a system dialog shown to users. Because these dialogs let users deny requests — an actual and specific choice — app developers increasingly see value in enhancing transparency around their permission requests. While apps can add purpose information to the system's permission dialogs, many apps provide additional explanations before and after permission requests to explain the rationale and implications of the data practice, thus integrating privacy notices and controls into their apps' interaction flows.

These developments are an indication that transparency and control can work, but that privacy policies are an ineffective realization of notice and choice. We argue that the key for making privacy notice and choice effective is to rethink the purpose of privacy notices. A privacy policy is a useful compliance tool but a terrible user interface. Privacy policies need to be complemented with privacy notices that are short, tailored to the transactional context, and integrate real choices. Such notices can provide users with timely, relevant, actionable, and understandable information in the context of an interaction.

References

1. J. Turow, M. Hennessy, and N. Draper, *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them up to Exploitation*, tech.

report, Annenberg School for Comm., Univ. of Pennsylvania, 2015.
2. A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and Human Behavior in the Age of Information," *Science*, vol. 347, no. 6221, 2015, pp. 509–514.
3. G. Greenleaf, "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories," *J. Law and Information*, vol. 23, no. 1, 2014, pp. 4–49.
4. L.F. Cranor, "Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice," *J. Telecomm. and High Technology Law*, vol. 10, 2012, pp. 273–307.
5. F. Cate, "The Limits of Notice and Choice," *IEEE Security & Privacy*, vol. 8, no. 2, 2010, pp. 59–62.
6. F. Schaub et al., "A Design Space for Effective Privacy Notices," *Proc. 11th Symp. Usable Security and Privacy*, 2015; www.usenix.org/conference/soups2015/proceedings/presentation/schaub.
7. R. Calo, "Against Notice Skepticism in Privacy (and Elsewhere)," *Notre Dame Law Rev.*, vol. 87, no. 3, 2012, pp. 1027–1072.
8. C. Jensen and C. Potts, "Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices," *Proc. Sigchi Conf. Human Factors in Computing Systems*, 2004, pp. 471–478.
9. J.R. Reidenberg et al., "Ambiguity in Privacy Policies and the Impact of Regulation," *J. Legal Studies*, vol. 45, no. 2, 2016, pp. S163–S190.
10. A.M. McDonald and L.F. Cranor, "The Cost of Reading Privacy Policies," *I/S: A J. or Law and Policy for the Information Society*, vol. 4, no. 3, 2008, pp. 540–565.
11. US Federal Trade Commission (FTC), "Internet of Things: Privacy & Security in a Connected World," *FTC Staff Report*, 2015; www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
12. E. Ramirez, "Privacy and the IoT: Navigating Policy Issues," *CES Opening Remarks*, FTC public statement, 2015; https://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf.
13. "Consumer Privacy Bill of Rights Act of 2015: Administration Discussion Draft," The White House, 2015; https://www.democraticmedia.org/sites/default/files/field/public/2015/draft_consumer_privacy_bill_of_rights_act.pdf.
14. "National Privacy Research Strategy," US National Science and Technology Council report, 2016; https://www.nitrd.gov/PUBS/NationalPrivacyResearchStrategy.pdf.
15. Regulation EU 2016/679: General Data Protection Regulation, European Parliament and Council, 2016; http://eur-lex.europa.eu/eli/reg/2016/679/oj.
16. B. Ur, J. Jung, and S. Schechter, "Intruders versus Intrusiveness: Teens' and Parents' Perspectives on Home-Entryway Surveillance," *Proc. Int'l Conf. Ubiquitous Computing*, 2014, pp. 129–139.
17. B. Anderson et al., "Users Aren't (Necessarily) Lazy: Using NeuroIS to Explain Habituation to Security Warnings," *Proc. Int'l Conf. Information Systems*, 2014; http://aisel.aisnet.org/icis2014/proceedings/ISSecurity/28.
18. A. Felt et al., "How to Ask for Permission," *Proc. Hot Topics in Security*, 2012; www.usenix.org/conference/hotsec12/workshop-program/presentation/felt.
19. J. Gluck et al., "How Short Is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices," *Proc. 12th Symp. Usable Security and Privacy*, 2016; www.usenix.org/conference/soups2016/technical-sessions/presentation/gluck.
20. H. Nissenbaum, "A Contextual Approach to Privacy Online," *Daedalus*, vol. 140, no. 4, 2011, pp. 32–48.
21. A.M. McDonald et al., "A Comparative Study of Online Privacy Policies and Formats," *Proc. Symp. Privacy Enhancing Technologies*, 2009, pp. 37–55.
22. M. Langheinrich, "A Privacy Awareness System for Ubiquitous Computing Environments," *Proc. Int'l Conf. Ubiquitous Computing*, 2002, pp. 237–245.
23. I. Adjerid et al., "Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency," *Proc. 9th Symp. Usable Security and Privacy*, 2013; http://dx.doi.org/10.1145/2501604.2501613.

Florian Schaub is an assistant professor in the School of Information at the University of Michigan. His research interests span privacy, human-computer interaction, mobile and ubiquitous computing, and the Internet of Things. Schaub has a doctoral degree in computer science from the University of Ulm. He's a member of ACM and the International Association of Privacy Professionals (IAPP). Contact him at fschaub@umich.edu.

Rebecca Balebako is an information scientist at RAND Corporation. Her research focuses on digital privacy and how we make decisions to share information. Her research relies on an understanding of computer science, human-computer interaction, and public policy. Balebako has a PhD in engineering and public policy from Carnegie Mellon University. Contact her at rebeccabalebako@gmail.com.

Lorrie Faith Cranor is a professor of computer science and of engineering and public policy at Carnegie Mellon University, where she's the director of the CyLab Usable Privacy and Security Laboratory (CUPS) and co-director of the MSIT-Privacy Engineering master's program. Her research focuses on online privacy and usable security. Cranor has a PhD in engineering and policy from Washington University in St. Louis. She's an IEEE Fellow and ACM Fellow. Contact her at lorrie@cmu.edu.