2018

Are Privacy Laws Deficient?

Woodrow Hartzog
Boston University School of Law

Are Privacy Laws Deficient?

Woodrow Hartzog

Introduction

Privacy law around the world is deficient because it ignores design.[6] Lawmakers have attempted to establish limits on the collection, use, and distribution of personal information. But they have largely overlooked the power of design. They have discounted the role that design plays in facilitating the conduct and harm privacy law is meant to prevent. Design pitches and picks privacy winners and losers, with people as data subjects and surveillance objects often on the losing side.

Bad Design

Bad design can undermine data protection by distorting user expectations and obscuring privacy harms. A study by the Pew Research Center found that most adults do not believe online service providers will keep their data private and secure. When the design of technology consistently violates users' expectations - and companies' promises - about how data will be shared, users are tempted to give up on privacy. Many privacy laws only protect people who have reasonable expectations of privacy. Design can alter those expectations and, in doing so, erode our cultural reserves of privacy. Exposure and vulnerability become the norm that is difficult to change.

Threats

In a world of social media, search engines, and the Internet of Things, most threats of privacy harm are not obvious, like the clear physical danger posed by faulty automobile airbags. Instead, they are incremental. Click by click, our privacy is slowly being eroded. While major privacy failures grab the headlines, the most significant corrosive force on our privacy is often barely noticeable, like death from a thousand cuts. And because most information privacy harms are small and dispersed among many people, courts and lawmakers fail to recognize them.

Regulation

Even when it is conceded that some regulation of disruptive new technologies might be necessary, regulation is delayed lest we impede innovation. Progress is at stake, and regulation would impede that progress. To the opponents of a legal response, regulations aimed at the design of technologies are too paternalistic. Government regulators are cast as ill suited to the task. Their expertise in technology is perceived as too limited, and opponents argue that much will be lost at the hands of regulators. They ask, "Why should government bureaucrats with no technical expertise tell tech companies how to design their products and services?" Imagine a regulator knowing better how to architect systems than the high-priced engineers at Apple. Nonsense, opponents say.

Lawmakers are in a difficult position. If courts and regulators prohibit too much collection, use, or disclosure of information, they will frustrate commerce, free expression, and our ability to freely interact with others. Overregulating design is dangerous. But so is ignoring it, and an important balance must be struck. Perhaps because of this delicate equilibrium and industry opposition, privacy law has been largely silent on the design of information technologies. This silence is regrettable.

[6] This is an extract version from Woodrow Hartzog's book *Privacy Blueprint: The Battle to Control the Design of New Technologies*, Harvard University Press (2018).

Design and Design Decisions

This is about the technology design decisions that affect our privacy. It's about going beyond scrutinizing what gets done with our personal information and confronting the designs that enable privacy violations. And it's about how everyone - companies, lawmakers, advocates, educators, and users - can contribute to and interact with the design of privacy-relevant technologies. At base, I am critiquing the structure of our technologies and the rules for that structure. I will explore why privacy is eroding and how the deck is being stacked to ensure privacy's degradation. What we have now is a blueprint for disclosure and exposure. But it doesn't have to be that way.

My argument boils down to one simple idea: the design of popular technologies is critical to privacy, and the law should take it more seriously. Law and policy makers can do so through recognition and guidance. Lawmakers and courts should better recognize how design shapes our privacy. Torts, contracts, consumer protection, and surveillance laws can all better reflect how design influences our perceptions and actions with respect to our information. Privacy law should guide the design of information technologies to protect our privacy. The law must set boundaries and goals for technological design. Doing so will improve our ability to trust others and interact in the world with an acceptable risk of exposure. But the law must be careful to broach design in a way that is flexible and not unduly constraining. In short, I'm arguing for a design agenda for privacy law.

Design and Privacy Laws

The design of information technologies is far more important than lawmakers have acknowledged. Technology design should be a fundamental component of privacy law, and this in turn will make it a key aspect of industry policy and practice. Now is the time to act. Many important technologies are still relatively new. Old technologies are being redesigned all the time. We can mitigate lock-in effects, which keep certain designs and technologies around long after they should have been replaced, and still right the ship. But so far we have no principled way to approach using law to encourage or mandate technology designs that protect our privacy. What we need is a blueprint for the next wave of privacy protections for users of digital products and services.

Blueprint for Privacy Law and Design

I develop such a legal blueprint - a framework to fill privacy law's design gap. It is designed to help legislators, regulators, judges, designers, executives, privacy advocates, and others in industry and civil society properly assess privacy design parameters and ideals for common information technologies. I focus on websites, apps, browsers, drones, malware, facial recognition technologies, and anything connected to the Internet that affects our privacy. While design concepts such as data architecture and auditing technologies are also critical for our privacy, this book is primarily about the design of technologies that are used by consumers and about the people whose privacy is at stake. Scrutiny for consumer-facing products and services is enough for one book.

A logical approach to design can answer pressing questions in the privacy debate. How far can governments go in crippling privacy-protective technologies like encryption? Should surveillance technologies be designed to be undetectable? What technical safeguards should companies be required to use to protect their users' data? What should be the limits of nudging, default settings, and structured choice on social media? Should companies be allowed to create manipulative software interfaces that encourage users to disclose information they otherwise would not? What kinds of obligations should be associated with the "wiring up" of everyday objects to be part of the Internet of Things?

This is also directed at exploring why design is so critical for our privacy in the modern age. Media scholar Marshall McLuhan is said to have asserted, "We shape our tools and thereafter our tools shape us." Design decisions establish power and authority in a given setting. They influence societal norms and expectations. When people say they use modern information technologies, what they are really doing is responding to the signals and options that the technology gives them. We can only click on the buttons that we are provided. Each design decision reflects an intent as to how an information technology is to function or be used.

At base, the design of information technologies can have as much impact on privacy as any tort, regulation, or statute regulating the collection, use, or disclosure of information. Design can be an incredible force to protect cherished privacy-related values like trust and autonomy. In some contexts, design is capable of protecting personal information more efficiently than laws targeting the actions of data collectors and controllers. Privacy design principles can protect people from exploitation. But design can also undermine our privacy, security, and safety; it can make us more vulnerable, less safe, and more transparent in ways that can disadvantage us.

Instead, if companies commit themselves to protecting privacy through design, they can earn the trust of users. Trust is the essential ingredient for commerce, intimacy, and any other avenue for human flourishing that requires other people. So if we want to improve commerce, our relationships, and our search for self, we need better privacy design.

This is for anyone interested in privacy, technology, and policy. While the blueprint I develop in this book is primarily focused on law and policy, it is meant to be useful to executives, designers, advocates, students, and anyone interested in the future of privacy and technology. We all have a role to play in the design of information technologies. For example, companies that seek to earn user trust might benefit from the blueprint's user-centered approach to design parameters and the way it leverages concepts like transaction costs and mental models that shape user expectations. Privacy advocates can take advantage of concepts developed in this book like "obscurity lurches" and "abusive design" to rebut common myths surrounding value-neutral technologies and the misguided notion that there is no privacy in public. Advocates can use the blueprint to find common ground with companies and governments to help create international standards and detailed guidelines.

Conclusion

Finally, we users can educate ourselves on how design affects our privacy. The companies asking us to trust them with our data are responsible for protecting our privacy and security, but there are also things we can do to mitigate the harm of design and use it for good. When we are mindful of design, we can mitigate the harm from confusing and manipulative user interfaces and adverse defaults. We can also proactively obscure ourselves or our data from surveillance from search technologies. We can work with companies to protect our information from hackers. We can demand better. And if push comes to shove, we can fight back with the help of the law. If we all work together on design, better information technologies can be created and used for the benefit of all.

A design agenda has great value. It can redirect some of the focus of privacy law from costly ex post facto remedies for limited categories of information to broadly effective ex ante protection for the full slate of privacy interests in personal information. It can also provide an additional perspective for companies seeking to earn people's trust. It can even be an educational tool for all who care about their privacy and want to know what to look for in the design of the devices they use. Most important, privacy law's blueprint will help us control information technologies before they control us.

Woodrow Hartzog
Professor of Law and Computer Science
School of Law & College of Computer and Information Science, Northwestern University
Author, *Privacy Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press, 2018)

IDPP

International journal for the
Data Protection Officer
Privacy Officer
Privacy Counsel

Contact
Subscriptions and submissions should contact the
International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel at:

lex@mydistillex.com
www.idpp.info

IDPP

International journal for the

Data Protection Officer

Privacy Officer

Privacy Counsel

JOURNAL ADDRESSES

Personal data | Privacy | Data protection | Law, regulation and caselaw | The new DPO profession | Compliance | Independence and conflict | Resources | Records | GDPR | Ethics | Security incidents and notifications | Breach notification | Pre-problem solving | PbD/DPbD | Audits and assessment | Education, training and programmes | Solutions and systems | Resource update review |

ISSUE INCLUDES

Court of Appeal Confirms First Successful UK Class Action for Data Breach
Miriam Everett and Lucy McAlister, Herbert Smith Freehills

The Implementation of Administrative Fines Under the General Data Protection Regulation from the German Perspective
Prof. Dr. Heinrich Amadeus Wolff, Universität Bayreuth

Understanding Cyber Insurance
Judy Selby, Judy Selby Consulting LLC

Comment on Tim Cook Brussels Speech
Laure Landes-Gronowski, Agil'IT

2018 VOLUME 2 ISSUE 11

CHIEF OPERATING OFFICER & EVP
GDPR ASSOCIATES
DATA PRIVACY & INFORMATION SECURITY OFFICER
JOHN LEWIS
DIRECTOR OF GROUP DATA PROTECTION
HOMESERVE
DEPUTY DATA PROTECTION OFFICER
MONZO