WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES, (2018)

Cambridge, Massachusetts, 2018
Harvard University Press
ISBN: 9780674976009
Price: #35.00 Hardcover
Page Length: 366 pages

Keywords: Privacy Law, Data Privacy

Reviewed by Kelly Wong
Journal of High Technology Law
Suffolk University Law School

---

**Privacy's Blueprint: Should the Law Regulate Technology Design to Protect Consumers?**

*"There are many jokes about whether anyone reads privacy policies, but these jokes rest on the undeniable truth that meaningful control over information is almost impossible to scale."*[1]

**Introduction**

Woodrow Hartzog promulgates an argument for an increased focus on design in privacy law in his new book, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* ("Privacy's Blueprint"). Hartzog argues that the current privacy regulatory framework of adherence to the Fair Information Practices (FIPs), which implements the "consent and notice" structure, is insufficient in protecting consumers and operates as a mere formality. Further, the author highlights that the "consent and notice" structure gives consumers an illusion of control over their personal information and places the burden on them to prove any tangible harm from an infringement of their data. In response, Hartzog proposes that there should be a design agenda embedded in privacy law to place the burden on companies to create safe technologies due to

[1] Woodrow Hartzog, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES, 15 (2018)

design's power in influencing how humans make decisions in disclosing their information. To illustrate this power, he discusses that the design of a platform such as the language, buttons, and default settings manipulate humans into oversharing information. To protect humans from over disclosure, his design agenda which he calls a "blueprint" is to identify the values affected by design, create boundaries to foster those values, and implement legal tools for the enforcement of those standards.

Hartzog's book provides a novel and nuanced perspective on how data privacy should be regulated given consumers increasing reliance and use on technology. Overall, the purpose of this book review will be to analyze Hartzog's arguments and examine whether his idea of a design agenda will be valuable to data regulation.

**About the Author**

Woodrow Hartzog currently holds a position at Northeastern University School of Law as well as an appointment at Northeastern's College of Computer and Information Science.[2] At the College of Computer and Information Science, Hartzog teaches privacy and data protection.[3] Hartzog has earned a J.D. degree from Samford University, an LLM in intellectual property from George Washington University, and a PHD in mass communication from the University of North Carolina at Chapel Hill.[4] Throughout his career, Hartzog has been published in multiple law journals, and national periodicals such as The Guardian, BBC, CNN, and The Atlantic.[5] Notably, Hartzog's expertise in data privacy has led him to testify twice before Congress on data

[2] See *Faculty Directory*, *Woodrow Hartzog*, NORTHEASTERN UNIVERSITY SCHOOL OF LAW (2018), https://www.northeastern.edu/law/faculty/directory/hartzog.html (providing a biography of Hartzog's career).
[3] *See id.*
[4] *See id.*
[5] *See id.*

protection.[6] Prior to teaching, Hartzog worked as a trademark attorney for the US Patent and Trademark Office and clerked for the Electronic Privacy Information Center.[7]

**About Privacy's Blueprint**

The premise of Privacy's Blueprint is to address the faults with the Fair Information Practices as the sole guide for data privacy and regulation, and to propose the implementation of a design agenda into this area of law. Hartzog introduces the reader to a real-life example of how technology has failed us with respect to privacy through the unfortunate circumstance that fell upon Bobbi Duncan. Bobbi Duncan attempted to hide her sexuality from her father through adjusting her privacy settings on Facebook. However, the platform failed her when she was added to a Facebook group called "UT's Queer Chorus" and the post was made available to all her Facebook friends, including her father. This led to an estrangement with her father. The lack of notification asking Bobbi whether she wanted her addition to the group to be publicly posted to all her friends was the fallacy of the design.

Hartzog's book consists of an introduction and is divided into three parts. Hartzog argues in the introduction that lawmakers should take the design of secure technology more seriously to ensure our privacy is protected. In the introduction, he illustrates the shortcomings of design regulation by discussing the exploitation of Snapchat by hackers. He reveals that the pictures taken on Snapchat were accessible by third-party applications although its privacy terms prohibited this kind of access. The hackers took these pictures taken by users and posted them online for the world to see. Snapchat blamed its users for using an insecure application; however, Hartzog argues that Snapchat is the one to blame for not designing its software securely and

[6] *See id.*
[7] *See id.*

merely stating in its terms that third party access is prohibited. Hartzog uses this anecdote to stress his argument that the notice and consent model of using boilerplate terms of use contracts are insufficient to protect consumers, and what is needed is secure design regulation.

Part I of *Privacy's Blueprint* consists of two chapters which address why design should be taken seriously in the law. The first chapter addresses the fact that privacy design is entrenched in so much of our technology such as phones, laptops, and drones. The author argues that the designer's values and motivations are embedded in the design of technologies and are communicated through transaction costs and signals. Hartzog argues that the combination of transactions and signals determine how we share personal data and how often consumers do it, so technology should be designed with the consumer's best interest. The author argues that design is powerful due to its ability to control how a consumer communicates with the technology and should not be designed to manipulate a user into oversharing their personal information. The second chapter discusses that the FIPs' "notice and consent" model gives consumers a false impression of control and is not sufficient to protect consumers' privacy. The author argues that the notice or choice given to consumers in the form of boilerplate contracts cannot render meaningful consent since consumers do not actually read these contracts prior to clicking accept. Thus, this leads to companies being able to legally insert provisions allowing them to use, collect, and share in any manner that they so choose.

In Part II of *Privacy's Blueprint*, the author sets out his design agenda for privacy law. In Chapter 3, he discusses the values which he believes should be rooted in design privacy law to provide a safe area for consumers to share information. He lists obscurity, trust, and autonomy and discusses them in turn. These values are highlighted since trust enables consumers to form positive relationships and obscurity would allow consumer personal information to be safe and

far from reach from those unauthorized to possess it. As long as trust and obscurity are reinforced, autonomy allows consumers the freedom to make disclosures knowing their information is safe.

Chapter 4 outlines standards and boundaries for the implementation of safe design. Hartzog argues that there needs to be a standards-based framework for privacy design and that the FIPs should be used to articulate the goals of privacy design. Hartzog looks to product safety law and consumer protection law as a model for privacy design. Deceptive design, abusive design, and dangerous design should be the boundaries for a design agenda Hartzog argues. Chapter 5 discusses the tools that lawmakers and regulators can use to apply privacy design into privacy law. The first tool that he addresses is soft responses which are meant to educate and incentivize safe design. If soft responses are not enough, moderate responses should be used which place obligations to designers to safely design technology. Lastly, robust responses are to be used only when necessary and they impose tort liability or prohibitions for unsafe design.

Part III discusses the application of *Privacy's Blueprint* to today's technologies and software. Chapter 6 addresses how a design agenda would be applied to social media. Chapter 7 applies the design agenda to hide and seek technologies such as drones, while Chapter 8 applies the agenda to the Internet of Things (IOT). His application of the design agenda for social media, hide and seek technologies, and the IOT are nuanced and incorporate the tools he discussed in Part II. For example, in the context of social media, where people are bombarded with clickwrap and browsewrap agreements, Hartzog argues for a more holistic view on these types of contracts. He argues that courts should supplement the terms of use contract with the user interface or privacy settings that are integrated into the contract  rather than relying solely on the terms of use contract.

**Analysis of *Privacy's Blueprint***

*Privacy's Blueprint* proposes an innovative approach to data privacy law through the regulation of secure design in technologies and software. Hartzog is correct in opining that privacy law today is static: it focuses too much on the manner in which data is collected; the illusion of consumer consent; and the need for actual harms to obtain remedies for the use, collection, and sharing of data. Hartzog alternatively asserts lawyers and regulators should look towards other areas of law that regulate the design of products to supplement the current data privacy regime of "notice and consent." For example, Hartzog articulates that other areas of law embrace values that minimize harm through safe design in architecture, cars, and medical devices. The FDA and the National Highway Traffic Safety Administration have standards that must be followed in order for medical devices and cars to enter the market. Lastly, his argument for the inclusion of design agenda into privacy law is not a far-off reality. Hartzog points to the Federal Trade Commission and the European Data Protection authorities for support. He states that these two entities have already started to incorporate regulating design into data security, user interfaces, surveillance technologies, and systems that process and store personal information.

Hartzog's book *Privacy's Blueprint* is laden of real life examples of persons affected by the fallacies of the design of technology. This method allows him to educate readers on the implications of insecure design and the gaps in the current privacy law regime in a relatable manner. The concepts of data privacy can be difficult to comprehend and daunting to the unlearned reader, yet Hartzog well organizes his book and uses vernacular language to make it easier to grasp. Hartzog aims to make his argument understandable by all readers through thorough and detailed explanations, however, at times it comes off a bit redundant. Although the

author is stressing the importance of a design agenda, he does not concede that it is the only answer to data privacy. His awareness that data design is not the end all solution legitimizes his argument since he is mindful of its potential difficulties in being applied to certain technologies, such as IOT. Hartzog's application of various sources into his book such as case law and different law review journals signals that he carefully thought and analyzed different ideas encompassing the regulation of privacy law before asserting his design agenda.

**Evaluation of *Privacy's Blueprint***

Hartzog's Privacy Blueprint is a valuable contribution to the field of data privacy law due to its unique and well thought out approach to mitigating the pitfalls that the current regime suffers from. The ideas that emanate from this book are important since it introduces the reader to the increased risks of data breach and data collection from surveillance. Thus, lawyers and regulators should read this book to understand and initiate dialogue on improving and amending data privacy law.

In the wake of multiple data breaches such as the Equifax breach, this book is significant since it addresses an innovative solution that places the burden on the entity that is most likely to prevent these types of harms. It is paramount that an entity with full information on its software and technologies use transaction costs to inculcate the values of trust, autonomy, and obscurity into its design so that their users are protected. It is unreasonable to continue the practice of poor design and placing the risk on consumers simply because they consented to a terms of use contract that they didn't even read.

**Conclusion**

Prior to reading *Privacy's Blueprint*, I didn't fully understand the importance of data privacy laws and ignorantly thought that they were doing an effective job. However, this book

really convinced me that it is not advisable to continue using the laws in place and we need change. Just recently, Marriot Hotels had a breach that affected 500 million users. This should not be the new normal; these companies should be held accountable for implementing poor design and allowing these types of invasions to our privacy. It is obvious that the current laws in place don't incentivize designers and companies to protect our data and the laws should begin at the onset of the process. Although the design agenda is a rather new idea in the field of data privacy, it should be taken seriously; and implemented in software and technology just as it is in other areas of the law like architecture and product design. I recommend that anyone concerned with their personal information to read this book to fully understand how our data is being regulated and what needs to be done to maximize its security.