scripted

Volume 17, Issue 1, January 2020

Book review: *Privacy's Blueprint: The Battle to Control the Design of New Technologies*

Woodrow Hartzog
Cambridge, Massachusetts: Harvard University Press, 2018. 384 pages.
ISBN 9780674976009. £25.95

*Reviewed by Wenlong Li**

DOI: 10.2966/scrip.170120.160

* PhD researcher, University of Edinburgh, wenlong.li@ed.ac.uk.

At a critical time when the idea of Privacy by Design (PbD) is on the rise, many readers would, like me, be attracted by this book, *Privacy's Blueprint* ("Blueprint" hereinafter), provisionally assuming it to be a timely survey of PbD's recent development. The drawer of this Blueprint, Woodrow Hartzog, in fact commits to depict a self-sustaining world of ethical design, in parallel with the mainstream discourse. In his book, Hartzog does not intend to cover technological endeavours to protect privacy, e.g. architectural design or auditing technologies; nor does *Blueprint* relate to privacy-enhancing technologies (PETs). In contrast to what blueprint literally means (as in technical drawing, architectural plan or engineering design), this book is essentially about a legal proposition much more comprehensive than what the principle of PbD could entail.

As a professor of law and computer science at Northeastern University in the US, Hartzog is more interested in the role of law (or more precisely, what he categorises as privacy law) in addressing multidimensional implications of technological design. In addition to his skilled legal analysis, the author's expertise in mass communication and computer science is also evident throughout the book, making its content diverse, inter-disciplinary and highly readable. Readers may find some of the arguments in this book familiar as they are readapted from Hartzog's numerous articles published earlier.

Blueprint is neatly divided into three parts. Hartzog starts by challenging several popular claims that underpin a hands-off, self-regulatory approach to technological design, e.g. "we should regulate uses of technology, not the technology itself" (p. 5). Drawing upon knowledge of behavioural economics and cognitive psychology, the author insightfully reveals three major characteristics of design – i.e. design is power-conferring, political and value-laden - to refute those claims. In connection to his objection against self-regulation, Hartzog points to the failure of privacy law to address problems arising from technologies designed to exploit our vulnerabilities. According to the author, privacy law here

is not narrowly interpreted as US privacy torts and legislation, but refers generally to modern privacy law across the globe. (pp. 56-58) Apart from the Fair Information Practice Principles (FIPPs), Hartzog somehow recognises "Do Not Harm" and "Do Not Lie" as components of privacy law, two principles ostensibly mimicking the US "Do Not Track" rhetoric.

In response to design-related problems, Hartzog proposes a soft, co-regulatory framework, what he calls *Privacy's Blueprint*. This legal framework is meant to remedy the failure of privacy law by articulating goals, setting up boundaries and issuing guidelines. While Hartzog calls for all stakeholders' actions including companies, lawmakers, advocates, educators and users, *Blueprint* has its prime focus on the role of privacy law in duly recognising and addressing issues caused by technological design. His starting point is that "privacy law is deficient because it ignores design". (p.5)

The second part of this book respectively introduces *Blueprint*'s values, boundaries and toolkits. First, Hartzog's identification of three core values underpinning his framework is concise, clear and to the point. Whereas a *trust* relationship between consumers and businesses is increasingly important for protecting our personal information, *obscurity* is sometimes needed when such a relationship is broken. A third value, *autonomy*, is somehow related to the previous both: as an underlying design value, it helps sustain our ability to trust and enable obscurity/obfuscation when necessary. In together, these values minutely represent a modern conception of privacy

To put forward "the boundaries for lawmakers to set" (p.16), Hartzog somehow turns to legal principles outside privacy law, suggesting that those developed in areas like product safety and consumer protection are transferable. It appears, however, that rules against deceptive, abusive and dangerous designs are more concerned with the legal boundaries of design than safeguarding specific values identified above. Instead of outlining the contours of *Blueprint*,

Hartzog provides for an overview of rules that may have an impact on design in general (hence broader than protection of privacy). It may indeed be easier in the context of US law that the concept of privacy relates to consumer protection, as manifested by the frequently used term "consumer privacy". Still, how other rules considered as components of *Blueprint*, such as product safety, add much to privacy law and sustain the values identified is less expressed. That said, the consideration of safety issues is pertinent and crucial to the quest for better, ethical designs and it cannot be too careful keeping alert of emerging technologies that have entered into our lives and interact with us on a daily basis.

Blueprint is then substantiated by a delicate set of legal tools, put into three categories in terms of their level of intervention and effects (soft, moderate and robust). A few innovative ideas about design regulation have been raised, such as "promissory design". As Hartzog notes, privacy settings can be seen as code-based promises in addition to Privacy Policies, and the courts often fail to recognise this important yet disguised technical layer. (p.171)

In the last part of the book, *Blueprint* is applied to various types of consumer-facing technologies and Hartzog explains, with concrete examples, how his framework can be proportionally used. For instance, the problems of social media lie mainly with default settings, infrastructure and interfaces designed for information oversharing. His proposal of *interactive* privacy management represents a promising solution to many of the lengthy, incomprehensible Privacy Policies. The following coverage of online harassment and abuse appears, again, a bit divergent from the book's focus on privacy, even when the term is broadly interpreted.

Further, what Hartzog portrays as "seek and hide technologies" covers a broad range of digital tools; they can be largely put into two conflicting parts, based on the concept of transaction cost. Whereas search engines, browsers and drones have the potential to greatly reduce search costs (one important facet of

transaction cost), encryption, deletion tools and spyware would do quite the opposite, i.e. increasing search costs or enhancing obscurity. Hartzog's emphasis on the protection of hiding technologies and his call for less efficient seeking technologies seem to prioritise obscurity over trust, yet a careful response to his balancing between obscurity and transparency deserves more space than this review can provide.

Last, *Blueprint* is implemented to the Internet of Things (IoT), one of the most cutting-edge technologies creeping into our private and public lives. It is important that Hartzog draws a distinction between computers and more innovative "things" in terms of their security vulnerabilities. When technology companies are keen on "wiring up" every possible object surrounding our lives, Hartzog's warnings of the "hidden and dispersed risks" (p.262), as well as the need to cut off continuous connectivity at certain point, are visionary.

In contrast to my initial motive to read this book, that is, to inquire how Hartzog's theory would add to the developing idea of PbD, and in particular, an altered version – Data Protection by Design (DPbD) embodied in the EU General Data Protection Regulation, Hartzog in fact takes a different approach, primarily by drawing lessons from several areas of law other than privacy. He frames his theory as a contrasting path towards ethical, privacy-friendly design, but acknowledges at the same time that *Blueprint* is in essence "in the same spirit as PbD" (p.12). Hartzog argues that *Blueprint* is narrow than PbD because the former does not concern the organisational aspect of design. In contrast, it may be reasonable to contend that *Blueprint*, by incorporating rules other than privacy, is wider than PbD as well.

Hartzog has insightfully provided for a comprehensive picture of interplay between privacy, design and law. With a view to "taking design more seriously" (p.227), the author has made his point clear that legislators and policy makers should have better addressed design decisions through *recognition* and

guidance. While recommendations about guidance throughout the book are mostly commendable, I am somewhat sceptical of the author's claim that privacy law has not duly recognised the importance of design. This scepticism is closely related to another one concerning the scope of "privacy law" as referred to in *Blueprint.* If interpreted broadly, modern privacy law would incorporate latest developments across the globe. In the case of GDPR, for instance, the author's argument that privacy law ignores design instantly become less fact-based. Moreover, consumer protection and product safety rules examined in this book are all extendable to problems caused by the design of consumer-facing technologies. If considered as part of privacy law, as suggested by the author, these principles would represent due recognition and guarantee of better, ethical and privacy-friendly designs. Should the notion of privacy law be perceived narrowly, referring only to the FIPPs augmented by latest developments e.g. PbD, then the author's claim for more explicit recognition of consumer protection and product safety principles in privacy law itself cannot be reasonably deduced from the book's major conclusions.

Having said all the above, the concerns expressed do not refute *Blueprint* as an original, well-written and informative contribution to contemporary debates about technological design and regulation. With enthusiasm, I would recommend this book to designers seeking for a global view of legal rules influencing the design process, legal scholars and practitioners in search of knowledge about several intertwined areas of law, and other readers who have a general interest in the interplay between technology, law and design.