Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things

Aurelia Tamò-Larrieux

Reviewed by: Methinee Suwannakit

This is a pre-print version of a book review published in International Data Privacy Law, 2019
https://doi.org/10.1093/idpl/ipz013

The Internet of Things (IoT) literally means things or objects that connect to each other via the internet. The Organization for Economic Co-operation and Development (OECD) Digital Outlook 2015 report defines IoT as 'all devices and objects whose state can be altered via the Internet, with or without the active involvement of individuals'.[1] As a matter of fact, IoT market is growing rapidly. International Data Corporation (IDC) predicts that worldwide technology spending on the IoT will reach 1.2 trillion dollars in 2022.[2] Although connected devices or smart devices placed in offices or homes offer convenience and comfort to users, IoT raises several concerns with user's privacy and data protection. Moreover, while users benefit from smart wearable devices for tracking their physical activities, they do not want to share their health-related data with other third parties. Responding to privacy and data protection concerns, policymakers are therefore keen to develop legal frameworks to protect personal data in the smart digital environment. However, laws alone cannot lead to changes in practice because data protection stems from the design of technology. In regards with a relationship between law and technology, Lessig[3] argues that regulations of behaviour in cyberspace impose through code (technology). Thus, changing the 'architecture' of technology could be effective in altering a particular behaviour. Law also has an important role in changing the 'architecture' of technology by requiring an architect to modify his or her 'architecture'. Similar to this idea, the new notion of 'data protection by design', codified in Article 25(1) of the EU General Data Protection Regulation (GDPR), requires a controller to ensure that data protection is implemented into the design of new products both 'at the time of the determination of the means for processing' and 'at the time of the processing itself'. As a result, each smart product is required to design effective technical protection in the first place to prevent every possible way of data breach. Nevertheless, despite introducing the new concept of data protection by design, GDPR does not provide any prescription on how to apply the concept in practice. In other words, it does not clarify on how the architecture of technology should be designed. Accordingly, practical guidance is needed to be developed.

In this book, Tamò-Larrieux provides a more concrete guidance and illuminates how to apply data protection by design, particularly in the IoT environment. The book contains two types of knowledge: law and engineering. Hence, it is suitable for both lawyers and engineers. The author believes that the key obstacles for creating practical methods for data protection are unfamiliarity of data protection principles of engineers and complexity of technical tools, which is inaccessible for policymakers or lawyers. Accordingly, she aims to bridge the gap between law and engineering disciplines in order to strengthen data protection by design. The main question in this book is 'how can technology protect privacy and how can policymakers harness the protection of privacy via technology?' (p 13)

[1] OECD, Digital Outlook, 2015, p 244.

[2] 'IDC Forecasts Worldwide Technology Spending on the Internet of Things to Reach $1.2 Trillion 2022' *IDC* (18 June 2018) <https://www.idc.com/getdoc.jsp?containerId=prUS43994118> accessed 15 January 2019.

[3] Lawrence Lessig, *Code, and Other Laws of Cyberspace* (Basic Books 1999).

From chapter one to six, the author sets out background information on a digitalized environment and examines various privacy ideas within the legal and engineering disciplines. In chapter three, the book discussed privacy rationales by taking different perspectives into account. Chapter four then introduces specific protection mechanisms in three IoT case studies; Radio Frequency Identification (RFID), smart energy architectures and smart wearable devices. The major strength of this book is that it can simplify the complex terminologies of technical tools and confusing legal principles in an understandable manner. For example, in chapter five, Tamò-Larrieux constructs a taxonomy of legal principles aligning with technical tools for data protection. In chapter six, she then describes the taxonomy of technical tools in an accessible way for lawyers, for instance, she explains cryptosystems and illustrates the basic function of encryption by giving a clear example and figure.

From chapter seven to nine, the author combines legal and engineering approaches and discusses how this interdisciplinary approach may apply in designing for a privacy-friendly IoT environment. Starting with chapter seven, Tamò-Larrieux maps the legal principles and technical tools throughout the life cycle of data. In this chapter, the readers will learn legal principles underpinning each phase of data life and be able to identify the technical tools concerned with each phase. Consequently, chapter seven is useful for creating a more specific data protection guideline in following chapters.

In essence, chapter eight provides regulations guidance for data controllers so as to implement data protection by design. In other words, chapter eight explains how to use technical tools for designing data protection to meet legal standards, such as the specific security measures in Article 32 of GDPR. This guidance is practical and valuable for all developers and engineers. Moreover, the merit of chapter eight is that it answers the question of how policymakers can harness the protection of privacy via technology. In this chapter, Tamò-Larrieux analyses similarities and differences among legal and technical rationales, before deliberating lessons learned for policymakers. The findings indicate that if legal and technical objectives are similar, the guidance will be more certain, for instance, when conceptualizing security and transparency issues. In contrast, if legal and technical approaches are different, the regulations and guidance will remain broad. In addition, the author explains the differences between the three functions of legislation, namely regulation as a constraint, enabler, or leveler. In this regard, when policymakers need to develop a strict and precise regulation, they should focus on aligning regulation with technical concepts. If policymakers want a less strict regulation, they should consider parallel or related approaches, draft a technology-neutral regulation and leave the concrete one to lower-level regulations or allowing self-regulations. In spite of this, an in-depth analysis of differing approaches, for example, conflicts between technical objectives in data processing and legal principles of purpose limitation and data minimization, needs to be further discussed.

In chapter nine, the author demonstrates how to apply technical tools complying with laws in the typical actions of a startup scenario. By giving a hypothetical case study, this chapter does help answer some practical questions that the readers may have in mind during the previous chapters. In addition, the author deliberates lessons learned for startups in the IoT. For example, she suggests that a starting point for designing data protection is an understanding of overall data flows, then, a developer should assess risks and prioritize actions in every phase of data life cycle. Although designing data protection is not a 'one size fits all' concept, generally the operations of startup in IoT is similar. Therefore, this chapter is also beneficial for designing data protection in other related settings.

Furthermore, in chapter ten, the author looks beyond the hypothetical scenarios and observes the challenges of implementing technical tools, such as economic obstacles and issues of interoperability, usability and design issues, challenged anonymity and issues of erasure and control. Tamò-Larrieux argues that some of these challenges can be overcome by laws. She highlights that the concept of data protection by design can strengthen the relationship between law and technology. In spite of an in-depth legal analysis, Tamò-Larrieux makes her argument clearly on how engineering guidelines should be developed. While other engineering guidelines predominantly focus on a security engineering mindset, the author establishes a holistic set of data protection engineering guidelines. This set of guidelines is a significant contribution as it can fill in the gap in the engineering literature.

Despite some limitations, this book is worth reading for everyone interested in the privacy field in general and data protection by design in particular. Tamò-Larrieux makes her book phenomenal by its friendly format for practitioners. She establishes some essential guidelines, which lawyers, engineers, and all stakeholders can use as a reference for designing data protection. Most importantly, policymakers can use this book and its interdisciplinary approach as an initial source for developing a better legal framework for the growing IoT environment.

Methinee Suwannakit

Doctoral Candidate, School of Law, University of Glasgow