Holistic Data Security: A Balanced Approach to Data and Privacy

The expansion of the data economy has raised a multitude of concerns that scholars worldwide are working towards overcoming. Given the divergent views on data in fields such as law, economics, and sociology, varying approaches to data governance have been suggested. However, regardless of the approach chosen, the multi-dimensional aspects of data should not be disregarded. This book incorporates various research viewpoints on data governance and introduces the innovative notion of "Holistic Data Security", which can offer fresh avenues for exploration by academics across diverse fields of study.

Keywords: *Privacy, Data Law, Data Security, Holistic Data Security*

Acknowledgement

This work received financial support from the Beijing Municipal Education Commission (Research Program *Research on the Model Construction and Scale Development of the Learning Environment in the Capital's Senior University in the Internet Era,* Grant No. AIDB231).

Author Information

Yao Lu, College of Humanities and Development Studies, China Agricultural University
https://orcid.org/0000-0001-9277-5732

How to cite this article:

Lu, Yao. "Holistic Data Security: A Balanced Approach to Data and Privacy". *Információs Társadalom* XXIII, no. 4 (2023): 102–105.
https://dx.doi.org/10.22503/inftars.XXIII.2023.4.7

Holistic Data Security: A Balanced Approach to Data and Privacy

Breached!: Why Data Security Law Fails and How to Improve it, by Daniel J. Solove and Woodrow Hartzog, New York: Oxford University Press, 2022, £22.99 (Hardcover), 256 pp., ISBN:9780190940553.

It is now considered that the world has fully entered the digital economy era, and the importance of data is self-evident in this new age. As a new production factor that drives the development of the digital economy and empowers social governance and technological innovation, data is as important as oil was to the second industrial revolution. Daniel J. Solove and Woodrow Hartzog bring us a book on how to improve the approach to data security in law. Daniel J. Solove is the John Marshall Harlan Research Professor of Law at the George Washington University Law School, while Woodrow Hartzog is a Professor of Law and Computer Science at Northeastern University School of Law and the Khoury College of Computer Sciences. In this book, the authors propose a different approach to the laws governing data security. It is important to note that this book focuses on data security in relation to personal data, and as such, the term "data" primarily refers to data related to personal information. In this book, the authors make an important point that differs from the point of view many other researchers: that data breaches are a product of systemic problems and that the law should focus on the entire data processing system and the participants in it, rather than just on the breaches, in what the authors call a "holistic approach" to data security law.

In the introduction to the book, the authors outline a broad set of principles that could help bring consistency to the relevant legal systems. Their argument rests on one overarching point: In order to improve the rules for protecting personal information, policymakers need to counter-intuitively shift the focus of the law beyond just the data breaches themselves. The current data security law is effectively a "breach law" that overemphasizes the breach itself and ignores the other actors and factors that led to the breach. The authors offer an alternative, broader vision of data security policy in three areas: accountability, redress, and technical design.

The first part of the book focuses on the challenges facing data security and how the law does not adequately address these challenges. In Chapter 2, the authors briefly review the history of data security in this century and list nine common reasons for data breaches (big lapses in oversight, human error, hacking of vendors, too much data being kept and stored together, lost or stolen devices, data not encrypted, phishing, failure to learn from the lessons of previous data breaches, careless simple mistakes), from which it is easy to see how individuals, companies, and governments alike can fall victim to data breaches. In Chapter 3, the authors divide current data security laws into three categories (Breach Notification Laws, Security Safeguards Laws, Private Litigation), and then describe and analyse their strengths and weaknesses in detail. However, by revealing the imperfections of the existing law here, the authors are not advocating abandoning the path of legal regulation; quite

the contrary, they recognize that the law can play a large role in improving data security, but that it requires a significant shift in its focus and means of adjustment.

After presenting the background to the privacy–data use problem, the authors propose a different approach to data security in the second and core part of the book, which they call "holistic data security". In Chapters 4 to 8, the authors introduce the core values of "holistic data security", the relationship between privacy and security, and propose the concepts of "Maximizing Data Minimization" and "Data Mapping" as an attempt to bridge the reality of data security in the privacy–data use divide. In addition to the fragmentation between privacy and the need for data, human error plays an important role in most data intrusions. Therefore, the authors argue that the law could achieve the goal of ensuring data security through direct restrictions or by using a mix of incentives and disincentives, and suggest that this could be achieved by "Changing the Default Settings", "Promoting Mutual Trust", "Encouraging Balanced Security Measures" and "Sending Sensible Signals" to achieve good law and good governance in the field of data. Finally, the authors summarize the book in Chapter 9 and come up with some detailed revisions for their data method, such as "The law should recognize that data security is a systemic and societal problem, one where the effects of one's poor security can affect many others".

As a Chinese scholar, I would like to emphasize the value of this book to the readers of this article from the perspective of China's law. A series of legal issues concerning data have been widely discussed in this book, and controversies exist on how to define the connotation and extension of data, the attribution of data, and the attributes of rights and the content of those rights. Among these, determination and legalization of the attribution of data rights is the legal basis and prerequisite for the construction of a unified data market, but this has not been clearly stipulated in China's current civil legislation. Article 127 of the Civil Code of the People's Republic of China rather provides: "Where there are laws particularly providing for the protection of data and online virtual assets, such provisions shall be followed". From the content of this article, the current Civil Code only provides for the protection of data in principle, and establishes the principle of data protection in accordance with the law at the level of the basic civil law. The reason for this is that the process of codification of the Civil Code remains controversial, and there is still no consensus yet on the relevant theories, at home or abroad, so it is not appropriate to make more institutional arrangements for data in the various parts of the Civil Code at this time; at the same time, in terms of legislative techniques, the positioning and chapter structure of the General Provisions cannot provide systematic and detailed provisions for this series of systems. Therefore, the current Civil Code can only provide for the protection of data in principle under the General Provisions, with a view to reaching a consensus in practice and filling the institutional gaps in the future based on the recommendations from subsequent academic and practical circles. The data security issues discussed by the authors in this book actually involve not only the concept of data or privacy, but also a debate on property rights in economics. In China and even in some civil law countries, scholars have tended to focus on the "ownership of data" due to research inertia, resulting in data security laws effectively becoming "violation laws". At the same time, treating data rights as ownership rights could

make it difficult to address the issues of data monopoly and personal data rights, resulting in a fragmentation of privacy, property rights and data. In China, most of the literature on data rights is vague in terms of the concept of data, and it is not possible to effectively conduct dialogue between different disciplines; the research method is singular, and there are few papers that have conducted comprehensive, multi-path and interdisciplinary research on data rights, and it remains difficult to grasp the "pain points" of data rights from a global perspective. As a result, the current research is not deep enough, and the relevance and practicability of the ideas proposed so far are weak. The reason for these problems is that it is difficult for scholars to see past the property rights perspective of "data". Nevertheless, there is a clear need for Chinese scholars to conduct research on data rights. The institutional advantages of data rights include the potential to stop disputes, correct market failures, establish an effective market for data circulation and utilization, and realize the concept of "constant production before constant mind" in the field of data. Further, the more far-reaching significance of resolving the data rights issue is to realize the self-determination of personal information through the domination of data property rights, and to guarantee people's autonomy and security in building their digital living space in the information society.

This book presents a comprehensive and vivid picture of data security with a wealth of detailed case studies and a down-to-earth approach to writing, allowing a glimpse of future rights beyond data rights in rem. At the same time, this book can assist scholars in developing a pluralistic perspective on data and may also be advantageous for countries in regard to assisting their data legislation. From this point of view, this book would be helpful for the improvement of China's Civil Code and Data Security Law, and this help would not only be applicable in China, I believe that scholars in other countries could also benefit from this book. Notably, this book is not about cybersecurity in the broadest sense; rather, its focus is on data security. The authors recognize that data security laws are currently in an awkward space between cybersecurity and privacy, and are unable to balance these cybersecurity and privacy aspects. At the same time, the authors keenly observe the nature of data security and propose a new research paradigm. The dichotomy of "data and privacy" proposed by the authors is, however, questionable, as it does not strike a good balance between the individual, the enterprise, and the public. However, the "holistic data security" approach proposed in this book is actually an approach that focuses not only on data security as a whole, but also on scenarios and details, which will inspire readers interested in privacy and data, data governance and the digital society.

References

Solove, Daniel J, and Woodrow Hartzog. *Breached!: Why Data Security Law Fails and How to Improve it*. New York: Oxford University Press, 2022.