Osgoode Hall Law Journal

Volume 59, Issue 3 (Summer 2022) Article 17

2022

A Commercial Law of Privacy and Security for the Internet of Things by Stacy-Ann Elvy

Melissa Indome
melissaindome2019@osgoode.yorku.ca

Book Review

A Commercial Law of Privacy and Security for the Internet of Things by Stacy-Ann Elvy

Abstract

N/A

A Commercial Law of Privacy and Security for the Internet of Things by Stacy-Ann Elvy[1]

Melissa Indome[2]

From smart cars to smart refrigerators, the internet of things (IoT) has revolutionized various facets of our lives. These novel developments galvanized what scholars now deem to be the Fourth Industrial Revolution. This new era is characterized by technology-driven innovation that marries aspects of the physical, digital, and biological domains, going so far as to defy preconceived notions of human capabilities and behaviour.[3] The societal proclivity towards digitization and automated processes has spurred the proliferation of companies entering the technology arena. Corporations are leveraging emerging technologies to cater to consumers' idiosyncratic needs more effectively. Central to this objective is the collection of consumer data, which invites scrutiny from a privacy and security law perspective.[4]

Experts have theorized that the current legal frameworks for protecting consumers from privacy and security harms are inadequate.[5] Present legislation enables companies to circumvent the adoption of appropriate and fully transparent security and privacy practices, thereby rendering such measures essentially "optional."[6] Stacy-Ann Elvy, Professor of Law at the University of California, Davis School of Law, aptly elucidates the legal and consumer implications of the IoT in her book, *A Commercial Law of Privacy and Security for the Internet of Things* ("*Privacy and Security for the IoT*"). Diving deeply into the previously distinct worlds of commercial law and privacy law, Elvy highlights the inescapably intertwined nature of the two, which have come together through rapid evolutions of technology. In exploring this new digital epoch, Elvy draws on the impact of COVID-19 to provide readers with a topical analysis of US privacy and security law issues in the corporate sphere.

The advent of COVID-19 revealed the social, psychological, and geopolitical impacts of a global pandemic on human behaviour. A notable insight that emerged from the coalescence of these factors is the privacy ramifications for consumers. The global pandemic has compelled us to re-evaluate how we think about privacy, with particular attention to the legal frameworks that facilitate the protection of personal data.[7] In an effort to address public health concerns, some have called for a relaxation of the laws governing our privacy. In contrast, others have advocated for more stringent regulatory oversight to protect consumer information from collection through smart technologies, such as surveillance data and vaccine passports.[8] Elaborating on this contention, Elvy illustrates how the use of disease-related data may have inadvertent privacy consequences. For example, in an effort to reduce the spread of COVID-19, South Korea implemented public safety text messages that disclosed the location history, gender, and age-related data of individuals who

---

[1] (Cambridge University Press, 2021).

[2] Juris Doctor 2023, Osgoode Hall Law School.

[3] See Klaus Schwab, *The Fourth Industrial Revolution* (Crown Business, 2016).

[4] See Elvy, *supra* note 1; Marcy E Peek, "Information Privacy and Corporate Power: Toward Re-Imagination of Information Privacy Law" (2006) 37 Seton Hall L Rev 127.

[5] These materials exclusively discuss legal frameworks in the United States. See Mary Kraft, "Big Data, Little Privacy: Protecting Consumers' Data While Promoting Economic Growth" (2020) 45 U Dayton L Rev 97; Daniel J Marcus, "The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information" (2018) 68 Duke LJ 555; Anna Karapetyan, "Developing a Balanced Privacy Framework" (2018) 27 Southern California Rev L & Soc Justice 197. See also Elvy, *supra* note 1; Peek, *supra* note 4.

[6] See Jamie Lee Williams, "Privacy in the Age of the Internet of Things" (2016) 41 HR 14 at 15.

[7] See Elvy, *supra* note 1.

[8] *Ibid*. See generally Vincent J Samar, "Cyber-Security, Privacy, and the Covid-19 Attenuation?" (2021) 47 J Legis 1.

had been infected by the virus.[9] Despite being implemented in an effort to protect the public, this tactic resulted in the stigmatization of COVID-19 patients, as well as enabling inferences to be drawn regarding individual behaviours such as extramarital affairs and insurance fraud.[10] The global pandemic has highlighted the ongoing tension between advancing public health interests and ensuring regulatory protection of personal information.

The IoT has equipped companies with the ability to access large quantities of personal data, which has created new opportunities for consumers and businesses. Elvy sets out to reveal how these novel possibilities are also laden with privacy and security risks that may eventually undermine the advantages they purport to provide. In doing so, the book offers a myriad of powerful stories that shed light on these concerns, while offering practical recommendations for rectifying shortcomings in the law.

The book is divided into three parts with a total of nine chapters: Part I: Privacy and Security in the Connected Era; Part II: Commercial Law's Impact on Privacy, Security, and Liability; and Part III: Concrete Legal Solutions for a Commercial Law of Privacy and Security. Part I analyzes the data security concerns that the IoT poses to consumer privacy.[11] Elvy introduces the relevant legal framework governing privacy and information security in the United States, illuminating the gaps that fail to effectively address these issues. The first chapter explores the types of information that IoT technologies collect and identifies the potential corporate beneficiaries of data collection. The second chapter sheds light on the security failings of IoT devices, including the limits of anonymity. The third chapter examines the main privacy and security laws and regulations applicable to the governance of the IoT.[12]

Part II provides the reader with an overview of the applicable legal regime governing commercial and corporate practices that permits businesses to transfer and disclose consumer data, obtain consent to collect consumer data, and shield themselves from liability for defective IoT technologies.[13] Chapter four dissects the issue of assent to IoT contracts (and their terms) and provides a historical overview of commercial law to facilitate a deeper understanding of commercial law's consent problem. Chapter five uncovers the limitations of products liability law and warranty principles in the digital age. Chapter six evaluates the subprime auto lending and vehicle title lending industries to illustrate the various harms arising from IoT devices that allow lenders to track consumers and disable their vehicles. Chapter seven uncovers how corporations leverage privacy policies and conditions of use to permit consumer data transfers in mergers and acquisitions, bankruptcy proceedings, and secured finance transactions.[14]

Part III offers practical legal solutions to rectify inadequacies in commercial law and privacy and security law frameworks, emphasizing the increasing overlap between commercial law and privacy law.[15] In chapter eight, Elvy proposes various approaches at the state and federal level to remedy overreliance on notice and choice, and to better account for IoT harms that occur at the intersection of privacy and commercial legal domains. In chapter nine, Elvy expands on the proposals set out in chapter eight and argues that a comprehensive approach to addressing the

[9] See Elvy, *supra* note 1 at 3.
[10] *Ibid*.
[11] *Ibid* at 23-116.
[12] *Ibid*.
[13] *Ibid* at 117-266.
[14] *Ibid*.
[15] *Ibid* at 267-340.

deficiencies in privacy and security legislation will necessitate substantial revisions to the legal regimes regulating commercial practices.[16]

Elvy succeeds in delivering a perceptive analysis with a provocative flair that may elicit strong emotions in the reader. For instance, Elvy illustrates how a lack of sufficient privacy and security protection can be leveraged to uphold forms of class and racial hierarchy. Highlighting the growing gap between those who can afford to shield themselves from the privacy threats posed by IoT devices and those who cannot, the book explores issues of unequal access. Consider the use of pay-for-privacy (PFP) offerings, such as VPNs that conceal user identity and encrypt data. These products require consumers to incur an additional cost to protect their privacy. Low-income users who cannot afford to pay for PFP products are at an increased risk of heightened surveillance and privacy invasions.[17]

Similarly, widespread adoption of IoT technologies may facilitate unequal access to privacy protection for racialized groups. COVID-19 response efforts have leveraged IoT products to track the spread of the virus, which, in certain areas, has resulted in increased COVID-19-related data of racialized communities.[18] These troubling findings offer a valuable contribution to current literature exploring the potential for discriminatory practices arising from IoT data aggregation. Researchers have uncovered similar results, revealing that IoT data can serve as a proxy for racial and class-based discrimination, particularly in cases where seemingly innocuous economic decisions are being made, such as with a creditor or insurer.[19] As Elvy analyzes the legal and regulatory frameworks guiding IoT use, it becomes apparent that traditional legislation is unprepared for the new forms of discrimination that are set to arise.[20]

Privacy and Security for the IoT is timely, offering noteworthy revelations on the intersecting worlds of privacy, technology, and commercial law. Smart devices and artificial intelligence applications have driven the acceleration of the IoT and are radically transforming the way consumers conduct daily activities. As we progress through this digital era, consumer trends towards the consumption of technologies that collect personal information will continue to rise as long as they enhance the ease and efficiency of consumers' lives.[21]

With the introduction of over 160 consumer privacy laws passed by thirty-eight US states in 2021,[22] *Privacy and Security for the IoT* arrives during a time when it is very much needed. Despite the United States being home to some of the world's most comprehensive privacy and security laws, scholars have called for closer scrutiny to explore the gaps in state and federal-level legislation.[23] Elvy critically engages with many of these legal frameworks, adroitly highlighting the ways in which the IoT amplifies shortcomings in the law. Further, Elvy proposes several

---

[16] *Ibid*.
[17] See "Digital Domination in Consumer Lending Transactions" in Elvy, *supra* note 1, 196.
[18] See generally *ibid*.
[19] See Graham Johnson, "Privacy and the Internet of Things: Why Changing Expectations Demand Heightened Standards" (2019) 11 Washington U Jurisprudence Rev 345 at 360-62.
[20] See Elvy, *supra* note 1. See also Scott R Peppet, "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent" (2014) 93 Tex L Rev 85; Williams, *supra* note 6; Johnson, *supra* note 17.
[21] See Andrea Sestino et al, "Internet of Things and Big Data as Enablers for Business Digitalization Strategies" (2020) 98 Technovation 1.
[22] See National Conference of State Legislatures, "2021 Consumer Data Privacy Legislation" (27 December 2021), online: <www.ncsl.org/research/telecommunications-and-information-technology/2021-consumer-data-privacy-legislation.aspx> [perma.cc/D5GR-4XHS].
[23] See Hala Bou Alwan, "Policy Development and Frameworks for Cyber Security in Corporates and Law Firms" (2018) 46 Intl J Leg Info 137.

concrete solutions that can be implemented to foster a more robust commercial law of privacy and security.[24] The adoption of a federal baseline privacy statute in tandem with revisions to existing sources of law would address consumer concerns while accounting for the interconnected worlds of commercial law and privacy law. Elvy advocates for selective use of European data privacy and security frameworks—namely, the General Data Protection Regulation (GDPR)—to reformulate the US' data protection laws.[25] Adoption of GDPR-like principles would enable the United States to learn from GDPR deficiencies and adapt federal legislation and regulation. The projected outcome would restrict data collection that is not pertinent to a legitimate interest, and ultimately, enhance consumer autonomy.

Elvy's evaluation of IoT harms is undoubtedly captivating. However, the book may have benefitted from engaging more deeply with an analysis of consumer behaviour. Scholars have acknowledged that the dangers of IoT technologies are at least partially self-imposed. Research shows that consumers prioritize IoT products due to their relative convenience, despite the various risks they pose to their privacy.[26] In instances where consumers were initially nescient regarding the extent to which they must give up their privacy in exchange for an IoT device, they typically continued to use these technologies upon becoming aware. It is prudent to distinguish between consumers who leverage a cost–benefit analysis and rationally decide to purchase IoT devices irrespective of the potential harms and consumers who unknowingly relinquish their privacy but would otherwise prefer not to.[27] Examining the motivations behind consumer behaviour could have produced an even more nuanced analysis.

Notwithstanding this criticism, Elvy achieves the objective that is set out at the beginning of the book. *Privacy and Security for the IoT* delivers a thoughtful analysis of the potential for corporate infiltration of private spaces, offering tangible recommendations to remedy gaps in the legal frameworks that inadequately protect consumer privacy and security. The interdisciplinary and wide-ranging approach of *Privacy and Security for the IoT* makes it well-suited for members of the legal community and beyond.

[24] See "Part III: Concrete Legal Solutions for a Commercial Law of Privacy and Security" in Elvy, *supra* note 1, 269.
[25] "Establishing Baseline Privacy and Security Frameworks" in Elvy, *supra* note 1, 269.
[26] See Johnson, *supra* note 19 at 351.
[27] See Melissa W Bailey, "Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things" (2016) 94 Tex L Rev 1023 at 1035-41.