Chapter 89
Consumer Privacy Regulations:
Considerations in the Age of Globalization and Big Data

Martha Davis

ⓘD https://orcid.org/0000-0001-8756-8616
University of Denver, USA

ABSTRACT

Big data and analytics have not only changed how businesses interact with consumers, but also how consumers interact with the larger world. Smart cities, IoT, cloud, and edge computing technologies are all enabled by data and can provide significant societal benefits via efficiencies and reduction of waste. However, data breaches have also caused serious harm to customers by exposing personal information. Consumers often are unable to make informed decisions about their digital privacy because they are in a position of asymmetric information. There are an increasing number of privacy regulations to give consumers more control over their data. This chapter provides an overview of data privacy regulations, including GDPR. In today's globalized economy, the patchwork of international privacy regulations is difficult to navigate, and, in many instances, fails to provide adequate business certainty or consumer protection. This chapter also discusses current research and implications for costs, data-driven innovation, and consumer trust.

INTRODUCTION

Big data and data analytics are still evolving fields of study. Thus, an agreed-upon and fully comprehensive definition is yet to be established (Uthayasankar, Muhammad, Zahir, & Vishanth, in press). It is also debatable whether big data is a disruptive technology (Frizzo-Barker, Chow-White, Mazafari, & Ha, 2016). However, we do know that it is changing how businesses understand, connect with, and ultimately profit from their customers. Manyika and Brown (2011) state that big data has the potential to increase business operating margins by up to sixty percent. Data is becoming crucial for companies

in decision-making, relationship-management, production, and maintaining an overall competitive advantage. It is particularly valuable once turned into digital intelligence.

The overall amount of data collected is doubling every two years, with an estimated 44 zettabytes of data by the end of 2019. That is equal to 99 billion years of music files, 686 billion 64GB tablets, or 1.4 billion years of HD video. Businesses can monetize all this data in several ways, including use for advertising revenue (Facebook, Google, etc.), marketplace transactions (Amazon, eBay, Alibaba, Uber, etc.), production optimization (Rolls Royce, Caterpillar, etc.), and the selling or renting of cloud services (AWS). Users often pay for seemingly free services, such as downloadable white papers and e-books, by signing up with their data.

Big data and analytics have changed not only how consumers interact with businesses, but also how they interact with the larger world. Smart cities, IoT, cloud, and edge computing technologies are all enabled by data and have the potential to provide significant societal benefits through efficiencies and the reduction of waste. While digitization has the potential to benefit both businesses and society at large through new intelligence, innovation, and profits, the primary challenges are that of privacy and security (Frizzo-Barker et al., 2016). In the age of big data and business analytics, concern over privacy and data protection is increasingly at the forefront of consumers' minds. Massive data breaches have caused severe economic, social, and psychological harm to customers by exposing personal information. Data breaches have also severely damaged the consumer-trust relationship with the companies at issue, often reducing firm market valuations and forever tarnishing brands (Choong, Hutton, Richardson, & Rinaldo, 2017). A simple Internet search shows the scale of this problem, with massive data breaches involving even high-profile companies, such as Equifax, Marriot, Yahoo, and Uber, to name just a few examples. It is also worth mentioning that consumer privacy concerns can extend beyond unauthorized data breaches. For example, there was significant consumer backlash in the United States related to the Facebook sale of personal data to Cambridge Analytica for political purposes (Meredith, 2018). With the proliferation of big data, there are also numerous new policy questions relating to data ownership, a concentration of large companies that control this data, and data flows across international borders.

The objectives of this chapter are to:

- Provide an overview of the various international data privacy regulations, including GDPR;
- Discuss the pros and cons of the different data privacy regulations and lessons learned;
- Discuss the implications of data privacy regulations on data-driven innovation, the economics of privacy, and consumer trust; and
- Suggest potential solutions and recommendations.

BACKGROUND

Information privacy is the ability to control personal data and associated identities, and it is now widely regarded as one of the most vulnerable aspects of online use (Nissenbaum, 2011). Privacy regulations are concerned with how businesses handle data and information privacy. While privacy regulations have existed for many years, the number of proposed government regulations have been increasing as a result of the growing number of data breaches and associated consumer backlash. One of the more well-known regulations is the General Data Protection Regulation (GDPR) in the European Union (EU). Globally, the current position of consumer data privacy regulations is not ideal. Many jurisdictions have no regu-

Related Content

Cyber Threats in Civil Aviation

Calvin Nobles (2017). *Security Solutions for Hyperconnectivity and the Internet of Things (pp. 272-301).*

www.irma-international.org/chapter/cyber-threats-in-civil-aviation/164700

Relationships between Information Security Concerns and National Cultural Dimensions: Findings in the Global Financial Services Industry

Princely Ifinedo (2011). *Security and Privacy Assurance in Advancing Technologies: New Developments (pp. 134-153).*

www.irma-international.org/chapter/relationships-between-information-security-concerns/49500

A Comprehensive Consent Management System for Electronic Health Records in the Healthcare Ecosystem

Swapnil Shrivastavaand T. K. Srikanth (2023). *Information Security and Privacy in Smart Devices: Tools, Methods, and Applications (pp. 194-233).*

www.irma-international.org/chapter/a-comprehensive-consent-management-system-for-electronic-health-records-in-the-healthcare-ecosystem/321343

A Smart System of Malware Detection Based on Artificial Immune Network and Deep Belief Network

Dung Hoang Le, Nguyen Thanh Vuand Tuan Dinh Le (2021). *International Journal of Information Security and Privacy (pp. 1-25).*

www.irma-international.org/article/a-smart-system-of-malware-detection-based-on-artificial-immune-network-and-deep-belief-network/273589

Smartphone Confrontational Applications and Security Issues

Abhishek Kumar, Jyotir Moy Chatterjeeand Pramod Singh Rathore (2020). *International Journal of Risk and Contingency Management (pp. 1-18).*

www.irma-international.org/article/smartphone-confrontational-applications-and-security-issues/246844