ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law
&
Security Review

Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data

Nancy J. King [a,*], *Jay Forder* [b]

[a] *College of Business, Oregon State University, Corvallis, Oregon, USA*
[b] *Law Faculty, Bond University, Gold Coast, Australia*

Keywords:
Big Data
Data analytics
Consumer profiling
Privacy
Data protection

ABSTRACT

In Big Data, the application of sophisticated data analytics to very large datasets makes it possible to infer or derive ("to discover") additional personal information about consumers that would otherwise not be known from examining the underlying data. The discovery and use of this type of personal information for consumer profiling raises significant information privacy concerns, challenging privacy regulators around the globe. This article finds appropriate privacy principles to protect consumers' privacy in this context. It draws insights from a comparative law study of information privacy laws in the United States and Australia. It examines draft consumer privacy legislation from the United States to reveal its strengths and weaknesses in terms of addressing the significant privacy concerns that relate to Big Data's discovery of personal data and subsequent profiling by businesses.

1. Introduction

Governments and commentators around the world are wondering how to best protect consumers' privacy in the world of Big Data, with notable policy analysis being issued by European regulators and the Office of the President in the United States (The White House).[1] Fueled by the availability of vast datasets and technical advances in data analytics, Big Data has the potential to provide big value to citizens, businesses and governments.[2] It is the next giant leap in the knowledge revolution. Enormous quantities of data are being collected into digital databases from many sources such as Internet activity, satellites, sensors, RFID tags and GPS-enabled devices like cameras and smartphones.[3] Analysis of this data by Big Data facilitates data-directed decision-making, which, according to

[*] *Corresponding author.* College of Business, Oregon State University, Corvallis, Oregon, USA.
E-mail address: kingn@bus.oregonstate.edu (N.J. King).

[1] *See, for example*, Big Data: Seizing Opportunities, Preserving Values, Exec. Office of the President, Under Discussion United States (May 2014) (White House Report on Big Data); Meeting the Challenges of Big Data, A call for transparency, user control, data protection and accountability, European Data Protection Supervisor, European Union, Opinion 7/2015 (Nov. 19, 2015) (EDPS OPINION ON BIG DATA).

[2] *See generally*, Christopher Kuner et al., *The Challenge of "Big Data" for Data Protection*, 2(2) Int' Data Privacy L. 47 (2012); K. Krawsnow Waterman & Paula J. Bruening, *Big Data Analytics: Risks and Responsibilities*, 4(2) Int'l Data Privacy L. 89 (2014).

[3] Working Paper on Big Data and Privacy, Privacy principles under pressure in the age of Big Data analytics, International Working Group on Data Protection in Telecommunications, 55th Meeting, Skopje, p. 3 (item 9) (May 5–6, 2014) (Berlin Group Working Paper on Big Data and Privacy) http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf?1407931243 (last visited Feb. 15, 2016).

http://dx.doi.org/10.1016/j.clsr.2016.05.002
0267-3649/© 2016 Nancy J. King & Jay Forder. Published by Elsevier Ltd. All rights reserved.

recent research, helps companies improve productivity and managerial performance.[4] Further, Big Data's use of data analytics helps companies offer personalized goods and services, deliver targeted marketing communications, strengthen companies' information security systems and prevent fraud.[5]

Consumer profiles produced in Big Data are not limited to simple compilations of factual information about consumers that has been collected from consumers during their direct interactions with companies. Instead, Big Data facilitates construction of consumer profiles to include other personal data that has been derived or inferred through data analytics, the so called "fruits" of data analytics.[6] In this article, we refer to the fruits of data analytics as "discovered data".[7] Consumer profiles so constructed in Big Data "can be exceptionally detailed, containing upwards of thousands of pieces of data".[8] As The White House concluded "more often than not, consumers do not understand the degree to which they are a commodity"[9] in Big Data and "there remains the potential for a disquieting asymmetry between consumers and the companies that control information about them".[10]

The primary aim of this article is to help global regulators find appropriate privacy principles and use them to craft legislation to protect consumers' information privacy in Big Data, a goal that has been taken-up by policy-makers, regulators and scholars in many other countries.[11] In the European Union, the European Data Protection Supervisor (EDPS) emphasizes the importance of meeting consumer privacy challenges associated with Big Data's application of data analytics."[12] According to the EDPS, these privacy challenges include "lack of transparency" between organizations that process personal data about individuals and those individuals, with organizations claiming "secrecy over 'how' data is processed on grounds of commercial confidentiality".[13] The EDPS predicts "informational imbalance between the organisations who hold the data and the individuals whose data they process is likely to increase with the deployment of big data applications."[14]

Another aim of this article is to contribute ideas to the ongoing effort in the United States to adopt federal consumer privacy legislation that protects consumers' privacy in the era of Big Data.[15] Following comprehensive study of the need to protect consumers' information privacy in Big Data, a discussion draft of legislation for a federal consumer privacy law was issued by the Office of the President in 2015.[16] This article analyzes the strengths and weaknesses of this discussion draft and makes suggestions to improve it in order to address significant privacy concerns related to the discovery of personal data through data analytics and its use for consumer profiling.

Following this introduction, Section 2 provides an overview of Big Data, describing how the industry's use of data analytics facilitates consumer profiling by businesses. Section 3 identifies important consumer privacy concerns associated with Big Data's use of data analytics to discover personal data for consumer profiling. Section 4 argues that the scope of information privacy legislation should include discovered data that is also personal data. Section 5 applies recognized principles of data protection and privacy to the context of personal information discovered through data analytics, providing suggestions for drafting consumer privacy legislation to encompass discovered personal information and its use for consumer profiling. These drafting suggestions benefit from a comparative-law analysis of consumer privacy principles found in information privacy laws in the United States and Australia.[17]

[4] Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11(5) Nw, J. Tech. Intell. Prop., 239, 243-44 (2013) (summarizing studies that show companies using "data-directed decision-making" are more productive and there is a strong link between effective data management strategy and financial performance).

[5] Tene & Polonetsky, *supra* note 4, at 249–251.

[6] White House Report on Big Data, *supra* note 1, at 44; Waterman & Bruening, *supra* note 2, at 89. In this article, the authors use the terms "data" and "information" to mean the same thing.

[7] Discovered data includes data described as "modeled data" in the White House Report on Big Data, *supra* note 1.

[8] White House Report on Big Data, *supra* note 1, at 44.

[9] White House Report on Big Data, *supra* note 1, at 41 (discussing the advertising-supported ecosystem of Big Data).

[10] White House Report on Big Data, *supra* note 1, at 39.

[11] *See generally*, White House Report on Big Data, *supra* note 1; Big Data and Privacy: A Technological Perspective, Report to the President, Executive Office of the President, President's Council of Advisors on Science and Technology, United States, ix (May 2014) (Big Data and Privacy: A Technological Perspective); Big Data: Seizing Opportunities, Preserving Values, Interim Progress Report, Executive Office of the President, United States (Feb. 2015) (Interim Progress Report); FTC Report, Big Data, A Tool for Inclusion or Exclusion, Federal Trade Commission, United States (Jan. 2016) (FTC Report, Big Data); Data Brokers, A Call for Transparency and Accountability, Federal Trade Commission, United States (May 2014) (FTC Data Broker Report); EDPS Opinion on Big Data, supra note 1; Berlin Group Working Paper on Big Data and Privacy, *supra* note 3; Comments of the Information Accountability Foundation, Before the National Telecommunications & Information Administration, Department of Commerce, Washington, D.C., United States (Aug. 4, 2014) (IAF Comments), http://informationaccountability.org/wp-content/uploads/TIAF-Big-Data-Comments-for-NTIA.pdf.

[12] *See generally*, EDPS Opinion on Big Data, *supra* note 1.

[13] EDPS Opinion on Big Data, *supra* note 1, at 8.

[14] EDPS Opinion on Big Data, *supra* note 1, at 8.

[15] Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, The White House, Washington, D.C., United States (Feb. 2012) (2012 CPBR) (announcing the Obama administration's vision for new federal consumer privacy legislation requiring private-sector businesses to follow seven Fair Information Privacy Principles (FIPPs) that are collectively referred to in this policy paper as "The Consumer Privacy Bill of Rights"), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. Gregory, et al., *President Obama's Plans for Cybersecurity, Broadband, and "Big Data,"* Lexology (Jan. 15, 2015).

[16] The document titled "Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015" was released by The White House on February 28, 2015 (Discussion Draft), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf (last visited Feb. 2, 2016). To date, no proposed consumer privacy legislation has been introduced in Congress to implement the FIPPS announced in the 2012 CPBR, *supra* note 15, or in the Discussion Draft.

[17] The Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) amended the Australian Privacy Act 1968 (Cth). It amalgamated the two sets of privacy principles which had previously operated in different spheres into one set of 13 Australian Privacy Principles (APPs). It took effect on March 12, 2014.