Chapter 78
Data Protection and BI:
A Quality Perspective

Daragh O Brien
Castlebridge Associates, Ireland

ABSTRACT

Data Protection (DP) and Privacy are increasingly important quality characteristics of Information, particularly in the context of Business Intelligence and Big Data. This relationship between Data Protection and Information Quality (IQ) is often poorly understood, and DP itself is often misunderstood as being an issue of security control rather than information governance. This chapter examines the relationship between DP, IQ, and Data Governance (DG). It provides an overview of how techniques and practices from IQ and DG can ensure that BI projects are grounded on appropriate privacy controls that ensure that the right information is being used in the right way by the right people to answer the right questions.

INTRODUCTION

We live in an information-rich age. Social networks, electronic point of sale systems, ecommerce sites, mobile phones with GPS, cellular communications networks, and an increasingly dizzying array of technologies provide the ability, in theory at least, for organizations to obtain data for a variety of analytics purposes. Entire industries have grown up around the tracking of how we use the Internet for example. Multi-billion dollar IPOs have been launched on the promise of dollars from data provided by people using 'free' services like Facebook.

However, consumers and citizens are increasingly aware of and resistant to the idea that their data is being logged, tracked, and analyzed in this way. In a recent EURO Barometer survey (European Commission, 2011) 54% of EU citizens were concerned about their behavior being recorded via payment cards, with relatively high levels of concern recorded regarding behavior tracking via mobile phone and mobile internet (49% and 40% respectively). 70% of Europeans were concerned that organizations would use data that they held about individuals for purposes ***other*** than that for which it was collected. These findings are echoed in similar research in Canada. In a study conducted for the Office of the Privacy Commissioner of Canada 65% of Canadians felt that "*protecting the personal information of Canadians will be*

DOI: 10.4018/978-1-5225-8897-9.ch078

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

one of the most important issues facing the country in the next ten years", with 55% expressing concerns about data privacy on social networking sites (Office of the Privacy Commissioner of Canada, 2011).

With such concern being shown in Europe and Canada, two jurisdictions with relatively mature Data Protection laws, it is unsurprising that in 2012 the FTC in the United States published its report on *Protecting Consumer Privacy in an Era of Rapid Change* (Federal Trade Commission, 2012) that set out a number of clear Data Protection/Privacy principles that organizations in the US that are proposed to supplement the existing statutory privacy regulations in sector-specific legislation such as HIPAA (Health Insurance Portability and Accountability Act), the Graham-Leech-Bliley Act, and the HITECH Act (Health Information Technology for Economic and Clinical Health Act). This, coupled with the FTC's increased enforcement actions on data protection issues in 2011 and 2012, and the release in February 2012 of the Obama Administration's "Consumer Privacy Bill of Rights" (The White House, 2012), represents a clear message to US organisations that respect for Data Protection and Privacy is essential in the digital economy.

However, recent developments such as the disclosure of the nature and extent of data processing by US Intelligence services has been hailed by FTC Commissioner Julie Brill (Brill, 2013) as a spark for what she terms "a necessary and overdue debate". In particular she highlights how the disclosures mean that:

Americans are now more aware than ever of how much their personal data is free-floating in cyberspace, ripe for any data miner – government or otherwise – to collect, use, package, and sell.

This renewed awareness on the part of Americans should not be equated with an absence of consumer demand however. Consistently studies have highlighted consumer concern about and resistance to the excessive capture of, sharing of, and analysis of personal information. For example a 2012 study (Hoofnagle, Urban, & Li, 2012) found that 81% of respondents to their survey objected to the transfer of telephone number data to retailers where they used mobile payment services (e.g. Near Field Communication). The same percentage of respondents objected to the transfer of their home address to the retailer. A report from the Pew Research Center found that 68% of respondents were "not okay" with targeted advertising as they did not like having their on-line behaviour tracked and analysed. Interestingly, 55% of 18-24 year olds shared this view despite the 'conventional wisdom' that that demographic is less concerned with their privacy (Purcell, Brenner, & Rainie, 2012).

The Spread of Legislation and Regulation

Globally there are approximately 90 countries with specific data protection laws on their statute books (Banisar, 2012), with others in development. This does not count countries with sector-specific legislation such as the United States. In general, the majority of these laws are based on the EU's Directive 95/46/EC (European Commission, 1995) or the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 1981).

There is a growing consensus on fundamental information processing principles that should be applied, and we are in the midst of a period of unprecedented activity in the development of data protection regulation globally which is already having a profound impact on the way in which global businesses are required to approach the collection and management of personal information.

24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/data-protection-and-bi/228799

Related Content

Exploring Privacy Notification and Control Mechanisms for Proximity-Aware Tablets
Huiyuan Zhou, Vinicius Ferreira, Thamara Silva Alves, Bonnie MacKay, Kirstie Hawkeyand Derek Reilly (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications (pp. 227-247).*
www.irma-international.org/chapter/exploring-privacy-notification-and-control-mechanisms-for-proximity-aware-tablets/228729

Understanding Continuance Usage of Mobile Social Network Sites
Tao Zhou (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications (pp. 1003-1017).*
www.irma-international.org/chapter/understanding-continuance-usage-of-mobile-social-network-sites/228766

Cloud Storage Privacy and Security User Awareness: A Comparative Analysis Between Dutch and Macedonian Users
Adriana Mijuskovicand Mexhid Ferati (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications (pp. 937-957).*
www.irma-international.org/chapter/cloud-storage-privacy-and-security-user-awareness/228763

Security and Privacy Issues of Big Data
José Mouraand Carlos Serrão (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications (pp. 375-407).*
www.irma-international.org/chapter/security-and-privacy-issues-of-big-data/228736

Wireless Body Sensor Networks: Security, Privacy, and Energy Efficiency in the Era of Cloud Computing
Wassim Itani, Ayman Kayssiand Ali Chehab (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications (pp. 731-763).*
www.irma-international.org/chapter/wireless-body-sensor-networks/228753