CSEC620

CSEC 620 IA 2: Retail Consumer Data Use and Need for Better Privacy

(Introduction Updated 2017 to Better Clarify Scope of Content)

Megan Bell

University of Maryland University College

NOTE: This is a layman's perspective and not an attorney's legal review. The report considers public information only and does not draw from private information sources. Finally, this report is a snapshot perspective based on the information available at the time of writing.

Table of Contents

Introduction

A 100 gigabyte (GB) storage hard drive can hold basic demographic information for all individuals on the planet (Jacobs, 2008). Today, 100 GB is less than 0.0001% of more than 295 billion gigabytes of data created since 1996 (Mearian, 2011). This vast quantity of personal data became part of the digital revolution that transformed the U.S. economy into a data-centric economy. For retailers, demographic detail and other personal information provide the opportunity for further sales through the monetization of data (Wolken, n.d.).

This paper begins with an exploration of online retailer Amazon's success at the ownership, control and use of personal customer data to achieve data-derived business success. Next, this paper transitions to a broader discussion of regulating and protecting consumer data. Concerning Amazon, this paper reviews important contributors of Amazon's ability to develop insights from consumer personal data. Amazon's collection of personal data provides the foundation for data analysis. Customer data is employed in the development of insights that translate to greater sales. While customer data is pivotal to providing customer-centric services, even a firm such as Amazon has incurred issues where availability of customer data has led to identity compromise for certain individuals and has demonstrated limits to even the strongest of information security programs. Amazon achieves its mission as a successful online retailer, in part due to U.S. federal and state government's limited privacy protections. However, U.S. laws concerning protection of consumer information demonstrate a patchwork approach to privacy, and government's need for deeper surveillance into individual privacy may involve online businesses' customer data without customer notice. Ultimately, a better solution to privacy could be a data economy where use and exchange of personal data has greater transparency.

Amazon as a Regulatory Test Case

Business Goals

Amazon (2015) is an online retail marketplace and provider of information services and infrastructure as Amazon Web Services (AWS). With its innovative data analysis, Amazon has developed a track-record of achieving tight profit margins that rival cost-conscious retailers such as Wal-Mart (Mourdoukoutas, 2014). Amazon's collection and control over its consumer data is also fundamental to its success.

Amassing Data

Amazon has 10 global marketplaces, 96 global fulfillment centers, and customers in 178 countries (Amazon, 2013). This includes an estimated 100 million U.S. consumers (Wohlsen, 2014). Through online marketplaces, Amazon captures and stores extraordinary amounts of consumer data such as name, contact and financial information. This includes Amazon marketplace shopping data and data from its own products such as the Amazon Silk browser.

The Silk browser demonstrates a powerful example of how Amazon captures of consumer data that far exceeds basic account information. The Silk browser was developed for the Amazon Kindle tablet and transmits an individual's website data through the Amazon cloud before an individual is connected with a particular website (Sutter, 2011). This practice contributes to Amazon collecting all information about an individual's web browsing use (Amazon, 2013). By collecting the full population for a customer's browser history, Amazon gains intimate knowledge on a customer's personal life.

Amazon's Self-benefiting Privacy Policies

Amazon's privacy policy outlines that Amazon collects, uses and also shares personal data (Amazon, 2014). Personal data includes traditional personal information such as user account detail and secondarily-collected data from computer devices, software applications and Internet browser use. Information sharing broadly applies to business partners, advertisers and regulatory and law enforcement agencies. To understand the latitude of amazon's data use, Amazon cloud storage customers provide Amazon the right to access, share and use a customer's cloud-stored data. Amazon can scan information about the type of files stored and the content of the actual files (Vaughan-Nichols, 2011). The explicit example of Amazon's right to scan personal cloud-stored data indicates to the possible breadth of personal data collection and utilization practices.

Derived Consumer Data's Value to Product Sales

Amazon conducts deep analysis of customer data to sell more products and further identify business opportunities. Amazon's analytics prowess may be observed in patents such as a programmatic software patent that makes product recommendations derived from group-oriented recommendations (Lam, Chakrabarti, Ionkov, Kim, & Witt, 2012). Interestingly, this patent also relates to Amazon's ability to successfully encourage consumers to voluntarily share information such as product reviews. Consumers generate published content on products that Amazon translates to monetized value. While Amazon makes great use of consumer data to sell product, customers do not necessarily fathom the breadth of Amazon data analytics (Ulanoff, 2014). The derived data that Amazon generates may rival the importance of original demographics data in that the derived data explains an individual's habits and behaviors.

Instances of Identity Highlight Date Privacy Concerns

The quantity and breadth of personal information stored by Amazon should be a cause for concern. Considering personal information alone, Amazon's approach to availability of personal information has been observed as a security vulnerability. In two publicized cases on the compromise of online identity, personal information held by Amazon on behalf of account owners lead to different types of identity compromise and loss. In one case, a software developer developer had his identity stolen when Amazon representatives leaked personal information as part of confirming account holder identity (Springer, 2016). On two separate occasions, the developer became of victim of identity theft due to Amazon's insufficient identity verification process. The second case involved Wired magazine writer Matt Honan (Honan, 2012). In this case, a hacker wanting Honan's Twitter account used social engineering to achieve full compromise of Honan's online accounts. Honan's role as a writer contributed to greater public awareness of data vulnerability and potentially false trust placed in companies such as Amazon to provide absolute protection of data.

Amazon's Data as a Privacy and Security Risk

In its annual report to shareholders, Amazon documents privacy and information security as significant business risks that could adversely impact business (Amazon, 2015). To demonstrate strong security posture, Amazon's chief information security officer Stephen Schmidt has publically described Amazon as having highly engaged information security practices with globally consistent security policies and data access restrictions to maintain consistent practices of confidentiality and integrity of data (McDougall, 2012). These practices suggest a highly secure infrastructure, but do not necessarily speak to granular data security.

While Amazon has focused on traditional information security, U.S. regulation has focused on data-related privacy and security issues. The gradient between Amazon's publically acknowledged secure systems and assertive rights to use customer data are a reminder of the need to clearly define individual privacy and the uses of personal information. Amazon's security issues with identity theft underlie the need for more comprehensive privacy laws.

Regulation of Consumer Information

Consumer Data Regulation Begins with Privacy

There are two approaches to regulating personal information. One approach regulates information with respect to the whole person, and a second approach addresses regulation of certain elements of personal information such as social security number (Schwartz & Solove, 2013). In the U.S., privacy laws and regulations follow the latter approach and are referred to as a sectorial approach since regulations exist by industry and issue (Swine & Ahmad, 2012). This sectorial approach contributes to the to privacy gaps that benefit U.S. retailers' use of personal data other than where specific regulatory regimes exist.

FTC as Consumer Data Protector

In the U.S., the lack of a singular regulatory authority for the protection of personal data created an opening for the Federal Trade Commission (FTC) to assume a role of personal data protector. In 2000, the FTC began outlined its initial presence by publishing a report on Fair Information Practices (FIPS) for online privacy (FTC, 2000). The FTC indicated that online businesses were responsible parties in the delivery of accurate information to consumers. The FTC also indicated it had the right to bring certain enforcement actions for unfair businesses practices. Over time, the FTC used its role to file suits against retailers such as Amazon and to

assess monetary penalties for certain deceptive personal information practices such as misuse of children's data (FTC, 1998). The FTC is one example of a U.S. federal regulator stepping in to provide protection of personal information, but the FTC is limited by its legislative mandates.

State Data Breach Laws

There are no U.S. federal data breach protection laws. Instead, 47 states have developed separate laws concerning data breach and security regulations (Alexander, 2008; Swire & Ahmad, 2012). State attorneys-generals such as Kamala Harris of California have prioritized consumer personal information as a legal issue and extended the ability of individuals to achieve certain rights concerning private industry use of personal information (State of California, 2014).

Using Business for Government Surveillance

With data increasingly being controlled by private industry, the U.S. federal government has sought greater access to private industry repositories of personal data. The latest bill to be and enacted into law is the Cybersecurity Act of 2015, formerly called the Cybersecurity Information Sharing Act (Center for Democracy and Technology [CDT], 2015). While opposed for its privacy intrusion potential, this law represents the most recent effort but U.S. federal authorities to access personal data without the need to inform individuals.

The Need for Security Context to Derived Personal Data

Historically, data is a component of information security and is addressed through data security, protection such as encryption and privacy-related controls (Vacca, 2013). This explicit definition of data does not necessarily encompass derived data or related mathematic functions. Because the focus centers on original data rather than data and its related ecosystem, certain types of data such as derived data remain unsecured.

Modern-day large data systems known as big data do not fit historic information systems constructs such as relational databases or file servers (Jacobs, 2008). Private industry and government analyze big data to understand individuals (Kakutani, 2013). This analytic process addresses confidentiality of original personal data but not the derived leanings of customer data. As analytics continues to analyze amassed quantities of customer personal data, security and privacy protections should more directly address data and not solely systems hosting data.

Conclusions

It has been argued that consumers' data is their respective virtual property, and this virtual property should be part of the economic exchange with business. According to Hettche (2009), the exchange of data between parties is a form of what John Locke called a "social contract." Hettche interprets Locke's classic social contract theory by defining electronic data as personal property. Individuals are the owners of their data and exchange data in the marketplace as part of economic activity. Extending this argument further, the concept of privacy indicates that an individual has rights to control personal information (Swire & Ahmad, 2012; Tipton & Krause, 2003). The challenge is today's abundance of data is defining the framework of personal information commerce and the relationship between business and individuals.

Marketers who collaborate with retailers to understand customers and increase sales understand that consumers own their data (Simpson, 2014). Marketers discuss collaboration between consumers and business as a means to justify use of personal data. In a marketplace where customers own their data, the marketplace for data becomes more representative of a market-driven economy based on the agreed exchange of data (Hettche, 2009). From this perspective, derived data achieves more accurate marketplace value, and regulators are able to

engage private industry in more transparent discussions on the economics of personal data. Regulators also have better control due to transparency of business data practices.

References

Alexander, P. (2008). Information security: A manager's guide to thwarting data thieves and hackers. ABC-CLIO.

Amazon. (2015). 2015 Amazon annual corporate report. Retrieved from http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-reportsannual

Amazon. (2013) Amazon global selling: Two ways to sell internationally. Retrieved from http://g-ec2.images-Amazon/images/G/01/amazonservices/globalselling/AGS_Infographic_US_version._V340381695_.pdf?ld=NSGoogleAS%27

Amazon. (2014). Amazon privacy notice. Retrieved from http://www.Amazon/gp/help/customer/display.html?nodeId=468496

Amazon. (2013). Amazon Silk terms & conditions. Retrieved from http://www.Amazon/gp/help/customer/display.html/?nodeId=200775270

Center for Democracy and Technology. (2015). Final civil society security expert letter opposing CSA 2015 [Abstract]. Retrieved from https://static.newamerica.org/attachments/12218-51-civil-society-groups-and-security-experts-tell-congress-they-oppose-cyber-legislation/FINAL_Civil_Society_Security_Expert_Letter%20Opposing_CSA_2015.efca7165edbf4beaa392e5ef66cfff70.pdf

Federal Trade Commission (FTC). (2000, September), Advertising and marketing on the Internet. Retrieved from https://www.ftc.gov/system/files/documents/plain-language/bus28-advertising-and-marketing-internet-rules-road.pdf

Federal Trade Commission (FTC). (1998). Children's Online Privacy Protection Rule ("COPPA"). Retrieved from https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

Jacobs, A. (2009). The pathologies of big data. Communications of the ACM, 52(8), 36-44. doi:10.1145/1536616.1536632

Hettche, M. (2009). Privacy, e-commerce, and virtual property: Outlining a Lockean theory of Internet consumer rights. AMA Winter Educators' Conference Proceedings, 20425-431.

Honan, M. (2012). How Apple and Amazon security flaws lad to my epic hacking. Wired Magazine. Retrieved from http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Kakutani, M. (2013, June 10). Watched by the Web: Surveillance Is Reborn. Retrieved from http://www.nytimes.com/2013/06/11/books/big-data-by-viktor-mayer-schonberger-and-kenneth-cukier.html

Lam, S., Chakrabarti, K., Ionkov, G., Kim, S., & Witt, B. (2012). U.S. Patent No. US8260787 B2. Washington, DC: U.S. Patent and Trademark Office. Retrieved from http://www.google.com/patents/US8260787

McDougall, P. (2012). 5 ways Amazon web services protects cloud data. NetworkComputing. Retrieved from http://www.networkcomputing.com/cloud/5-ways-amazon-web-services-protects-cloud-data/1330559781

Mearian, L. (2011, February 14). USC report calculates amount of stored data grew by 23% a year between 1986 and 2007. Computerworld. Retrieved from http://www.computerworld.com/article/2513110/data-center/scientists-calculate-total-data-stored-to-date--295--exabytes.html

Mourdoukoutas, P. (2014, October 27). What's wrong with Amazon's business model? Forbes.com Retrieved from http://www.forbes.com/sites/panosmourdoukoutas/2014/10/27/whats-wrong-with-amazons-business-model/

Schwartz, P., & Solove, D. (2013, September 6). Reconciling personal information in the United States and European Union. http://dx.doi.org/10.2139/ssrn.2271442

Simpson, P. (2014, January 31). Who “really” owns customer data? DMN. Retrieved from http://www.dmnews.com/privacy/who-really-owns-customer-data/article/331976/

Springer, E. (2016. January 25). How Amazon customer service was the weak link that spilled my data. Retrieved from

Sutter, J. (2009). Amazon's 'cloud' browser raises privacy concerns. CNN. Retrieved from http://www.cnn.com/2011/09/29/tech/gaming-gadgets/amazon-silk-browser/

Swire, P. P., & Ahmad, K. (2012). U.S. private-sector privacy: Law and practice for information privacy professionals. NH: International Association of Privacy Professionals.

Ungerleider,N. (2015, November 16). A new report shows how Amazon is different around the world. Fast Company. Retrieved from http://www.fastcompany.com/3053659/behind-the-brand/a-new-report-shows-how-amazon-is-different-around-the-world

Ulanoff, L. (2014). Amazon knows what you want before you buy it. Predictive Analytics Times. Retrieved from http://www.predictiveanalyticsworld.com/patimes/amazon-knows-what-you-want-before-you-buy-it/3185/

Tipton, H. F., & Krause, M. (2003). Information security management handbook (Volume 5). CRC Press.

Vacca, J. (2013). Computer and information security handbook (Second edition). Waltham, MA: Morgan Kaufmann.

Vaughan-Nichols. (2011). No privacy on Amazon's cloud. Retrieved from http://www.zdnet.com/article/no-privacy-on-amazons-cloud-drive/

Wolken, M. (n.d.) Building an ethical big data practice. CIOReview. Retrieved from http://bigdata.cioreview.com/cxoinsight/building-an-ethical-big-data-practice-nid-1794-cid-15.html

Wohlsen, M. (2014). The next big thing you missed: Thanks to Amazon, time sellers can now reach across the globe. Wired Magazine. Retrieved from http://www.wired.com/2014/08/the-next-big-thing-you-missed-thanks-to-amazon-tiny-sellers-can-now-reach-across-the-globe/