J. of the Acad. Mark. Sci. (2017) 45:160–163
DOI 10.1007/s11747-016-0502-9

COMMENTARY

Broadening marketing's contribution to data privacy

O. C. Ferrell[1]

Published online: 8 October 2016

Introduction

Data privacy is one of the most important issues facing marketing today. Providing knowledge on the current state of privacy scholarship is an effective starting point to advance understanding and solutions to this important issue. Martin and Murphy's (2017) multi-dimensional classification of scholarship related to consumer, organizational, ethical, and legal domains is an excellent review of contributions. The assumption from this multi-dimensional approach is that we may have identified the most important data privacy issues in marketing. While marketing scholarship has contributed to understanding that advances managerial decisions and public policy, there are dimensions that have not been addressed in existing research. Unfortunately, organizations and consumers cannot control the data privacy environment through ethical conduct, and the legal environment often fails to stop data piracy. Cybercrime, such as identity theft and online fraud, is a major concern of the Federal Trade Commission (FTC).

Information technology advances result in rapid change that moves through society, affecting all institutions. These advances are usually self-sustaining and serve as a catalyst for even more change. Issues relating to data privacy and big data emerge on a constant basis. For example, the FTC considers ransomware as one of the most challenging cybersecurity issues. Hackers, using software to access consumer and business computers, encrypt files including critical data and demand a ransom in exchange for providing a key to decrypt the files. There are firms, such as the NSO group, that legally sell surveillance tools to capture all activity on smartphones. These products are sold to government and law enforcement, and the company has an ethics committee to vet potential customers. Cyberarms operate in a legal, "gray" area and have been called "digital weaponry" (Perlroth 2016).

There is a need to evaluate and advance knowledge in this critical area of consumer protection. An assessment of advances through consumer, organizational, ethical, and legal domains should be helpful in describing and analyzing the data privacy environment. On the other hand, academic research needs to examine why data breaches occur and conduct research that could address the risk for consumers and organizations. Most data piracy comes from the external environment beyond the direct control of consumers, organizations, and regulators.

My position is that academic marketing research is focused on existing conceptual frameworks, methods, and stakeholders and is not addressing the most important issues. I agree with Martin and Murphy (2017) that "marketing practice using consumer data and analytics has advanced at a more rapid pace than has marketing academic scholarship." Many of the theoretical frameworks used in academic research have not advanced knowledge. The deep analysis of past privacy scholarship may not unearth directions for relevant future research. Privacy research should be grounded in existing knowledge and needs a refocus to address this rapidly changing digital environment. The focus should be on the issues that relate to protecting consumers, organizations, and enhancing public policy. The failure to address the uncontrollable environment related to cybercrime is a serious limitation.

Taking care of stakeholders

Consumers, organizations, and regulators are important stakeholders in data privacy. Each has a unique interest and

✉ O. C. Ferrell
ocferrell@gmail.com

[1] Distinguished Professor of Leadership & Business Ethics, Jack C. Massey College of Business, Belmont University, 1900 Belmont Blvd, Nashville, TN 37212, USA

responsibility in their interface with marketing. Marketing activities in organizations involve the collection and utilization of massive amounts of consumer data. There are ethical and legal responsibilities to maintain an acceptable level of privacy, and not all of these issues have been addressed in marketing privacy literature. Today, most consumers have to sacrifice their privacy to exist in the digital world. To be competitive, firms use data analytics and big data to understand consumers. This opens the door to those who want to exploit these large data files. There are so many risks that the National Institute for Standards and Technology (NIST) was asked by the U.S. government to become an authoritative source for information security best practices (Romanosky 2016).

Organizations have the opportunity and responsibility to protect consumer data. Both ethical and legal considerations should be incorporated into organizational data privacy management. From an ethical perspective, a data privacy culture should include the development of principles, values, norms, and best practices that meet consumer and regulatory expectations and requirements for privacy. Therefore, establishing a data privacy culture in an organization should be a top priority.

The organizational culture should be an advocate for increased cybersecurity internally as well as through effective public policy efforts. As organizations demand even more data from consumers they should include an assessment of the risks as well as the methods of protection. Marketing research needs to address the interface between acquiring and using data and cybersecurity.

Marketing requirements for utilization of big data and the use of marketing analytics to remain competitive means that most organizations at risk, especially from criminals that hack their data systems. Well-known firms including Target, Home Depot, J.P. Morgan, and Sony have all been the victim of hacking attacks. As the Target hacking scandal demonstrates, strong security protocols are useless if the firm does not heed warning signs and take action to prevent hacking attacks. Target's $1.6 billion detection tool detected the initial hacking and flagged Target's security team, but no action was taken until after 40 million credit card numbers had been stolen from its databases (Riley et al. 2014). As they develop better security tools and software, cybersecurity specialists must constantly work to stay one step ahead of hackers, who are discovering ever more sophisticated ways to bypass security protections.

Privacy ethics is a good start

Martin and Murphy (2017) address important normative and descriptive areas of ethics that provide opportunities to understand the role of ethics and compliance in enhancing the integrity of data privacy. In addition, organizations interface constantly with the legal and regulatory community in developing compliance but often also engage in conflicts concerning regulatory requirements for data protection. The regulatory community is important in addressing consumer protection and the criminal element that engages in data piracy. There is a need to explore progress gaps and perspectives that encourage meaningful research.

Ethics is part of almost every strategic decision in the digital world. Understanding the risks associated with electronic point-of-sale systems and branded mobile apps, examples of widely used digital systems that put consumers at risk, is ipmortant. These systems can contain diverse and sensitive data such as health and medical records as well as credit card and social security numbers. Research is needed to address the ethical dimensions of these risk areas.

There is a need for research in data privacy using a normative ethical perspective such as social contract theory. Collective stakeholder norms based on integrative stakeholder theory (Donaldson and Dunfee 1994) can provide normative rules for all stakeholders, including organizations, consumers, and regulators. On the other hand, organizations may accept or comply with stakeholder norms on privacy or avoid complying with these so-called hypernorms. There will be considerable variation in how organizations address norms on data privacy. This is because organizational norms will stipulate which stakeholders are important and whether data privacy is a top priority, including the ability to provide resources and policies to protect consumers (Maignan and Ferrell 2004). While these "ought to do" concepts are helpful, they can be applied to any ethical dilemma. Therefore, decision makers have to use their own judgments in reaching conclusions related to privacy.

Social contracts rest on the foundation of fairness. The Federal Trade Commission has developed a policy statement on unfairness that focuses on the harm an act or practice can cause (Ohlhausen 2014). The concept of unfairness could be applied to data privacy risk assessment and the prevention of data breaches. Martin and Murphy (2017) do an excellent job of outlining normative frameworks that could be used to establish fairness in privacy, including justice theory and power–responsibility equilibrium. While these frameworks may explain how fairness expectations evolve, it does not explain how to manage privacy in an organization or in a regulatory agency such as the FTC. These normative foundations drive our values and norms. Beyond values and norms are activities, policies and plans.

Descriptive ethical decision models help to advance understanding of how ethical decisions are made in an organization. Hunt and Vittell (1986) provide a descriptive model that explains how normative reasoning enters into the decision process. Normative and descriptive ethical models are complementary, not alternative models. Ferrell and Gresham (1985) provide a descriptive model for understanding ethical decision making in organizations. For privacy decisions, the model would indicate individual values and attitudes (derived from normative foundations), organizational factors (the impact of significant others), and opportunity (policies and compliance requirements). Therefore, descriptive ethical models

can provide a framework for empirical research to learn more about how ethical decisions about privacy are made in the context of an organization. More information must be known about the effectiveness of codes of ethics that specifically address data privacy. For example, it has been found that a specialized code of ethics for top financial and accounting officers improves the integrity of financial reporting (Ahluwalia et al. 2016). Specialized data privacy codes should help organizations create a more effective data privacy culture that provides ethical decisions.

Most important is an understanding of the risks to the organization and consumers and the development of effective cybersecurity. In the current information technology environment, data breaches and piracy will most likely happen. All organizations must determine their data privacy risks and have a contingency or crisis management plan about how to respond when a data breach occurs. This plan needs to be embedded in an effective ethics and compliance program for data privacy and security. The view that social contracts, values, norms, and policies can be an effective deterrent in cybersecurity fails to address the most important risks. Since many risks are external, organizations need to collaborate on risk management. Other research, such as Romanosky (2016), provides an analysis of federal data breach lawsuits. Therefore, there is some progress in understanding cybercrime and the risk areas to manage.

The missing link in data privacy research

Most data privacy research conducted in marketing focuses on consumer, organizational, ethical, or legal silos. There have been many helpful, descriptive studies that document data security issues and gaps in knowledge. However, criminal activities that constantly attack both consumer and organizational data are not included in data privacy research in marketing. A search of Martin and Murphy's (2017) review indicates that there are no articles cited in the references that use the word "criminal" or "crime" in the title. This is because marketing research has focused more on consumer and organizational behavior in the title of the article. If marketing is to advance knowledge, it needs to address the criminal elements. White-collar crime represents some of the most devastating and destructive damage associated with data privacy. According to the Department of Justice, a white-collar crime is "a non-violent criminal act involving deceit, concealment, subterfuge, and other fraudulent activity." These white-collar data pirates are highly educated and are often more skilled in information technology operations than leading software experts and even top technology companies. As we have seen, anyone with the ability to hack into what is believed to be highly secured and sensitive data systems can commit a white-collar crime that can cost millions of dollars and the reputation of a company. The cost of a typical cyber incident is slightly less than $200,000 (Romanosky 2016). Identity theft, overpayment fraud, advanced-fee fraud, as well as non-delivery of merchandise are all top Internet scams, according to the Department of Justice.

Possibly one of the greatest risks is complacency by both consumers and organizations in protecting their data and privacy. Akhter (2014) found that internet self-efficacy affects privacy concerns negatively. Privacy concerns affect the frequency of online transactions negatively. This type of social psychological research demonstrates why organizations must assure consumers that their privacy is protected and secure. This confirms the importance of privacy concerns in purchasing online.

We need to advance marketing research to address and develop frameworks and an awareness of issues that will assist in investigating the current state of cybersecurity. With data breaches occurring on an ongoing basis, and consumers experiencing the consequences, the concept of secure online transactions may be fading. Therefore, more needs to be known about the erosion of consumer trust of organizations reputations and brand image. Cybersecurity is unlike many so-called controllable marketing decisions. How can we develop trust when the problem is often external and uncontrollable?

The research agenda going forward

No matter who you are or the nature of your organization, there is probably a hacker targeting your data. Therefore, the opportunity exists for research to advance the understanding of what types of consumer data is needed and how to protect it. Research to evaluate the effectiveness of privacy policies, or a specialized organizational privacy code of ethics, is the first step for organizations managing big data and using data analytics to make decisions. There is a need to determine data privacy risks and how to develop a contingency plan to address those risks when there is a data breach. Remember that Target detected the initial hacking, but no action was taken until credit card numbers were stolen. Research to understand and advance risk management related to data security is an important gap in data privacy research.

Research related to data breach disaster recovery is needed to assist understanding of how to cope with data breaches. A focus on issues related to consumer-centric communication plans would be helpful to avoid reputation loss. Assisting consumers in rebuilding trust after a data breach is an important marketing issue that needs research. Martin and Murphy (2017) address the "understanding of 'firm recovery strategies' to re-energize consumers after massive privacy failures," representing a noticeable gap in the current state of research.

More research is also needed to understand the external environment that is the most significant threat to data privacy. Rather than deep understanding and narrow research in organizational, ethical, or legal silos, there need to be synergies that direct this understanding to the broader risk issues, especially cybercrime. Existing knowledge may be useful in

protecting consumers and preventing data breaches. The criminal element that is the most significant risk has to be included in data privacy marketing research.

I believe an examination of theories and research from the field of criminology will advance our knowledge in the area of data privacy. Criminologists use psychology, anthropology, and sociology to study how and why people commit crimes. This understanding could be useful in controlling, protecting, and developing regulations that help safeguard data privacy. Knowing how cybercriminals threaten security is the first step in assessing data privacy risks. Understanding structural chokepoints and interventions reducing opportunities and incentives to engage in online crime through increasing operational costs and the risk of apprehension is important (Leontiadis and Hutchings 2015). Marketing has the opportunity to integrate knowledge about consumer behavior, internal organizational environments, and the regulatory community in addressing the role of the external environment and cybercriminals in advancing a holistic approach to knowledge on data privacy.

References

Ahluwalia, S., Ferrell, O.C., Ferrell, L., & Rittenburg, T. (2016). "Sarbanes-Oxley 406 Code of Ethics for Senior Financial Officers and Firm Behavior," *Journal of Business Ethics*. doi:10.1007/s10551-016-3267-7.

Akhter, S. H. (2014). Privacy concern and online transactions: the impact of internet self-efficiency and internet involvement. *Journal of Consumer Marketing, 31*(2), 118–125.

Donaldson, T., & Dunfee, T. W. (1994). Toward a Unified Conception of Business Ethics: Integrative Social Contracts Theory. *Academy of Management Review, 19*(2), 252–284.

Ferrell, O. C., & Gresham, L. G. (1985). A Contingency Framework for Understanding Ethical Decision Making in Marketing. *Journal of Marketing, 49*(3), 87–96.

Hunt, S. D., & Vittell, S. (1986). A General Theory of Marketing Ethics. *Journal of Macromarketing, 6*(1), 5–16.

Leontiadis, N., & Hutchings, A. (2015). Scripting the Crime Commission Process in the Illicit Online Prescription Drug Trade. *Journal of Cybersecurity, 1*(1), 81–92.

Maignan, I., & Ferrell, O. C. (2004). Corporate Social Responsibility and Marketing: An Integrative Framework. *Journal of the Academy of Marketing Science, 32*(1), 3–19.

Martin, K. & Murphy, P. (2017). "The Role of Data Privacy in Marketing," *Journal of the Academy of Marketing Science, 45*(2). doi:10.1007/s11747–016–0495-4.

Ohlhausen, M. K. (2014). Privacy Challenges and Opportunities: The Role of the Federal Trade Commission. *Journal of Public Policy and Marketing, 33*(1), 4–9.

Perlroth, N. (2016). How Spy Tech Firms Let Governments See Everything on a Smartphone. *New York Times, September, 2*, A1.

Riley, M., Elgin, B., Lawrence, D. & Matlack, C. (2014). "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," *Bloomberg Business,* retrieved on August 19, 2016 from http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data.

Romanosky, S. (2016). Examing the Costs and Causes of Cyber Incidents. *Journal of Cybersecurity*, 1–15.