Journal of Information Privacy and Security

ISSN: 1553-6548 (Print) 2333-696X (Online) Journal homepage: http://www.tandfonline.com/loi/uips20

Utilizing normative theories to develop ethical actions for better privacy practices

Zareef A. Mohammed, Gurvirender P. Tejay & Joseph Squillace

To cite this article: Zareef A. Mohammed, Gurvirender P. Tejay & Joseph Squillace (2017) Utilizing normative theories to develop ethical actions for better privacy practices, Journal of Information Privacy and Security, 13:4, 296-315, DOI: 10.1080/15536548.2017.1419018

To link to this article: https://doi.org/10.1080/15536548.2017.1419018

Published online: 29 Dec 2017.

JOURNAL OF INFORMATION PRIVACY AND SECURITY
2017, VOL. 13, NO. 4, 296–315
https://doi.org/10.1080/15536548.2017.1419018

Routledge
Taylor & Francis Group

Utilizing normative theories to develop ethical actions for better privacy practices

Zareef A. Mohammed[a], Gurvirender P. Tejay[b], and Joseph Squillace[c]

[a]Department of Management, Information Systems, & Analytics, State University of New York (SUNY), Plattsburgh, NY, USA; [b]College of Business, St. Thomas University, Miami, FL, USA; [c]College of Engineering and Computing, Nova Southeastern University, Fort Lauderdale, FL, USA

ABSTRACT

This study examines the privacy practices of organizations. We argue that successful deployment of privacy practices based on ethical actions will strengthen privacy protection measures to better protect clients' PII. We propose a set of ethical actions based on six normative theories following multiple case study approach to study three prominent data breaches. Our analysis indicates that ethical actions based on normative theories can be effective in developing better privacy practices for organizations. The theory that has the strongest effect on privacy practices is the deontological approach, while the liberal-intuitive has the weakest effect on privacy practices.

Introduction

For organizations to retain a competitive advantage, they require personally identifiable information (PII) of their clients so as to build better relationships and offer better services (Awad & Krishnan, 2006; Culnan & Armstrong, 1999). Yet, polls and surveys have indicated that within the past decade, there is an increased concern from individuals over the privacy of their PII (Dinev & Hart, 2006; Madden, Fox, Smith, & Vitak, 2007; Smith, Dinev, & Xu, 2011) with an increasing number of data breaches. Individuals' PII is at risk when they disclose it to an organization, and even after original data breaches occur, they are vulnerable to further incidents (Culnan & Williams, 2009). While individuals accept the need to disclose their PII to organizations in order to complete a business transaction, studies have indicated that they need to perceive their information is handled fairly (Culnan & Armstrong, 1999; Malhotra, Kim, & Agarwal, 2004), while retaining a level of control over their information (Malhotra et al., 2004). Similarly, individuals require a level of trust and a sense of assurance that organizations would protect their PII (Belanger, Hiller, & Smith, 2002).

Fair information practices (FIPs) were developed to protect individuals' PII and impose some accountability on organizations that collected PII (Schwaig, Kane, & Storey, 2006). Essentially, organizations were required to notify their clients of their information practices and allow their clients access to collected PII (FTC, 2006; Liu & Arnett, 2002). However, even with the adoption of FIPs, there are no direct privacy practices offered to individuals to protect their PII, nor do they attain assurances that privacy of their PII would be managed properly by the organization. Legally, organizations are required to implement the "mandatory minimum requirements" necessary to stay in compliance and avoid heavy government fines. Moreover, research has indicated that organizations do not fully comply with FIPs (Hsu, 2006 Liu & Arnett, 2002; Scwhaig et al., 2006).

CONTACT Zareef A. Mohammed zmoha003@plattsburgh.edu 101 Broad Street, Au Sable Hall, Office 315, Plattsburgh, NY-12972.

Evidence indicates that some data breaches could have been averted had the organizations applied proper security and privacy measures (Baker, Hylender, & Valentine, 2008). However, Schwaig et al. (2006) found that less than 4% of the fortune 500 companies complied with all four dimensions of FIPs. The most notable compliance was the dimension of notice (Liu & Arnett, 2002; Schwaig et al., 2006). Liu and Arnett (2002) reported low percentages of websites including access, choice, and data security within their privacy policies. As such, organizations' privacy practices need to be reevaluated and reformed so as to properly protect their clients' PII. For this study, we examine the privacy practices that should be adopted by organizations in order to better protect their clients' PII.

Culnan and Willaims (2009) argued that organizations have a moral responsibility to protect their clients and could enhance their privacy practices by going beyond laws and regulations to incorporate ethical actions. Specifically, Culnan and Williams (2009) suggested a number of privacy principles that organizations should adopt. These principles included creating a culture of privacy, implementing governance processes for privacy, and avoid decoupling (disassociating organizational processes from the personal implications). We extend the work of Culnan and Williams (2009) by arguing that successful deployment of specified ethical actions within corporate privacy practices will strengthen implemented privacy protection measures. To achieve the objective of our study, we propose a set of ethical actions that could be implemented to strengthen privacy practices. We draw upon Siponen and Iivari (2006) to emphasize the role of normative theories in developing such ethical actions.

Our research contributes to the field of privacy by providing set of ethical actions that organizations can adopt to enhance the protection of their clients' PII. Moreover, our research contributes to the limited research at the organizational level in the information privacy field (Belanger & Crossler, 2011; Smith et al., 2011). The rest of the article is structured in seven sections. Next section presents a review of prior literature followed by section on theoretical basis of this research study. The subsequent sections provide data collection and analysis of three data breach cases followed by discussion of implications for privacy. We then conclude the article by outlining limitations of this study and explore directions for future research.

Literature review

Privacy is a heavily discussed subject in philosophy and other social sciences such as psychology, sociology, and law (Smith et al., 2011). Yet, despite centuries of debate among philosophers and researchers, privacy is still difficult to define (Belenger & Crossler, 2011; Smith et al., 2011). The complexity of privacy may be due to its broad nature, multidimensionality, and relevance to a particular society's cultural values (Culnan & Williams, 2009; Smith, 1993). Furthermore, privacy is broader than information privacy, where information privacy is related to how PII is used, and who has access and control over such PII (Solove, 2006). However, similar to the general concept of privacy, information privacy has often been defined into four categories of value-based definitions (privacy as a right or privacy as a commodity), and cognate-based definitions (privacy as a cognitive-state or privacy as a control) (Smith et al., 2011).

Stemming from a human rights' perspective, privacy (and subsequently information privacy[1]) could be defined as the right to be left alone (Smith et al., 2011; Warren & Brandeis, 1890). Essentially, an individual's ability to keep his/her PII private is a human right awarded by the state. Even in the case where an individual was to disclose his/her PII to some entity (human or organization), that PII must be used only based on the permission of the owner, as well as protected by the entity that has access to it (Alderman & Kennedy, 1997; Smith et al., 2011; Solove, 2007). Yet, when privacy was observed in the context of consumer behavior, a privacy paradox was found, where consumers were willing to disclose their PII for specific benefits, despite claiming concerns for the privacy of their PII (Smith et al., 2011). Essentially, this led to the notion that privacy could be

[1]From this point onwards, the term "privacy" will be referring "information privacy" and not the umbrella term of *privacy*.

defined as a commodity, where individuals would trade their PII for something of equal value (Smith et al., 2011). Numerous researchers have used this definition of commodity in their study of privacy, such as Dinev and Hart (2006) who explained that individuals would undergo a cost–benefit analysis of salient but contrary factors when deciding to disclose or withhold their PII.

Cognate-based definitions of privacy as a state and privacy as a control differ from that of value-based definitions (right and commodity) in the overview that privacy is not an absolute value to society but rather subjective to individuals' perceptions and beliefs (Smith et al., 2011). Privacy as a cognitive state is explained as an individuals' state of limited access to himself/herself, and in the case of privacy, the state of limited access to his/her PII (Smith et al., 2011). Essentially, an individual's state is based on a continuum which lies anywhere between "no privacy" and "absolute privacy" (Smith et al., 2011). Conversely, the definition that privacy is a control is explained as the "selective control of access to the self" (Altman, 1975, p. 24). Westin (1967) defined privacy as the control an individual has over the collection and use of his/her PII. An individual may perceive a degree of control over his/her PII, which may be why he/she would be willing to disclose it to others.

Prior studies in privacy have often focused on issues such as the privacy paradox, so as to understand why individuals would disclose or withhold PII (Acquisti & Grossklags, 2005; Dinev & Hart, 2006; Pavlou, Liang, & Xue, 2007; Van Slyke, Shim, Johnson, & Jiang, 2006). Many of these studies focused on different contexts such as personalization (Awad & Krishnan, 2006; Culnan & Armstrong, 1999), e-commerce adoption (Acquisti, 2004; Belanger et al., 2002; Dinev & Hart, 2006; Dinev et al., 2006; Pavlou et al., 2007; Van Slyke et al., 2006), health care (Anderson & Agarwal, 2011; Angst & Agarwal, 2009; Bansal, Zahedi, & Gefen, 2010), and location-based services (Xu, Teo, Tan, & Agarwal, 2010). The role of privacy may have different effects on these various contexts, such as in the case of health care as explained by Anderson and Agarwal (2011), where the nature and risks are different, as well as the emotions an individual has over his/her medical state has to be considered. However, despite the rich literature in understanding individuals' behavior with regards to privacy, little research exists explaining how organizations should handle PII they have collected about individuals (Culnan & Williams, 2009).

According to Culnan and Willaims (2009), when organizations collect and process individuals' PII, problems may arise that could potentially harm such individuals. These problems could be classified into major categories of *information reuse* and *unauthorized access to PII* (Culnan & Williams, 2009). Essentially, organizations could legally reuse individuals' PII; however, the outcome of such reuse is often unknown to the individuals. This information reuse may cause possible harm to the individual, such as in the case of an organization sharing this collected PII with other organizations (Culnan & Willaims, 2009). On the other hand, unauthorized access is concerned with both the illegal internal and external use of PII. This may occur when an employee accesses PII the organization he/she works for but does not have sufficient access rights to do so. Unauthorized access may also include data breaches, where individuals who are not a part of the organization gain access to the PII the organization has collected (Culnan & Williams, 2009). Indeed, it is upon the organization to apply appropriate protection to the PII they have collected, as well as use such PII only based on the permissions of the individual owner of collected PII (Solove, 2006). Yet, organizations privacy practices were found to be reactive and driven by external threats, which is not adequate enough for organizations to protect the privacy of the PII they have collected from individuals (Greenaway & Chan, 2005; Smith, 1993).

A number of laws and regulations have been enacted so as to increase organizations privacy practices, such as the FIPs, fair credit reporting act (FCRA), health insurance portability and accountability act, and section 5 of the Federal Trade Commission Act (Culnan & Willaims, 2009). In the United States, many of these privacy regulations are self-regulated and sector specific (Rose, 2006). This often leads to a great deal of flexibility in organizations' privacy practices with respect to regulations. Studies have found that many organizations belonging to the fortune 500 failed to completely implement FIPs (Liu & Arnett, 2002; Schwaig et al., 2006). Similarly, Peslak (2006) found that while the 73% of the fortune 100 websites post privacy

notices, they were not comprehensive of all the dimensions of FIPs. Furthermore, even if organizations were to adhere to necessary privacy laws and regulations, these laws and regulations do not guarantee that privacy is achieved since they are also often reactionary and outdated by the time they are enacted (DeGeorge, 2006).

Culnan and Williams (2009) argued that organizations' privacy practices could be enhanced through ethical reasoning. While Smith et al. (2011) indicated that privacy does not equate to ethics and that empirical privacy-related research could be conducted without ever considering ethics, Mason (1986) explained that ethics is related to privacy. Accordingly, an organizations' adoption of ethical practices in informing their privacy practices is a moral responsibility, as well as a benefit to the organization (Culnan & Williams, 2009). It is upon the organization to ensure that any business between them and their clients is completed, as well as to ensure that further exchanges would occur by retaining that client (Caudill & Murphy, 2000). Ethics is thus considered good business, whereby proactive privacy practices would retain consumers (Culnan & Williams, 2009). Furthermore, by applying ethical reasoning to privacy practices, organizations would be more compliant with laws and regulations, thereby avoiding the negative consequences of violating those regulations (Culnan & Williams, 2009).

Theoretical basis

Organizations should make a moral commitment to better their privacy practices so that their clients' PII is well protected. As indicated by Culnan and Williams (2009), organizations should avoid harm that could be caused due to the way they handle PII. Additionally, organizations should recognize that "ethics is good business" (Culnan &Williams, 2009, p. 683). Essentially, Culnan and Williams (2009) explained that since consumers are vulnerable, organizations should try to protect them, as it is a moral responsibility. If consumers acknowledge organizations' attempts at protecting their PII, they will be more likely to disclose it to organizations.

While Culnan and Williams (2009) recommended that organizations should build a culture of privacy, implement governance processes for privacy, and avoid decoupling of privacy, the question of how this could be done arises. Siponen and Iivari (2006) proposed six normative theories that could be used in addressing "exceptional situations" (i.e., situations that are not covered in a policy), so as to safeguard critical information assets. These theories include conservative deontological theory, liberal-intuitive, virtue design, prima-facie, utilitarian, and universalizability theories. We can apply these theories to better organizations' privacy practices. Specifically, organizations should handle consumers' PII in an ethical manner so as to protect consumers from privacy-related threats (Culnan & Williams, 2009). Table 1 presents the six normative theories along with ethical actions derived from these theories.

The conservative deontological theory posits that objective moral rules exist, which are mandatory to follow (Siponen &Iivari, 2006). The rules should consist of every possible situation, while deviation from the rules is forbidden. Specifically, if an action was not sanctioned by the rules governing a situation, the action is regarded as forbidden. Based on this theory, there are two ethical actions of *comprehensiveness* and *voluntariness* (Siponen & Iivari, 2006). The action of voluntariness defines the degree to which objective rules should be followed (i.e., either they are voluntary or mandatory). With regards to privacy practices, a set of obligatory rules should be comprehensive exhausting as many situations (Siponen & Iivari, 2006). While organizations are required to abide by certain standards and laws (such as FIPs and FCRA), they should also develop comprehensive privacy policies. Furthermore, organizations need to reinforce the necessity of privacy practices among their employees.

The liberal-intuitive theory is antithetical to the conservative deontological theory in that it assumes individuals would make autonomous decisions. Thus, a set of objective rules should only consist of necessary actions, while allowing individuals to make their own moral judgments. Essentially, if an action is not specified as forbidden within the rules, it should be regarded as

Table 1. Normative theories and ethical actions.

Normative theory	Description	Ethical actions
Conservative deontological theory	Ethical actions are based on a set of absolute rules whereby deviation from such rules is considered forbidden	Comprehensiveness, voluntariness
Liberal-intuitive theory	Only the necessary rules should be defined, while individuals are free to make autonomous ethical decisions	Necessary rules and procedures, voluntariness
Virtue-design theory	A moral agent is virtuous if he/she was to engage in supererogatory actions that would produce better outcomes	Virtuousness, voluntariness
Prima-facie theory	The moral agent should perform an action with greater expected net benefits	Comprehensiveness, voluntariness, expected net benefits
Utilitarian theory	Ethical actions are actions that achieve an outcome of happiness for everyone involved in a situation	Comprehensiveness, voluntariness, happiness
Universalizability theory	An action is only morally right if everyone can perform such action	Comprehensiveness, voluntariness, universalizability

allowed (Siponen & Iivari, 2006). A limitation of the conservative deontological theory is that despite its comprehensiveness, situations may exist that are not included within the objective rules. The actions an individual may take to address these exceptional situations however would be regarded as forbidden. Yet, under the liberal-intuitive view, such actions would be allowed. The ethical actions derived from the liberal-intuitive theory are *voluntariness*, and *necessary rules and procedures*. Organizations should only define the necessary rules and procedures to safeguard sensitive PII. These rules and procedures, however, are considered mandatory (i.e., less voluntary). Organizations should therefore go beyond laws and standards that they are required to follow and implement privacy practices that they deem as salient in better protecting PII.

The virtue design theory posits that ethical actions are supererogatory (voluntary), and performance of such actions would produce better outcomes (Siponen & Iivari, 2006). The individual is regarded as virtuous if they behave ethically. However, if these ethical actions are not followed, the individual is not considered guilty of wrongdoing (Siponen & Iivari, 2006). The ethical actions derived from this theory are *voluntariness* and *virtuousness*. For instance, an organization's implementation of strong privacy practices and going beyond obligations are voluntary but would be virtuous.

The prima-facie theory, utilitarian theory, and universalizability theory are all used in exceptional situations that obligatory comprehensive rules do not cover. Essentially, they explain the actions individuals could take to address these situations and are considered ethical. Similar to the conservative deontological theory, these three theories consist of the ethical actions of *voluntariness* and *comprehensiveness*. However, unlike the conservative deontological theory, actions not included in the obligatory rules are not considered forbidden but are accepted based on some criteria.

The prima-facie theory is based on exceeding the obligations governing a situation. Essentially, an exceptional situation could be addressed based on estimated net benefits. If the expected benefits of performing an action to address the exceptional situation exceed the expected benefits of not performing the action, then it is recommended for that action to be performed (Siponen & Iivari, 2006). Therefore, the *expected net benefit* is the third ethical action based on the prima-facie theory.

Under the utilitarian theory, actions that maximize felicity are considered ethical. Felicity is described as the presence of pleasure and the absence of pain (Siponen & Iivari, 2006). Therefore, in protecting privacy of consumers' PII, for situations that are exceptional, organizations should perform actions that would achieve happiness for every entity involved. Ethical action of *comprehensiveness, voluntariness*, and *happiness* are derived from the utilitarian theory. However, the universalizability theory posits that an action is deemed morally right if it could be performed by everyone (Korsgaard, 1985). Therefore, *universalizability* is the third ethical action derived from the universalizability theory. Organizations should therefore consider taking actions to protecting the privacy of consumers' PII as if it were their own information.

The six normative theories discussed above serve as underlying theoretical basis of our study. We utilize these to analyze privacy practices at three organizations that suffered data breaches. These cases are discussed next.

Data collection

We followed multiple case study approach. The study involved secondary data from three prominent privacy breaches: the ChoicePoint data breach in 2006, the South Carolina Department of Revenues (SCDOR) data breach in 2012, and the Equifax data breach of 2017. The ChoicePoint data breach is used as the primary case of analysis for this study since it was amongst one of the first incidents of a major data breach that affected thousands of individuals. It is one of the most feasible cases in examining the application of ethical actions to the privacy and security practices implemented before and after the data breach. Specifically, ChoicePoint suffered great financial losses, as well as, stigmatization by the general public. The impact by the ChoicePoint incident became exemplary for other organizations with regards to their security and privacy practices in history.

The SCDOR data breach case in 2012 was chosen, as the incident occurred within the past 5 years despite the increased recognition by government and organizations for the betterment of privacy and security practices. Moreover, this impacted 6.4 million individuals and multiple organizations under the context of a government-controlled institute, which was supposed to have stronger privacy and security practices due to regulations. Finally, the Equifax data breach was one of the most recent and impactful data breaches of 2017, affecting 143 million consumers in the United States, whereby PII as sensitive as Social Security numbers were compromised (Privacy Rights Clearinghouse, 2017). In summary, the ChoicePoint case is studied as the primary case due to the impact it had with SCDOR and Equifax serving as sub-cases to support our analysis.

Case: ChoicePoint data breach

The data broker, ChoicePoint, collected and sold consumers' PII to the government and organizations. The company collected data from a number of third-party sources such as public records, insurance claims, and credit reports, and usually without any direct contact from the individual (Culnan & Williams, 2009). In February 2006, in compliance with the California Security Breach Notification Law, which required organizations to inform their affected consumers of a compromise to their PII, the company disclosed that they suffered a data breach (Litan, 2006). Some of the subscribers created fake accounts through which they could purchase consumer data profiles. Furthermore, they used commercial mail drops as business addresses in order to obtain consumers' PII. The consequences of the fraudulent access of consumers' PII led to an initial impact on 140,000 individuals whose PII were compromised and were now victims of identity theft (Litan, 2006). However, upon further review of the case, it was found that the number of affected records was actually 165,000 individuals (Privacy Rights Clearinghouse, 2017). ChoicePoint was faulted for failing to properly verify the identity of their subscribers, as well as neglecting to investigate the intentions toward the use of the data profiles that were purchased and collected (FTC, 2006).

ChoicePoint suffered a number of costs due to the data breach. Apart from the negative press, ChoicePoint lost 22% of their consumers, as well as stigmatized with the term "identity theft" (Litan, 2006). ChoicePoint had violated section 5 of the FTC Act, which prohibits organizations from unfair or deceptive acts or practices. Furthermore, the FTC charged ChoicePoint with violations of FCRA. This led to ChoicePoint spending $10 million in civil penalties, and a further $5 million for consumer redress (FTC, 2006; Litan, 2006). Overall, ChoicePoint suffered $30 million in costs due to the breach (Culnan & Williams, 2009). ChoicePoint was required to comply with an injunction for a 20-year period, whereby they had to credential their subscribers that were regulated by the FCRA, inspect some of the specific consumers' facilities, and conduct individual audits while being monitored by and reporting to the FTC (Litan, 2006). Companies that would do business with ChoicePoint were also

among the victims of the data breach since ChoicePoint had to apply correctional methods to turn-around damages caused by the data breach (Culnan & Williams, 2009). Specifically, ChoicePoint had to limit the type of information they sold, as well as the types of subscribers they sold to (Culnan and Willaims, 2009, Litan, 2006).

Privacy enhancing practices implemented after data breach. The data collected about ChoicePoint's privacy practices after the data breach are derived from a case study by Litan (2006). ChoicePoint redesigned their data and security practices whereby their goals were better knowing their consumers, transparently working with their consumers, and establishing a framework of enhanced controls for their organization. To improve their privacy policy, ChoicePoint implemented the Generally Accepted Privacy Principles (GAPP), developed by the American Institute of Certified Public Accountants (AICPA) and Canada Institute of Charted Accountants. The security policy was developed based on the ISO 17799 standard (formerly BS7799, but as of 2007, it was renamed to ISO/IEC 27002). ChoicePoint further created its own standard for customer credentialing, since no industry standard existed at the time. ChoicePoint focused on organizational governance, credentialing, technology, training, and compliance as the key areas to recover from the fallout caused by the data breach.

ChoicePoint hired a Chief Credentialing, Compliance and Privacy Officer (CCCPO), who managed the company's privacy program, was responsible for the compliance and auditing of ChoicePoint's consumers, and was responsible for the credential processes. The CCCPO reported to the Privacy and Public Responsibility Committee of ChoicePoint's board of directors. Information Security, customer support and credentialing programs were operated and owned by the Chief Information Officer (CIO). With minimal exceptions, ChoicePoint's customers were subject to extensive examination, including site visits to potential consumers. A credentialing checklist was employed, with separate site checklists that were confidential. ChoicePoint conducted physical site inspections, which was a response to address the fraudulent accounts and mailboxes that were used by the offenders in the data breach. ChoicePoint decided to discontinue business with those who were found difficult to be credentialed. Consumers were required to certify that they would use data profiles for permissible purposes, while third-party service providers and resellers were required to complete self-assessments of their data security practices. ChoicePoint also performed audits of their subscribers, whereby they would suspend or terminate the accounts of any subscriber that did not meet their standards.

To manage their data, ChoicePoint inventoried their files and applications, where proper protections were applied, and random machines were audited for individuals' PII, and proper security was applied to sensitive information. Furthermore, ChoicePoint developed a data classification tool which informed them of data protection and retention requirements. ChoicePoint encrypted their data, which included database encryption of their credit card processing, in compliance to the Payment Card Industry Data Security Standard, HTTPS, e-mail encryption techniques, and hard-drive encryption. All sensitive information sent to subscribers were truncated by ChoicePoint, thereby depriving subscribers full access to individuals' PII. Only based on specific conditions, subscribers were provided with individuals' full information. Also, ChoicePoint implemented a number of activity monitoring systems that provided efficient warnings of fraudulent behavior.

ChoicePoint mandated all permanent and temporary employees to undergo security and privacy training programs. Similarly, independent contractors were also required to take the training programs. Furthermore, employees were required to undergo privacy training programs annually and score over 80% in these programs. ChoicePoint also implemented a social engineering program for call center employees as they were most susceptible to social engineering attacks.

Case: SCDOR data breach

The SCDOR is a US-based government agency responsible for administering and collecting multiple taxes and registration fees in accordance to the South Carolina state law (South Carolina Department of

Revenue, 2015). Accordingly, SCDOR is responsible for the administration and collection of revenue from more than 32 different taxes and registration fees totaling $8.5 billion tax payments (Loy, Brown, & Tabibzadeh, 2014; South Carolina Department of Revenue, 2015). SCDOR was at the time, the 7th ranked state along with Illinois, Louisiana, Massachusetts, and Utah to process tax filings online with 88% of electronically filed tax returns. In 2012, SCDOR suffered a massive data breach, which was labeled the "mother of management dysfunction," where 3.8 million individual taxpayers and 699,000 businesses were affected through the compromise of PII (Loy et al., 2014). The data breach was considered as the largest data breach from a state information system in the United States (Brown, 2012).

SCDOR was victim of a spear phishing attack (an e-mail disguised as received from a trusted entity) which was carried out by an unknown individual (or group of individuals) from a suspected Eastern European country (Loy et al., 2014). On August 13, 2012, the director of SCDOR, James Etter, opened an e-mail with an attached file. Upon opening the attachment, a malware program was installed on the Etter's office workstation, opening a backdoor port which was redirected to a command and control website. Etter's user credentials were sent to the command and control website, while several utility programs were downloaded to his workstation (Loy et al., 2014). Over the course of August 2012, the attacker logged into the SCDOR's remote access server using Etter's user credentials, gaining access to Etter's workstation, several SCDOR servers, and databases. The attacker then installed a previously downloaded utility program so as to acquire additional user credentials (Loy et al., 2014). Subsequent activity from the attacker included gaining access to more SCDOR servers and reconnaissance. The attacker then proceeded to copy database backup files to a staging directory on the database server, then compressing the files in 7-Zip format. The 7-Zip files were copied from the database server to a staging server before being uploaded to an undisclosed website, after which the attacker deleted all backup and 7-Zip files from the staging server (Loy et al., 2014).

The Governor of South Carolina and SCDOR were notified on October 10, 2012, by the U.S. Secret Service (USS) that the credentials of three SCDOR employees' and PII of South Carolina taxpayers were available for sale on the Internet (Loy et al., 2014). The USS and a forensics team from Mandiant Corporation began investigating the data breach. The Mandiant forensics team proceeded to remove the attacker's access ports and monitor activity for further attacks (Loy et al., 2014). The investigation revealed that SCDOR's information systems contained two crucial vulnerabilities. First, SCDOR had no dual verification protocol to get into system. Etter and previous Director had refused to invest $25,000 to install a dual password authentication system advised by the CIO, despite the fact that all other government state departments had done so (Largen, 2012). The second vulnerability was the Social Security data of individual and business taxpayers were unencrypted (Cohn, 2012).

Overall, the magnitude of data breach resulted in approximately 6.4 million affected individuals. The Mandiant Incident Report (2012) indicated that 44 systems were compromised, and at least 33 unique pieces of malicious software and utilities were installed and used to carry out the attack (Loy et al., 2014). Additionally, a total of 3.3 million bank account numbers were stolen. A credit reporting service, Experian, was contracted by the state, costing $12 million, to provide all affected taxpayers and businesses 1 year of free credit monitoring and identity protection (Loy et al., 2014). The incident resulted in a lawsuit against SCDOR, as well as their contractor at the time, Trustwave (Privacy Rights Clearinghouse, 2017). Overall, the incident cost $14 million (Loy et al., 2014).

Case: Equifax data breach

Equifax, one of the largest credit bureaus in the United States, reported on September 2017 that an application vulnerability on one of their websites led to a data breach that exposed about 143 million consumers. The breach was discovered on July 29, but the company says that it likely started in mid-May. Compromised data included names, date of births, social security numbers, addresses, some driver's license numbers, and 209,000 U.S. credit card numbers (Privacy Rights Clearinghouse, 2017). Among the affected were also Canadian and UK residents (Ragan, 2017).

The Department of Homeland Security had warned Equifax of their data breach but failed to address the vulnerability (Dugan, 2017). As documented by Scipioni (2017), on July 29, Equifax observed suspicious network traffic and stopped it. However, by this time, the attackers had already gained unauthorized access to consumers' PII. Before disclosing the incident to public, three top executives of the company sold nearly 2 million dollars' worth of company stocks. While Equifax did disclose the breach in September, several months after the breach, they claimed that the executives were unaware of the intrusion at the time of selling the stocks.

The data breach to Equifax led to the resignation of top executives including Chief Executive Officer and CIO. The breach also led to backlash from U.S. senators (Scipioni, 2017), as well as lost a $7.2 million contract with the Internal Revenue Services (IRS) (Johnson, 2017). To address the data breach, Equifax allowed affected individuals to enroll in the TrustedID Premier service, which includes clause freeing them of liability in a lawsuit. The service offers consumers free credit monitoring and credit lock services, and up to $1 million in identity theft insurance.

Next section presents our analysis of three data breaches discussed in this section based on underlying theoretical basis presented earlier in the article.

Data analysis

We developed set of ethical actions that could better inform organizations privacy practices and applied it to three cases where an organization suffered a data breach. In this section, we follow Culnan and Williams (2009) in using the case of ChoicePoint as the primary source of analysis, where we examine the data breach that took place, privacy practices that ChoicePoint implemented at the time, and the actions they took after the breach took place. We then applied the set of ethical actions to this case in order to assess how the organization could have benefitted had they adopted ethical reasoning to their privacy practices.

Ethical actions derived from conservative deontological theory

The conservative deontological theory explains that objective moral rules exist, which must be followed. The theory does not allow for its adherents to violate the set of rules that govern a particular context and, as such, does not allow for exceptional situations. Specifically, according to the conservative deontological theory, a set of rules should be as comprehensive as possible, and as such exhaust as many possibilities that it can so that its adherents could achieve the best moral outcome in any given situation. Also, the voluntariness of adhering to the rules and procedures defined under a conservative deontological approach is essentially non-existent, i.e., it is obligatory to follow the rules. The ethical actions of *comprehensive* rules and procedures that are less *voluntary* to follow are derived from the conservative deontological theory.

Pre-data breach actions. Despite FCRA requirements, ChoicePoint sold consumer reports for impermissible purposes, while failing to verify the identity of their subscribers. Also, they violated section 5 of the FTC act through deception by "misrepresenting their security procedures in consumer publications" (Culnan & Williams, 2009, p. 680). Before the breach, the company should have employed the GAPP and ISO 17799 for structuring their security and privacy policies. The GAPP consists of 10 sections which are considered comprehensive of FIPs (Culnan & Williams, 2009). Similarly, the ISO 17799 standard is comprehensive in providing information security management recommendations. By explicitly defining that the company and its employees need to adhere to security and privacy policies developed based on GAPP and ISO 17799, ChoicePoint would have achieved a set of comprehensive guidelines that were obligatory to follow, ensuring that individuals' PII were protected. The existence of a privacy policy based on GAPP would have required ChoicePoint to notify individuals about the collection and use of their PII, as well as for what purposes it was being sold to third-party organizations. Furthermore, individuals would have

had control over their PII through the principles of choice and consent. Essentially, this would have prevented ChoicePoint from violating the FCRA and section 5 of the FTC Act.

Post-data breach actions. After the data breach, ChoicePoint strengthened their privacy and security practices by adopting GAPP and ISO 17799 in creating their privacy and security policy, respectively, as well as created their own standard in customer credentialing. Therefore, ChoicePoint achieved an adequate level of comprehensiveness with regards to how they handled PII. Furthermore, ChoicePoint accounted for exceptional situations, such as the criteria under which full data would need to be provided to subscribers instead of truncated data. Similarly, the adoption of multiple activity monitoring systems accounts for the numerous ways activities could be considered abnormal and, as such, subject to review. Their implementation of the social engineering training program for call center employees, and accounting for permanent and temporary employees, as well as independent contractors, added to their list of exhausting possibilities and limiting exceptional situations.

ChoicePoint adopted an obligatory (non-voluntary) stance toward the rules they created for their subscribers, pertaining to their security and privacy practices. ChoicePoint essentially rejected companies whose identities could not be verified, while terminating or suspending the accounts of subscribers who did not adhere to their standards of security and privacy. Employees also had to undergo obligatory annual assessments of both the security and privacy programs. Finally, compliance of policies and procedures was assessed based on the duties of key employees such as the CCCPO. Essentially, the actions ChoicePoint took after the data breach represents a conservative deontological approach of obligatory adherence to the comprehensive rules of the organization. Similarly, some of the practices they adopted post-incident were due to mandates established by the FTC to enforce better protection of individuals' PII.

Ethical actions derived from the liberal-intuitive theory

The liberal-intuitive theory, in contrast to the conservative deontological theory, indicates that if an action has not been made forbidden, then it is allowed. Essentially, the theory recognizes that exceptional situations exist but does not account for how these situations should be addressed (Siponen & Iivari, 2006). Based on this theory, adherents are obligated to follow the rules, similar to the conservative deontological approach, but they are free to act however they wish in a situation that is not included in the rules. However, the liberal-intuitive theory assumes that individuals would make autonomous decisions; therefore, policies within an organization should only include necessary rules. As such, the ethical actions derived from the liberal-intuitive theory are the existence of only *necessary rules and procedures* that are less *voluntary* to follow.

Pre-data breach actions. It can be observed that this approach has failed with regards to privacy practices in the case of ChoicePoint. Before the data breach, ChoicePoint did not adhere to security practices that they claimed to have. Also, they violated U.S. laws including FCRA and section 5 of the FTC Act. In essence, ChoicePoint did not adhere to the obligation of following rules and guidelines. Additionally, the cause of ChoicePoint's data breach was based on subscribers' fraudulent identities. While no set of rules or industry standard existed for consumer credentialing, it would have been ethical for ChoicePoint to adopt some approach. Moreover, the manner in which ChoicePoint collected data on individuals was usually without direct contact, and selling data profiles for impermissible purposes reflected bad ethics on the company's part (Culnan & Williams, 2009). It was due to the California Security Breach Notification law that ChoicePoint was obligated to notify individuals that their PII was compromised. Essentially, providing the company with freedom and a bare minimum of necessary rules, while assuming they would make autonomous decisions to protect consumers' PII, had proven to be ineffective, as essentially the company's actions were not ethical.

Post-data breach actions. Evidence of the ChoicePoint's post-incident actions indicates that the company was more secure and protected consumers' PII when a set of rules was put in place. Additionally, ChoicePoint went beyond obligations and acted ethically, post-incident. ChoicePoint

created policies for privacy and security based on GAPP and ISO 17799 standard, respectively, which were comprehensive in the steps the company should take to protect their data. However, they implemented their own standard for consumer credentialing, which is one instance that reflected the company's autonomous decision-making. Further instances of ethical behavior include the company's decision to truncate the PII of individuals they collected data upon. Among other ethical actions which went beyond necessary measures were their training guidelines for employees and individual contractors, training against social engineering attacks for call center employees, and the numerous encryption and activity monitoring security approaches they took to secure their data. Furthermore, instead of using a checklist for credentialing, ChoicePoint had a separate checklist for site visits and required that their subscribers adhered to privacy and security practices that the company approved off. This led to many small businesses suffering as ChoicePoint rejected them due to verification issues; however, it led to better protection of individuals' PII. Essentially, before the data breach, a liberal-intuitive approach to privacy practices seems ineffective. However, post-incident, ChoicePoint's practices went beyond bare minimums in protecting PII. While they did create a number of policies and procedures for their employees to follow, depicting a conservative deontological approach of the intrinsic business processes, overall the company regulated themselves ethically going over laws and standards. Therefore, the data lends support that a liberal-intuitive approach of ethical actions consisting of only necessary but obligatory rules could help inform organizations of good privacy practices. Yet, this approach is less effective and risky as opposed to directly enforcing regulations on an organization.

Ethical actions derived on virtue design theory

Adherence to the virtue design theoretical approach would require individuals to perform supererogatory ethical actions (i.e., voluntary or nonobligatory), to achieve success in an exceptional situation (Siponen & Iivari, 2006). These supererogatory ethical actions should be based on internal virtuous characteristics developed by the individuals. However, should the individuals refuse to perform these supererogatory actions, they are not guilty of wrongdoing (Siponen & Iivari, 2006). The virtue design theory therefore elicits the ethical actions of *voluntariness* and *virtuousness*.

Pre-data breach actions. ChoicePoint did not display virtuousness in the privacy and security actions before the data breach. ChoicePoint violated state regulations and failed to verify the credentials of their subscribers, which was the major cause of data breach. At the time, there were no standards present for customer credentialing. However, had ChoicePoint acted virtuously, they would have been able to prevent the data breach. Furthermore, virtuousness would have been displayed had they created privacy and security policies based on GAPP and ISO 17799, respectively, which would have been a step toward preventing the data breach. While not mandatory, ChoicePoint could have truncated the PII of individuals they collected, which would have prevented identity theft.

Post-data breach actions. It was not until after the data breach that ChoicePoint decided to enact practices that were considered virtuous. For instance, ChoicePoint was not required to use a separate site checklist for customer credentialing; however, they did in response to the offenders using commercial mail drops to fraudulently gain access to individuals' PII. Employees security and privacy training were rigorous with regards to the frequency and pass rate. Virtuousness was observed in ChoicePoint's audits of their subscribers, data management techniques, multiple encryption procedures, and activity monitoring systems, as well as the truncation of individuals' PII except in specific circumstances. While the truncation of individuals' PII was not a requirement, it highlights virtuousness since, at the time, ChoicePoint competitors did not do it (Litan, 2006). Moreover, the restructuring of organizational governance in hiring a Chief Credentialing Privacy Officer, as well as tasking each functional business area with security responsibilities, indicated virtuousness as the company was not required to do this under any U.S. law or standard but did for the betterment of individuals' personal privacy.

Ethical discretionary actions derived on prima-facie, utilitarian, and universalizability theory

The prima-facie theory, utilitarian theory, and universalizability theory all indicate that in the presence of obligatory rules and procedures, individuals should enact discretionary actions for exceptional situations. Essentially, all three theories argue that rules are obligatory and should be as comprehensive as possible, which is similar to the conservative deontological approach. However, unlike the conservative deontological approach, actions beyond the rules and procedures are not forbidden, so long as certain criteria are met. This also differentiates from a liberal-intuitive perspective since the prima-facie, utilitarian, and universalizability theories explain how exceptional situations should be addressed. All three theories consist of ethical actions of *comprehensive* rules and procedures that are less *voluntary* to follow. These ethical actions of comprehensiveness and less voluntariness were discussed above with regards to the conservative deontological theory. However, despite how comprehensive a set of rules may seem, every parameter cannot be fully explored. Furthermore, complications may arise in trying to implement all the comprehensive rules and procedures and therefore lead to bad practices (Siponen & Iivari, 2006). For this reason, discretionary approaches are advised (Siponen & Iivari, 2006).

Prima-facie theory posits that the expected benefits of doing an action that is not legislated by the rules to which the adherents of the theory are bounded by can only be carried out if it exceeds the expected benefits of not performing the action (and subsequently abiding by the rules) (Siponen & Iivari, 2006). Therefore, the ethical actions that organizations should adhere to ensure good privacy practices are obligatory comprehensive rules and guidelines that could only be breached in situations where the *expected net benefits* of violating the rules and procedures exceed the expected net benefits of following the rules and procedures. A prima-facie duty is different from an actual duty in that it consists of subverting actual duty in lieu of an action that would achieve better results. An example of prima-facie duty would be the truncation of PII with regards to the ChoicePoint's data breach. Had the company truncated the sensitive PII of consumers before they sold it to the fraudulent subscribers, there would be no compromise of the consumers' PII nor identity theft which subsequently followed. Also, truncating sensitive data would have prevented situations such as fraudulent accounts even if there were limited or no customer credentialing practices. Furthermore, ChoicePoint would have not been guilty of unfair practices stated in section 5 of the FTC act.

It was only after the data breach that ChoicePoint opted to implement this action of exceeding the expected benefits of bare minimum security and privacy requirements. While the FTC required ChoicePoint to perform audits of their customers after the data breach, ChoicePoint went beyond obligations such as making random audits on a daily basis, ensuring their customers had the permission to request consumer data profiles, while resellers and third-parties had abided to proper privacy and security practices approved by ChoicePoint. In essence, a prima-facie approach instigates moving beyond obligations due to moral responsibility. Therefore, while ChoicePoint was in violation of specific national regulations, they did not particularly need to implement all of the rules and procedures for better privacy and security that they did after the privacy breach. Yet, by employing the privacy and security practices in response to the data breach, they proved that they accepted the expected benefits of going beyond obligations.

Utilitarian theory describes the maximization of utility which is felicity, the presence of pleasure, and the absence of pain (Siponen & Iivari, 2006). Therefore, apart from comprehensive, obligatory rules and guidelines for specific situations, the utilitarian theory consists of the ethical action of *happiness*. Within the case of ChoicePoint, the company should have sought happiness for themselves, the consumers whose PII they collected, and their subscribers. ChoicePoint generally failed to achieve happiness for themselves due to their relaxed privacy and security practices, and their lack of customer credentialing. Essentially, the decision caused the company over $30 million in costs, affected 165,000 individuals, and led to them exiting business areas due to stringent customer credentialing that came from the fallout of the data breach. Before the data breach, ChoicePoint

could have developed customer credentialing procedures, as well as truncate sensitive data, in which case all entities related to the case would have achieved happiness. While ChoicePoint and other businesses essentially suffered from the decisions made in response to the data breach, and further protecting future sensitive PII, some of ChoicePoint's decisions essentially adhered to considering the happiness of the company, individuals, and future subscribers. For instance, fraudulent activity could be detected via the multiple activity monitoring systems, and truncated sensitive information could prevent further identity theft.

Universalizability theory posits that "an acceptable action should be one that the person would accept if he were on the receiving end of the action" (Siponen & Iivari, 2006, p. 452). Apart from a comprehensive set of obligatory rules, adherents to this normative approach should perform actions in exceptional situations if the action is allowable for anyone else in a similar situation, or a person in the position of power allows an action by anyone else they consider to be trustworthy (Siponen & Iivari, 2006). As such, *universalizability* is the third ethical action, alongside comprehensiveness and less voluntariness. From the perspective of universalizability, there were a number of procedures ChoicePoint should have implemented, even if regulations did not dictate them. For instance, ChoicePoint should have regularly audited their subscribers, as well as allow the consumers whom they collected data on, retain some level of control over their PII (such as opting out of having their PII collected).

Amongst the actions that ChoicePoint took after the data breach which applies to universalizability was the involvement of the entire company in the privacy and security practices (i.e., not limiting privacy and security to only specific divisions), stringent training programs and assessments for security and privacy, and truncated sensitive PII. Essentially, other ChoicePoint competitors did not employ all of the privacy and security practices that ChoicePoint did after the data breach, nor were they required by federal law to do so. Even the complete 10 principles of GAPP were not mandatory for organizations to follow, yet ChoicePoint adopted these in entirety. The refusal of subscribers that was not properly verified was also a principle which showcased a level of moral judgment which any other organization in ChoicePoint's situation could adopt to better protect themselves and clients by protecting individual PII.

In this section, we analyzed pre-data breach actions and post-incident actions of ChoicePoint with respect to ethical actions derived from underlying normative theories. The next section presents similar analysis of Equifax and SCDOR data breaches.

Data analysis – SCDOR and Equifax data breaches

This section presents our analysis of Equifax and SCDOR data breaches with respect to application of ethical actions to enhance privacy practices.

Ethical actions applied to SCDOR

While data breaches and external threats (intended malicious external cyber-attacks) are impossible to stop, the case indicates that SCDOR should have done more to better protect their citizens' PII. Specifically, developing adequate controls could have prevented the attack from occurring. While the cause of the data breach originated from the Director falling prey to a spear phishing attack, it is also possible that any other employee could have fallen into the same trap. Therefore, it is incumbent upon government agencies to develop privacy practices that are *comprehensive* in nature. Specifically, information security policies and privacy policies to which the agency actually adheres to are necessary. A *comprehensive privacy policy* should include all dimensions of the FIPs (Liu & Arnett, 2002; Schwaig et al., 2006). Moreover, the agency should follow the privacy policy and not only use it as a means of building trust with citizens. An extensive implementation of FIPs is the GAPP developed by the AICPA and the Canadian Institute of Chartered Accountants that consists of 10 principles an organization should enact when handling PII (Culnan & Williams, 2009). The GAPP could have been used as a framework for developing adequate privacy policies

in the SCDOR. Additionally, these security and privacy policies, alongside training and/or awareness programs, could be used to control employee behavior, while guiding and educating top management of the actions they could engage in that might endanger the agency. This way, threats to PII and employee behavior with regards to PII would be handled meticulously.

Siponen and Iivari (2006) explained that having comprehensive policies may not always result in the best outcome as it may become too much of a cognitive load for employees. Thus, a liberal-intuitive approach can be taken, whereby only *necessary rules* and practices are mandated, while employees act autonomously. While each employee has specific roles and responsibilities within a government agency, it is upon every employee to recognize that he/she has not an absolute authority over every issue. Specifically, the reason for roles such as CISOs is to guide and cultivate proper security (and possibly privacy) strategies within the organization (Brotby, 2009). In the case of SCDOR's data breach, the Director should have heeded the advice of the CISO in increasing security protocols. The government agency should regularly appraise how PII is handled among the different departments and employees. However, if the agency's culture emphasizes information privacy, then all employees, irrespective of hierarchy, would be more likely to act ethically to ensure PII is protected, and information systems are not abused.

Despite the state budget being restrained due to economic difficulties, which was the probable cause for SCDOR's relaxed security and privacy strategies (Loy et al., 2014), the agency should have engaged on assessment of costs and benefits from the possibility of attacks and evaluated alongside other business objectives. While it is unproductive to invest heavily and irresponsibly in strong security and privacy strategies, it is necessary for a government agency to recognize their duty toward their citizens and adequately protect PII from possible harm.

SCDOR should have also engaged in *virtuous* behavior. This pertains to top management as well as all employees. The Director of SCDOR ignored the advice of CISO and refused to implement technical controls that could have added a layer of security which could have inhibited the attack. Furthermore, the Director should have recognized the sensitive nature of the PII the agency collected. Essentially, a government agency responsible for handling taxes should advocate information privacy and security as a prioritized objective. Culnan and Williams (2009) indicated that ethics is good business, since an organization should try to retain clients for continued business transactions, which is best achieved by acting ethically toward that client (Caudill & Murphy, 2000). This is especially the case with government agencies, as citizens should perceive a sense of safety from their government. It is, therefore, more incumbent upon government agencies to enhance an ethical position through virtuous character. A virtuous employee would make assessments based on skills, knowledge, experience, common sense, and insight, while controlling his/her personal desires when handling PII and using information systems (Gray & Tejay, 2014). SCDOR and other government agencies should seek to employ virtuous individuals while implementing strategies to increase group dynamic focusing on virtuous behavior related to privacy practices.

SCDOR could have evaluated the activities that would ensure everyone connected to the collected PII were happy and content with the security and privacy practices. CISO had proposed a relatively cheap solution for a government agency to add an extra layer of security through dual authentication, which was utilized by other state government agencies. However, the Director ignored this suggestion which resulted in the frustration of employees, taxpayers, and businesses. Had the director acted upon CISO's advice, even at a small cost to the budget, the damages could have been minimized. Essentially, had the estimated *net benefits* of investing in better security as opposed to the benefits of not doing so, it would have led to a better outcome of protecting against this data breach.

Protecting taxpayers' PII should be a top priority for a government agency, just as the IRS claimed during the SCDOR data breach (Loy et al., 2014). This is because government agencies are established to provide services to citizens. It is upon the agency to ensure that the trust citizens endow upon them is reciprocated. Furthermore, privacy and security at government agencies should

not be seen as an expense, but rather a cost of doing business and an investment, the interim director of SCDOR, Bill Blume (Shain, 2013). Based on both the ethical actions of *happiness* and *universalizability*, SCDOR should have acted upon emphasizing protection of PII by considering how they would feel if it was their personal information that was disclosed to another entity, and how they would like that entity to handle their personal information. The outcome would have resulted in both their own benefit, and the benefit of those that were affected. This is similar to the principle suggested by Culnan and Williams (2009) in avoiding decoupling, whereby privacy is connected personally to an organization's business goals, as well as considered an asset to the organization and not just a tool.

Ethical actions applied to Equifax

Equifax should implement ethical actions in bettering their security and privacy practices moving forward after the breach. Strong security and privacy policies should be implemented that are *comprehensive* and mandatory (*less voluntary*) to follow. Had these policies been developed and adhered to before the breaches, they would have addressed the vulnerability and not been susceptible to the attack. Alternatively, Equifax could have acted beyond the bare minimums of *necessary rules* and acted *virtuously* by conducting vulnerability assessments and penetration tests to ensure their systems were secure. Even without regulations or policies specifying when and how these tests should be conducted, Equifax should have acted autonomously with a dedicated security team to assess their security and privacy posture.

As Equifax deals with sensitive consumer information such as social security numbers and credit card information, it was necessary for them to keep these information as protected as possible. By investing in better security and privacy, the *expected net benefits* of avoiding this breach, possible charges by the FTC, and the public backlash outweighed the benefits they gained from ignoring the problem. Equifax's practices before the breach reflected an approach of moral turpitude, whereby they only considered their own benefits, or *happiness*. As an organization that handles such sensitive PII, they should have considered the impact to themselves, as well as the individuals whose PII they collected, which would have motivated them to invest in better security and privacy practices. Under the ethical action of *universalizability*, as handlers of sensitive information, Equifax should have considered what they would do if the information they collected were their own. In such a case, they would have enacted stronger privacy and security practices as they would feel a level of ownership for the PII that would incite the need to protect it from data breaches.

Discussion

We used six normative theories to develop a set of ethical actions for better privacy practices. However, not all of the ethical actions are synthetic and may force organizations to adopt only some of them. The conservative deontological theory proposes two ethical actions of voluntariness and comprehensiveness. Under this approach, organizations should seek to eliminate exceptional situations by implementing comprehensive rules and procedures that are obligatory to follow. On the contrary, the liberal-intuitive theory indicates that organizations are only obliged to follow a limited set of necessary rules and use moral judgment to address exceptional situations. The theories of virtue design, prima-facie, utilitarian, and universalizability compliment both the limitations of the conservative deontological and liberal-intuitive theories (Siponen & Iivari, 2006). Essentially, virtue design encourages organizations to act virtuously, but they are not blameworthy if they do not do so in exceptional situations. Prima-facie expresses the need to go beyond obligations to prevent exceptional situations, while utilitarian theory considers the happiness of all entities given a situation. Universalizability encourages decision-making that could be applied universally because it is ethically right, to situations not covered in a set of rules.

The analysis of ChoicePoint, SCDOR, and Equifax cases has shown that a conservative deontological approach of comprehensive and obligatory rules and procedures often leads to best practices. The all-inclusive nature of this theoretical approach is limited in scope as every parameter may not always be practical and might be complicated to fully follow for organizations and their employees (Siponen & Iivari, 2006). Yet, having only a set of necessary guidelines assumes that organizations would act autonomously. As can be seen from the cases, this assumption is risky. Essentially, while ChoicePoint did go beyond obligations after the data breach, which suggests autonomous (ethical) behavior, it was too late. Similarly, despite regulations and standards for security and privacy, neither SCDOR nor Equifax act autonomously. An organization should seek to implement good privacy practices before data breaches occur. As such, it is less effective to implement liberal-intuitive ethical actions as opposed to comprehensive obligatory rules and procedures. At the same time, it is risky to assume that organizations would operate virtuously if there are no comprehensive rules or procedures. However, provided that comprehensive rules and procedures, such as government regulations, do exist, which are sometimes mandatory for organizations and their employees to follow, situations that are exceptions could be managed by virtuousness, expected net benefits of ethical actions, happiness, and/or universalizability.

Culnan and Williams (2009) explained that organizational activities require some level of ethical principles to continue their existence. We have emphasized how organizations could follow certain ethical actions to achieve some level of morality. The effectiveness of such ethical actions was examined through three data breach cases. In doing so, our study corroborated the argument of Culnan and Williams (2009) by providing further support from three data breach cases. Specifically, we extended the study of Culnan and Williams (2009) through application of the framework developed by Siponen and Iivari (2006) based on normative ethical theories. Culnan and Williams (2009) stated that a culture of privacy should be developed within organizations but needed to be developed from the top of organizations. Similarly, organizational governance processes could be used to ensure that their privacy practices comply with regulations (Culnan & Williams, 2009). As seen from the actions ChoicePoint took after the data breach, policies and organizational governance were restructured to better protect consumers' PII. The ethical actions derived from normative theories have been proven in our study as a means of establishing organizational governance processes, as well as creating a privacy culture. Culnan and Williams (2009) suggested that organizations should avoid decoupling with respect to privacy issues. Essentially, organizations should treat their clients' PII as if it was personally theirs and implement practices to safeguard it as they would safeguard their own (Culnan & Williams, 2009). Ethical actions could achieve coupling of privacy with business functions particularly through the universalization perspective.

The analysis of the three cases emphasized certain privacy principles that organizations should adhere to (see Table 2). First, organizations can follow a *contextually based approach* for developing comprehensive privacy policy and practices. Events in relation to privacy practices would entail the inner context (internal structural, cultural, and political environment) and outer context (external social, economic, and political environment) of an organization (Tejay, 2008). Such a consideration to context will in turn increase the comprehensiveness of organizational privacy practices.

Second, organizations can also develop *dyadic trust* among functional and hierarchical members in the organization. Trust in the workplace is found to be associated with enhanced job performance, job satisfaction, and organizational citizenship behavior (Colquitt, Scott, & LePine, 2007). This would help in developing strong privacy culture and control how PII is handled internally. Essentially, this helps an organization to act autonomously in the case of limited rules, and virtuously to address how PII is handled.

Organizations could also choose to employ individuals who are considered virtuous. Gray and Tejay (2014) posited four dimensions of a virtuous character, which consist of astuteness, conviction, rectitude, and self-discipline. If an employee displays these characteristics, it is probable he/she may engage in ethical behavior with regards to PII and carefully follow the rules, regulations, and culture of the workplace. Alternatively, based on the prima-facie theory, organizations would have various

Table 2. Information privacy principles based on ethical actions.

Ethical actions	Information privacy principles
Comprehensiveness	Develop contextually based privacy approach
Necessary rules	Develop dyadic trust
Virtuousness	Enhance ethical disposition through virtuous character
Net benefits	Balance privacy objectives and obligations
Happiness	Emphasize privacy-related societal responsibility
Universalizability	

duties to different stakeholders. These duties (and subsequent roles of stakeholders) should be prioritized, whereby the duty with the most net benefit is handled with urgency (Siponen & Iivari, 2006). Organizations should therefore review their priorities and balance privacy objectives and obligations.

Finally, organizations should emphasize *societal responsibility*. An organization's societal responsibility refers to the actions they engage in that appear to increase some social benefit beyond an organization's interests or legal obligations (McWilliams & Siegal, 2001). Essentially, an organization should engage in privacy practices that provide benefits not only to themselves but also to their clients and society as well.

Managerial implications

Based on the findings of our study, there are several managerial implications which organizations should follow. Organizations need to recognize the necessity of implementing good privacy practices. While regulations are meant to enforce organizations toward protecting individuals' PII, it is not enough (DeGeorge, 2006). Rather than waiting for incidents to occur and then invest in better security and privacy practices, organizations should implement strategies beforehand that will overcome security and privacy breaches. Organizations should go beyond regulations and employ technical and managerial solutions to properly protect individuals' PII. While encryption techniques and activity monitoring systems are crucial, organizations should implement comprehensive privacy and security policies that exhaust as much situations as possible. Doing so would minimize the occurrence of exceptional situations, which pose a threat to individuals' PII. Furthermore, organizations' privacy training programs should be conducted in a systematic manner so as to enhance importance of privacy practices among employees. Finally, organizations should truncate critical PII in every situation where it is not necessary for the full information to be revealed. Specifically, whether selling individuals' PII to other organizations, or in the case of employees accessing an individual's PII, data could be truncated if the full data are not required. This could avoid incidents such as data breaches, unethical behavior, and insider threats to individuals' PII.

Conclusion

Our study investigated the privacy practices that organizations should use to better protect their clients' PII. We developed set of ethical actions based on normative theories to explain how organizations could use some level of moral reasoning to achieve privacy. Our study contributed theoretically by establishing that ethics within an organization could strengthen their privacy practices. Our work essentially extended the study by Culnan and Williams (2009) and was developed based on the study by Siponen and Iivari (2006). As such, we explained how ethics could be implemented in organizations' privacy practices. Furthermore, with the majority of privacy research involved at the individual level, our study focused at the organizational level.

There were limitations within our study which future research should address. First, our data were collected from secondary sources. The findings might be richer with analysis based on primary data collected from another case organization. This would have provided us with better insights

regarding effective privacy practices. Second, due to the differences in the normative theories, cases could have been developed based on each theory and the ethical actions associated with it. This would have directly shown the effectiveness of any one normative theoretical approach over the others. While our study developed a set of ethical actions based on only six normative theories, there may be other theories that could have contributed to the development of additional ethical actions. Future studies could use cross-case comparisons for evaluating, as well as, to observe whether other theories could be used to extend or strengthen proposed set of ethical actions and privacy principles.

Notes on contributors

Zareef A. Mohammed, Ph.D., is a lecturer at the State University of New York (SUNY) at Plattsburgh, in the Management, Information Systems and Analytics department of the School of Business and Economics. Zareef received his Ph.D. in Information Systems from Nova Southeastern University. He also received his M.S. in Information Technology with a specialization in Information Security Management from Nova Southeastern University. Zareef's research interests include information privacy, information security, neuroscience in information systems (NeuroIS), ethics, and data analytics. He has previously published in *Computers & Security* and has had papers presented at *Americas Conference on Information Systems* and *International Federation for Information Processing Dewald Roode Workshop on Information Security*.

Gurvirender P. Tejay, Ph.D., is a Gary Goldbloom Endowed Distinguished Chair in Cyber Security Management at St. Thomas University, Florida. His research interests include information security, privacy and technological change. Gurvirender received Ph.D. from Virginia Commonwealth University. He also holds M.S. in Computer Science from the University of Chicago, and M.A. in Economics from the University of Wisconsin – Milwaukee. He has served as *co-editor* for Special Issue on Cybercrime, for Computers & Security journal. Gurvirender also served as *co-chair* for Emergent Research Forum for Americas Conference on Information Systems 2015.

Joseph Squillace is a doctoral candidate of Information Systems in the College of Engineering and Computing at Nova Southeastern University. He also earned his M.S. in Computer Information Systems, with a concentration in Information Security from Nova Southern University. His areas of research interest include information privacy, ethics, information security, health-care security, defense department information systems, integration of Information security and information technology (IT) in disaster preparedness and recovery, and economics of information security and privacy breaches.

References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM Electronic Commerce Conference*, 21–29.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *3* (1), 26–33.

Alderman, E., & Kennedy, C. (1997). *The right to privacy*. New York, NY: Vintage Books.

Altman, I. (1975). *The environment and social behavior: Privacy personal space, territory, and crowding*. Monterey, CA: Brooks/Cole Publishing.

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, *22*(3), 469–490.

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, *33*(2), 339–370.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled for online personalization. *MIS Quarterly*, *30*(1), 13–28.

Baker, W. H., Hylender, C. D., & Valentine, J. A. (2008). 2008 data breach investigations report. *Retrieved from http://verizonbusiness.com/resources/security/databreachreport.pdf; accessed* June *30, 2008*.

Bansal, G., Zahedi, F. M., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, *49*, 138–150.

Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017–1041.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems*, *11*, 245–270.

Brotby, K. (2009). *Information security governance a development and implementation approach*. Hoboken, New Jersey: John Wiley & Sons Inc.

Brown, R. (2012). *Hacking of tax records puts states on guard*. Available at: <http://www.governing.com/news/state/Hacking-of-South-Carolinaa-Tax-Records-Has-Put-States-on-Guard.html> [Accessed 20 October 2015].

Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing*, *19*(1), 7–19.

Cohn, M. (2012). *S.C. Governor urges encryption of taxpayer information after data breach*. Available at: <http://www.accountingtoday.com/news/SC-Governor-Urges-Encryption-Taxpayer-Information-Data-Breach-64758-1.html> [Accessed 20 October 2015].

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytical test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology*, *92*, 909–929.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the ChoicePoint and TJX data breaches. *MIS Quarterly*, *33*(4), 673–687.

DeGeorge, R. T. (2006). *The ethics of information technology and business*. Oxford, UK: Blackwell Publishing Ltd.

Dinev, T., Bellotto, M.,Hart, P.,Russo, V.,Serra, I., &Colautti, C. (2006). Privacy calculus model in ecommerce – a study of Italy and the United States. *European Journal of Information Systems*, *15*, 389–402.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80.

Dugan, K. (2017). *Equifax CEO: Execs failed to act on Homeland Security warning*. Available at: <https://nypost.com/2017/10/02/equifax-ceo-execs-failed-to-act-on-homeland-security-warning/> [Accessed 1 December 2017].

Federal Trade Commission. (2006). ChoicePoint settles data security breach charges; to pay $10 million in civil penalties, $5 million for consumer redress. *Retrieved from https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million*.

Gray, J. M., & Tejay, G. (2014). Development of virtue ethics based security constructs for information systems trusted workers. In: *Proceedings of the 9th International Conference on Cyber Warfare and Security (ICCWS-2014)*, West Lafayette, IN, USA.

Greenaway, K. E., & Chan, Y. E. (2005). Theoretical explanations of firms' information privacy behaviors. *Journal of the Association for Information Systems*, *(6)*(6), 171–198.

Hsu, C. W. (2006). Privacy concerns, privacy practices and web site categories. *Online Information Review*, *30*(5), 569–585.

Johnson, C. (2017). *Equifax data breach: Credit agency loses $7.2 million contract with IRS*. Available at http://clark.com/personal-finance-credit/equifax-data-breach-credit-agency-loses-7-2-million-contract-with-irs/> [Accessed on 1 December 2017].

Korsgaard, C. (1985). Kant's formula of universal law. *Pacific Philosophical Quarterly*, *66*, 24–47.

Largen, S. 2012. *S.C. Department of Revenue didn't use state cyber security system*. Available at: <http://postandcourier.com/apps/pbcs.dll/article?AID=/20121102/PC16/121109832/1165/sc-department-of-revenue-didn-t-use-state-cyber-security-system&template=printart> [Accessed 20 October 2015].

Litan, A. (2006). Case study: ChoicePoint *incident leads to improved security, others must follow*. Stamford, CT: Gartner Research.Retrieved from *https://www.gartner.com/doc/496516/case-study-choicepoint-incident-leads*.

Liu, C., & Arnett, K. P. (2002). Raising a red flag on global WWW privacy policies. *The Journal of Computer Information Systems*, *43*(1), 117–127.

Loy, S. L., Brown, S., & Tabibzadeh, K. (2014). South Carolina Department of Revenue: Mother of government dysfunction. *Journal of the International Academy for Case Studies*, *20*(1), 83–93.

Madden, M., Fox, S., Smith, A., & Vitak, J. (2007). *Digital footprints:Online identity management and search in the age of transparency*. PEW research center. Retrieved from http://www.pewinternet.org/files/old-media/Files/Reports/2007/PIP_Digital_Footprints.pdf.pdf

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355.

Mandiant 2012. *South Carolina department of revenue public incident response report*. Available at: http://governor.sc.gov/Documents/MANDIANT%20Public%20IR%20Report%20-%20Department%20of%20Revenue%20-%2011%2020%202012.pdf [Accessed 20 October 2015].

Mason, R. O. (1986). Four ethical issues in the information age. *MIS Quarterly*, *10*, 5–12.

McWilliams, A., & Siegal, D. (2001). Corporate social responsibility: A theory of firm perspective. *The Academy of Management Review*, *26*(1), 117–127.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly*, *31*(1), 105–136.

Peslak, A. R. (2006). Internet privacy policies of the largest international companies. *Journal of Electronic Commerce in Organizations*, *4*(3), 46–62.
Privacy Rights Clearinghouse (2017). *Chronology of data breaches*. Available at: https://www.privacyrights.org/data-breach/new?title=&page=2 [Accessed 1 December 2017].
Ragan, S. (2017). *Equifax says website vulnerability exposed 143 million US consumers*. Available at: https://www.csoonline.com/article/3223229/security/equifax-says-website-vulnerability-exposed-143-million-us-consumers.html [Accessed 1 December 2017].
Rose, E. A. (2006). An examination of the concern for information privacy in the New Zealand regulatory context. *Information & Management*, *43*(3), 322–335.
Schwaig, K. S., Kane, G. C., & Storey, V. C. (2006). Compliance to the fair information practices: How are the fortune 500 handling online privacy disclosures? *Information & Management*, *43*, 805–820.
Scipiono, J. (2017). *Equifax hack: A timeline of events*. Available at: < http://www.foxbusiness.com/features/2017/09/14/equifax-hack-timeline-events.html> [Accessed 1 December 2017].
Shain, A. (2013). *Acting head: Computer security 'non-negotiable' at hacked agency*. Available at: http://www.thestate.com/2013/01/23/2601585/acting-head-security-non-negotiable.html#.URah9aVX0rU [Accessed 20 October 2015].
Siponen, M., & Iivari, J. (2006). Six design theories for IS security policies and guidelines. *Journal of the Association for Information Systems*, *7*(7), 445–472.
Smith, H. J. (1993). Privacy policies and practices: Inside the organizational maze. *Communications of the ACM*, *36* (12), 105–122.
Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35* (4), 989–1015.
Solove, D. J. (2006). A taxonomy of privacy. *University of Pennyslvania Law Review*, *15*(3), 477–564.
Solove, D. J. (2007). 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review*, *44*, 745–772.
South Carolina Department of Revenue 2015. *History*. Available at: https://dor.sc.gov/about/history [Accessed 20 October 2015].
Tejay, G. P. (2008). *Shaping strategic information systems security initiatives in organizations*. Ph.D. *Virginia Commonwealth University*.
Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, *7*(6), 415–444.
Warren, S. D., & Brandeis, D. L. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.
Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Atheneum Publishers.
Xu, H., Teo, H. H., Tan, B. C. Y., & Agarwal, R. (2010). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems*, *26*(3), 135–173.