Cloud computing data breaches: A review of U.S. regulation and data breach notification literature

David Kolevski
School of Computing and Information Technology
University of Wollongong
Wollongong, Australia
dk616@uowmail.edu.au

Katina Michael
School for the Future of Innovation in Society
Arizona State University
Tempe, Arizona
katina.michael@asu.edu

Roba Abbas
School of Business
University of Wollongong
Wollongong, Australia
roba@uow.edu.au

Mark Freeman
School of Computing and Information Technology
University of Wollongong
Wollongong, Australia
mfreeman@uow.edu.au

2021 IEEE International Symposium on Technology and Society (ISTAS) | 978-1-6654-3580-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISTAS52410.2021.9629173

***Abstract*— Cloud computing services have enjoyed explosive growth over the last decade. Users are typically businesses and government agencies who are able to scale their storage and processing requirements, and choose from pre-defined services (e.g. specific software-as-a-service applications). But with this outsourcing has also come the potential for data breaches targeted at the end-user, typically consumers (e.g. who purchase goods at an online retail store), and citizens (e.g. who transact information for their social security needs). This paper briefly introduces U.S.-based cloud computing regulation, including the U.S. Health Insurance Portability and Accountability Act (HIPPA), the Gramm Leach Bliley Act (GLBA), and the U.S. Stored Communications Act (SCA). We present how data breach notification (DBN) works in the U.S. by examining three mini-case examples: the 2011 Sony PlayStation Network data breach, the 2015 Anthem Healthcare data breach, and the 2017 Equifax data breach. The findings of the paper show that there is a systemic failure to learn from past data breaches, and that data breaches not only affect business and government clients of cloud computing services but their respective end-user customer base. Finally, the level of sensitivity of data breaches is increasing, from cloud computing hacks on video game platforms, to the targeting of more lucrative network and computer crime abuses aiming at invasive private health and financial data.**

Keywords—cloud computing, data breach, regulation, data breach notification, consumers, sensitive data, health records, financial records, USA, Sony PSN, Anthem Healthcare, Equifax

I. INTRODUCTION

Cloud computing services have seen an exponential growth in adoption far outpacing traditional enterprise networks. From cloud providers, cloud customers, governments to end-users (i.e. everyday consumers), the demand for cloud services is at an all-time high [40]. Governments and businesses are outsourcing critical services and processes to the cloud with the intention of reduced infrastructure and system capital expenditure. However, with the rapid adoption of cloud services and the primary objective of reducing costs, we have seen an increase in data breaches due to hacking with undesirable consequences for the end-user. Sophisticated hackers and cybercriminal groups are targeting cloud services that have weak defenses, such as outdated security architectures, unsuitable employee training programs and inadequate cloud regulation. The aim of this paper is to review regulation and data breach notification (DBN) literature from a United States (U.S.) perspective. Three data breach cases are reviewed over a period of six years to investigate the progress towards improved data breach reporting. The three cases are the Sony PlayStation Network (2011), Anthem Healthcare (2015) and Equifax, Inc. (2017) data breaches. These cases are chronologically presented in this article. While there were sizeable breaches before the Sony PSN breach in 2011, it was the first of its kind by a significant number of compromised user accounts. Data breaches were then tabled as a significant vulnerability to company security profiles. The three selected cases in this study were chosen because of their impact, and the time it took for the data breaches to play out in the courts.

II. CLOUD COMPUTING REGULATION

Studies addressing the environmental implications of cloud computing data breaches generally reflect on issues relating to the applicability of regulation. While numerous studies discuss regulation, they also consider that end-user privacy is encapsulated in the design process. For example, [1] review the regulatory aspect concerning privacy issues in the Internet of Things (IoT). While the authors focus on the IoT landscape, the study's outcome is useful in the cloud domain. The authors conclude that regulation needs to be regularly updated and factor in end-user personally identifiable information (PII) protection. Likewise, in an earlier study by [2], regulatory issues pertaining to the cloud were highlighted as requiring urgent reform. As such, both studies aim to address regulatory issues in emerging technologies, however, they were lacking in evaluating the usefulness of regulatory amendments in data breach events.

Additional studies looking into regulation in the cloud computing have opposing views on the usefulness of regulatory amendments. While the majority of studies highlighted throughout this paper examine the need for a regulatory amendment, some studies identify regulatory reform as a potential drawback. For example, [3] claims that the process of privacy and security requirements must be included in regulatory amendments but that: "the price of privacy [and] security should not be the loss of innovation or inordinate constraints on business". This view is supported by [4] who wrote that imposing regulatory amendments into an ecosystem that has not yet matured can be a challenging task for all stakeholders involved. The idea that an industry

978-1-6654-3580-2/21/$31.00 ©2021 IEEE

in its nascent stage of development can be shackled by too much regulation is well-noted in the literature [42].

An alternative approach to examining regulatory responses to the cloud model is to explore previous studies that aim to serve as guides and future roadmaps. A study conducted by [5], while the cloud model was in its infancy, reviewed important cloud issues such as privacy, security, reliability and policy. The regulatory response is embedded in the overall summary. The authors concluded that past technology developments must be taken into consideration when constructing cloud regulation. Similarly, [6] reviewed Denmark's response to technology advancements and indicated that the Danish Data Protection Agency (DDPA) acted on changes that obstructed digital archives. Where an organization required managed storage services for their data, before even the onset of cloud computing, data protection had already been recognized as essential for keeping personal data private. These articles applied different methodological approaches. [5] reviewed existing works in the cloud model, while [6] applied content analysis to examine regulatory changes. These studies serve as guides to investigate cloud data breaches, from a socio-technical perspective, focusing on the environmental aspect.

III. U.S. Data Privacy Regulations

An important aspect of investigating cloud computing data breaches is to review existing U.S. data privacy regulations. Only when we can review what safeguards are in place today, can we assess what is required, and point to regulatory gaps or loopholes. For example, [7] examine the approach taken by U.S. authorities to address data privacy concerns and note the U.S. "does not have an omnibus information privacy statute". They concluded that instead of such a statute, other legal avenues are taken at state and federal levels, including case law and torts. Similarly, [8] reviews U.S. data protection and examines the 2005 TJX and 2011 Sony PlayStation data breaches. [8] agrees that a lack of a uniform federal regulatory stance needs an alternative approach. As such, the author concludes that "something must be done to motivate companies to pay attention to and implement such standards within their own security plans" [8].

A. U.S. Health Insurance Portability and Accountability Act (HIPPA) and the Gramm Leach Bliley Act (GLBA)

While much can be written on U.S. data privacy regulation in general, several other studies examine issues at state and federal levels. For example, [9] states that the U.S. Federal Trade Commission (FTC) aims to create a perception of data privacy through the absence of federal privacy law to build trust within the U.S. landscape. The author also states that other federal laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPPA) and the Gramm Leach Bliley Act (GLBA) allow for comprehensive health and financial data protection. Similarly, [10] states that in the U.S. there is a collection of state data privacy laws. However, in the absence of federal law, the FTC is assisting U.S. consumers (e.g. end-users) against companies that are failing to protect their data. In addition, [11] states that the patchwork of U.S. state laws causes increased business confusion, especially as a great many businesses sell across state borders. Businesses in their industry segments are promoting specific federal laws such as HIPPA and GLBA to demonstrate compliance with the manner in which they store sensitive personal and health information. Finally, [9-11] note that these federal laws are purposeful for their required industry segments. The three studies conclude that federal universal data privacy regulation is needed to ensure end-users are protected from data breaches.

B. U.S. Stored Communications Act (SCA)

Numerous studies focus on the U.S. Stored Communications Act (SCA) and its intended use for technology-driven applications. The studies have reviewed the SCA to include attributes applicable to technologies in use today. However, they have failed to explore the SCA's intended use on emerging technologies. While the studies show that the SCA is outdated and in urgent need of review, one study conducted by [7] examined that the SCA was initially intended to "expand Fourth Amendment protections in light of emerging computer technologies, like email". It is this level of data protection, in particular for data privacy regulation, that presents concerns in the U.S. context. In a previous study, [12] evaluates the SCA and implies that a robust and deterministic approach to legal infrastructure is outdated even for technologies that are in use today. Unlike [12][13] asserts that the SCA needs alterations, including removing the remote computing services (RCS) and electronic communication services (ECS) and issuing requirements such as warrants and implementing a statutory suppression remedy. While the three studies reviewed the applicability of the SCA with respect to today's technologies, both [12–13] failed to explicitly consider the concept of data privacy regulation in combination with society, technology and environmental needs. As such, [7] concluded that these needs are essential to improve end-users data protection rights.

IV. U.S. Data Breach Notifications

A. Cloud Computing Data Breaches Defined

A cloud computing data breach is defined as a breach that discloses end-user or business data stored on a cloud service [30]. Unauthorized hackers penetrate the defenses of the cloud provider or customer's cloud network and remain undetected. Hackers then retrieve the end-user or business-related data and disclose it for financial gain on the dark web [31]. [32] state that hackers can bypass basic cloud security in many cloud ecosystems. At the same time, the authors note that securing cloud services reduces the likelihood of data breaches, attack vectors through virtualization and data at rest (i.e. unencrypted data). [33] discuss attack vectors such as distributed denial of service (DDOS) attacks, SQL attacks and virtual machine (VM) hacks and the increase of these types of attacks on cloud services. According to [34], hackers target the cloud provider or customers' weakest link to enter the cloud service. For instance, in many situations, employees are targeted through social engineering attacks. Social engineering attacks target employees with end-user facing interfaces (i.e. email messages) and expose them to malicious programming code or embedded malicious attachments. Finally, hackers target both technology vulnerabilities and human weaknesses through exploitation techniques.

With the increased attention on data breaches, whether or not to notify affected individuals (i.e. end-users) is becoming an increasingly charged issue. In this section, past data breach studies are reviewed in the context of their application to cloud computing services. For example, [14] state that the absence of a federal U.S. law has encouraged the companies

affected by a data breach to pass on the costs to consumers (i.e. end-users), insurers and financial institutions. However, the authors do not explicitly mention DBNs; they cover data breaches from a legal perspective. One of their principle outcomes, in terms of environmental implications, is that the U.S. has 50 state laws concerning data breaches and this creates confusion for businesses (i.e. cloud customers and providers) operating nationwide [14].

B. Reporting Data Breach Cases

A study by [15] portrays the usefulness of DBNs. The authors state U.S. institutions need to disclose data breaches to their customers (i.e. end-users) when their personal information is stolen. The main goal of the study was to examine customers' reaction once they became informed about the 2012 South Carolina Department of Revenue data breach through a DBN and news media. The outcomes of the study are influential, indicating "that local media reporting on data breaches does not seem to amplify the effect of a data breach on the breached customers" [15]. An additional outcome of this study indicates that the affected customers opted-in for credit-freezing once they became aware of the data breach. Similarly, [16] state the DBN laws introduce additional avenues for end-user data protection; however, an emphasis that DBN laws are difficult to understand is prevalent. The authors in this instance studied the 2017 Equifax data breach using a case study approach. They used semi-structured interviews with 24 participants and indicated that ID theft is reduced through credit-freezing. However, they presumed that hackers would target individuals that have higher credit ratings. While the two studies present alternative methodologies, the outcomes were similar, in that they both identified that credit freezing could reduce ID theft.

[17] states that in the context of U.S. state DBN laws, some organizations are not reporting as they were not aware of the data breach occurring. As examined in [14][17] also notes that the U.S. has various state DBN laws, which may result in conflicting and inconsistent rulings. In this instance, organizations are required to notify end-users accordingly to each state's DBN law and abide by each state's legislative requirements. The author concludes that DBNs provide the end-users the ability to protect themselves from future ID theft. Organizations, on the other hand, need to determine when to report to avoid the issue of over-reporting. In a valuable analysis of reporting data breaches, [17] was able to show the positives and negatives of DBN laws, from the perspective of the U.S. Unlike [17][8] argues that U.S. state DBN laws inform customers (i.e. end-users) that their data was disclosed to third parties (i.e. hackers), but not in relation to "injury stemming from the underlying data breach", but rather simply a notification to follow due process. The study acknowledges the role of state DBNs but the underlying data breach problem is not examined.

C. Protecting End-User Data by Notification

A prevailing notion of data breaches is the concept of hackers accessing and infiltrating end-user data. While [18] claims that data breaches are not new, the unauthorized access of end-user data is more important than ever given the reach of the dark web. Furthermore, the author compares the Australian, U.S. and EU regulatory environment, in particular, the DBN landscape. [18] presents the 2013 Yahoo! Inc. data breach that affected over 1 billion users (e.g. end-users) as an example of the widespread data breach issue. In the U.S. context, [8] reviews, state-level DBNs and how organizations are seeking to operate within states that enforce "weaker standards". However, in this review, the author notes that negligence in view of the failure to protect end-user data is enforceable; however, not all data breaches can be predicted or prevented and "this means that businesses should not have a duty to guard against innovative breaches that have no known or effective defense at the time of attack". [8] also provides an example of an innovative breach in which hackers could remotely control HP printers over the Internet.

Finally, using a unique approach, [19] examines 13 DBN templates from U.S. state and federal agencies using document analysis. Apart from concerns for breached entities, the author's analysis showed that in that all 13 templates, the DBN message downplays the effect of the data breach. The concluding remarks from the templates found that apologies are rarely given, and all include a change in focus from undesirable to desirable news. The author concludes that the DBN templates signified a tendency to explain the data breach and to mitigate the blow of potential end-user PII risks and threats.

V. Data Breach Cases

Studies addressing data breach cases generally reflect on notable hacking events that have caused considerable end-user implications. The selection of three data breach cases allows the study to focus on several industry sectors such as online services, healthcare, and credit bureaus. While other cases were presented throughout the literature, it was the 2011 Sony PlayStation (PSN), 2015 Anthem and 2017 Equifax data breaches that stood out. The three cases included the timeline of events, such as when the attack occurred, when the data breach entity notified their end-users and other important events.

A. The 2011 Sony PlayStation Network Data Breach: End-Users Sidelined

In April 2011, a large-scale data breach affected the Sony PSN, which forced Sony to shut down the network until the breach was contained [20]. Several studies investigated the Sony PSN data breach and the financial impact it had on its shareholders, the distress for their users (i.e. end-users) and the long-term implications of disclosed end-user data [21–22]. [21] states that Sony did not notify its end-users that the data breach occurred and kept them in the dark for over a week until news reports emerged on the issue. Similarly, [8] reviews the Sony PSN data breach and states that over 75 million users (i.e. end-users) were affected. The author notes that the users' names, physical addresses, email addresses, dates of birth, usernames, passwords, and credit and debit card information were disclosed. More comprehensively, [20] investigated the Sony PSN data breach and analyzed end-user compensation by using the survey method in two data collection rounds. They noted that certain points along the data breach timeframe signified milestones in capturing end-user compensations, presented in Table I. However, they failed to factor in that data breach issues are long-lasting and might not be foreseen until years later. Unlike [20], [21] argues that data breaches often go unnoticed for a considerable period, and that compensating end-users provides little support for long-term implications.

Table I. Sony PSN Data Breach Timeline adapted from [20]

Date	Event
April 17-19, 2011	Initial attack occurs.
April 20, 2011	Sony turns off PlayStation Network, admits service outages.
April 23, 2011	Sony expresses regret at outage.
May 1, 2011	Sony promises a compensation package for affected users.
May 2, 2011	Sony issues press release saying PSN is offline for maintenance after suspected attack.
May 4, 2011	Sony confirms that personal information from users accounts had been compromised.
May 15, 2011	Sony begins bringing network services online.
June 3, 2011	Sony releases "Welcome Back" compensation package to users.
June 5, 2011	Sony "Welcome Back" package closed.

B. 2015 Anthem Healthcare Data Breach: Sensitive Data

The 2015 Anthem Healthcare data breach resulted in an unanticipated amount of scrutiny on the company. It is one of the most significant healthcare data breaches, affecting over 80 million customers [23]. [24] states that hackers disclosed records containing "names, birthdays, addresses and social security numbers". However, in this event, it was noted that the data breach was reported only days after it was discovered, as opposed to the Sony PSN data breach. Similarly, [25] examines the Anthem data breach and notes that hackers are increasingly targeting the healthcare sector. Table II below outlines key events from the Anthem data breach adapted from [25]. [23] notes that healthcare records have a higher value rate on the black market compared to credit card information. In an earlier study, [9] maintains that in order to improve trust, transparency must be practiced.

Table II. Anthem's Data Breach Timeline adapted from [25]

Date	Event
August 2014	Community Health Network was breached by hackers and disclosed sensitive information.
August 2014	Federal Bureau of Investigation (FBI) warned healthcare providers that hackers are targeting their systems.
December 2014	Hackers breached Anthem's security defenses and were inside critical services retrieving customer healthcare records.
January 27, 2015	Anthem discovered the data storage systems were hacked.
January 29, 2015	Anthem notified federal authorities their systems had been targeted and hacked.
February 4, 2015	Anthem notified the public that they suffered a data breach.
February 4, 2015	FireEye managing director David D'Amato noted that the Anthem data breach was a result of very advanced and customized hacking techniques.
February 5, 2015	Anthem advised customers to sign up for credit monitoring.
February 23, 2015	Anthem CEO, Joseph R. Swedish formally announced to customers that the organization had suffered a data breach incident from an advanced hacking technique.
March 18, 2015	Others disagreed that the data breach was sophisticated but rather stemmed from simple email phishing attacks.
May 27, 2015	Research showed that healthcare data breaches are the most expensive to rectify, costing $398 per personally identifiable record (PIR).
June 12, 2015	Customers realize financial harm is not their top concern but instead are monitoring their physical safety.

While the Anthem data breach bought undesirable consequences, the company immediately reported the data breach and notified the customers by email and if available, by mail [24].

C. The 2017 Equifax Data Breach: Financial Data

The 2017 Equifax data breach directly affected over 145 million people, including "names, Social Security Numbers, birth dates, addresses and, in some instances, driver's license numbers" [26]. Table III presents the Equifax data breach timeline and associated issues. The irony here is that not only did the data breach affected half of the U.S. population, but in fact, those affected were not even aware that their data had been collected. Those affected were not direct customers of Equifax, but rather Equifax is a credit bureau that collects and stores the social, financial, personal and other sensitive information of millions of individuals. [27] describes the Equifax data breach and presents the challenges that the hack brought to the people affected. Such challenges included the Equifax IT department's failure to patch "a known vulnerability in the Apache Struts server software" [27]. The former CEO, Richard Smith, failed to acknowledge poor corporate leadership and managerial decisions. However, the similarity of this breach [27] to others, e.g. to the 2013 Target Corp. breach [14] is that the DBN occurred only several weeks after the initial discovery by Equifax.

Table III. Equifax's Data Breach Timeline adapted from [26][28]

Date	Event
March 7, 2017	Apache Software Foundation notified of the vulnerability in its Struts software and released a patch update.
May 13, 2017	Hackers identified Equifax's Struts vulnerability and began accessing customer information.
July 29, 2017	Equifax discovered it had been breached and instructed the information security department to patch the Apache Struts vulnerability.
August 1-2, 2017	Two top Equifax executives sold millions of dollars' worth of shares before reporting the data breach to the public.
August 30, 2017	Equifax created a website intending to notify consumers about the data breach prior to reporting to the public; however, the link directed many consumers to a hoax website.
September 7, 2017	Equifax reported the data breach to the public.
September 2017	Equifax's poor customer support led 15 million consumers to visit the company's website for more information concerning the data breach.
September 27, 2017	Equifax offered affected consumers to use the company's Trusted-ID Premier service to monitor identity information.
October 2, 2017	Equifax determined that an additional 2.5 million consumers had their data disclosed.
October 12, 2017	Further investigation indicated that Equifax's website embedded fake Adobe Flash download links, leading customers to install adware.

While the 2017 Equifax data breach exposed the personally identifiable information (PII) of 147 million people [35], it was at this very time, that the company lobbied the U.S. Congress against data protection laws. For example, [10] describes how Equifax spent millions on promotion of anti-data protection rights and DBNs, in an attempt to curb passage of data protection laws. The author states that the Equifax data breach, arguably the most prolific data breach in history, bought attention to stakeholders including consumers, companies and politicians, that "Congress should pass a federal law that would regulate the way companies

collect and store mass amounts of personal data" [10]. Finally, [29] indicated that while stakeholders aim to enact adequate laws, responding to data breaches represents one of the greatest challenges to data protection.

VI. Discussion and Conclusion

This paper has reviewed cloud computing data breach literature with a focus on the regulatory implications of the technology. There are four outcomes from the review of cloud computing literature. The first outcome concentrates on the outdated U.S. data privacy regulation. From the analysis of studies centered on environmental considerations in the field of cloud computing, it is evident that regulation has not kept up with the technology. This is often known as the "pacing problem" [36][37]. Marchant describes the pacing problem as having two dimensions. The first dimension has to do with the existing legal frameworks that are static while the world is dynamic, and innovation happens as does the social shaping of technology. The second dimension is related to legal institutions and their inability to keep up with change in society and constantly adjusting technology, and with technology deployment models and their possible configurations. [36] squarely points the finger at legislatures, regulatory agencies, and the courts, noting that "[t]he legislative process is notoriously slow, with Congress and state legislatures only capable of addressing a small subset of the plethora of potential issues before them in any legislative session. Issues are often not addressed on the basis of their importance, but rather as a function of headlines and perceived political urgency and expediency." It's important to emphasize the new direction that Marchant is taking with the positive contributions of soft law, although that is not without its critics. More recently [38] has directly worked on the new ways in which the governance of artificial intelligence can occur.

A. U.S. Data Privacy Regulation Landscape

While existing U.S. data privacy regulation, such as the Health Insurance Portability and Accountability Act (HIPPA), Gramm Leach Bliley Act (GLBA) and Stored Communications Act (SCA), aim to protect end-user information, their applicability is questionable in the cloud context. In terms of SCA, it was evident that the regulation provided minimum data privacy benefits and is non-applicable to emerging technologies such as cloud computing. In the U.S. setting, cloud providers and cloud customers are using industry specific regulation, often not intended for cloud services. Finally, several studies recommended the introduction of universal and federal data privacy regulation targeting cloud services.

B. The Requirement for Federal Data Breach Notification

The second part of this paper examined U.S. data breach notifications, reporting on breaches and data protection implications. This formed the second outcome, focused on the absence of federal U.S. DBN laws. The absence of a federal DBN was the most debated topic within the literature. Studies revealed that 50 U.S. states have their own notification processes, which resulted in confusion and lack of clarity for cloud providers and customers in terms of adherence. When a data breach does occur, a cloud provider or customer is required to notify their end-users in one state, and completely ignore notifying customers in another. This type of inconsistency was challenging for cloud providers and customers, adding further delays to an overwhelmed reporting process. Another obstacle in DBNs was that of inconsistent penalties and accountability measures. Cloud providers or business/government customers that were breached, passed their penalty fees onto their insurers and gradually increased end-user subscription fees to a given service. The price of security and privacy is conveniently camouflaged to the end-user who bears the brunt of production failures [39].

C. Cross-Case Comparison of Data Breaches

The three case studies indicated that organizations are susceptible to data breaches regardless of their size and reputation. Table IV provides a cross-case comparison of the type of data disclosed in each of the data breach incidents. The 2011 Sony PSN breach impacted over 75 million end-users and disclosed their PII. The 2015 Anthem breach impacted over 80 million end-users and disclosed PII and health information. The 2017 Equifax breach had more than 145 million end-users having their PII, and financial information disclosed. Finally, the three data breaches each had a significant number of end-user data disclosed.

Table IV Cross-Case Comparison of Data Breaches

	2011 Sony PSN data breach	2015 Anthem data breach	2017 Equifax data breach
No. of end-users impacted	> 75 million	> 80 million	>145 million
Names	✓	✓	✓
Dates of birth	✓	✓	✓
Physical addresses	✓	✓	✓
Email addresses	✓		
Usernames	✓		
Passwords	✓		
Telephone numbers			
Credit and debit information	✓		
Financial information history			✓
Healthcare information		✓	
Social security numbers		✓	✓
Driver's license			✓

There were two similarities between the data breach cases. The first was that each company delayed notifying their respective end-users that their personal and sensitive information had been disclosed. The second similarity was they all insisted that end-users should consider obtaining ID fraud protection. It is of equal importance to address the differences between the cases. There were also two differences in how the organizations managed data breach prevention and their response to the incident. The first difference targeted data breach prevention, such as notices from third parties that hackers were targeting specific industries. Anthem received ample warnings from the FBI that hackers were targeting healthcare information. Equifax received an urgent update from Apache that a critical patch

was required to be installed to the Strut software program. The second difference was that Sony took their cloud service offline, while Anthem and Equifax kept their services active. Table V presents the similarities and differences between the three data breach cases.

Table V Similarities and Differences of Data Breach Cases

	2011 Sony PSN data breach	2015 Anthem data breach	2017 Equifax data breach
Similarity – Delayed notification	✓	✓	✓
Similarity – Recommending ID fraud protection	✓	✓	✓
Difference – Data breach notices		✓	✓
Difference – Service active after data breach		✓	✓

D. Conclusion

This paper demonstrates the failure to learn from past data breaches and to secure emerging technologies, such as cloud computing. It has additionally reviewed the likely problems facing organizations and end-users. While we are still learning how to address data breaches, the cloud has brought to the fore existing issues, while also adding new concerns related to devices and services that previously had not been associated to cloud systems. It is essential to ask why we are continuously failing to learn from past data breaches, but also vital to understand the future implications of adopting new technologies and how they will affect our day-to-day lives. The role of regulation must also be further examined in light of the findings of this research.

REFERENCES

[1] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things: threats and challenges," *Security and Communication Networks,* vol. 7, no. 12, 2014, pp. 2728-2742.

[2] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing - The business perspective," *Decision Support Systems,* vol. 51, no. 1, 2011, pp. 176-189.

[3] A. Adrian, "How much privacy do clouds provide? An Australian perspective," *Computer Law & Security Review,* vol. 29, no. 1, 2013, pp. 48-57.

[4] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," *IEEE Internet Computing,* vol. 16, no. 1, 2012, pp. 69-73.

[5] P. T. Jaeger, J. Lin, and J. M. Grimes, "Cloud Computing and Information Policy: Computing in a Policy Cloud?," *Journal of Information Technology & Politics,* vol. 5, no. 3, 2008, pp. 269-283.

[6] R. Helles and S. Lomborg, "Regulatory response? Tracking the influence of technological developments on privacy regulation in Denmark from 2000 to 2011," *Policy & Internet,* Article vol. 5, no. 3, 2013, pp. 289-303.

[7] N. Rastogi, M. J. K. Gloria, and J. Hendler, "Security and Privacy of Performing Data Analytics in the Cloud," *Journal of Information Policy,* vol. 5, 2015, pp. 129-154.

[8] J. A. Fisher, "Secure my data or pay the price: Consumer remedy for the negligent enablement of data breach," *William & Mary Business Law Review,* vol. 4, no. 1, 2013, pp. 215-239.

[9] J. A. Harshbarger, "Cloud Computing Providers and Data Security Law: Building Trust with United States Companies," *Journal of Technology Law & Policy,* vol. 16, no. 2, 2011, pp. 229-256.

[10] M. L. Kuhn, "147 million social security numbers for sale: Developing data protection legislation after mass cybersecurity breaches," *Iowa Law Rev.,* vol. 104, no. 1, 2018, pp. 417-446.

[11] C. A. Tschider, "Experimenting with privacy: Driving efficiency through a state-informed federal data breach notification and data protection law," *Tulane Journal of Technology & Intellectual Property,* vol. 18, no. 1, 2015, pp. 45-82.

[12] W. Robison, "Free at what cost?: Cloud computing privacy under the stored communications act," *Georgetown Law Journal,* vol. 98, no. 4, 2010, pp. 1195-1239.

[13] H. T. M. Nguyen, "Cloud cover: privacy protections and the Stored Communications Act in the age of cloud computing", *Notre Dame Law Rev.,* Article vol. 86, no. 5, 2011, pp. 2189-2218.

[14] N. Manworren, J. Letwat, and O. Daily, "Why you should care about the Target data breach", *Bus. Horiz.,* Note vol. 59, no. 3, 2016, pp. 257-266.

[15] V. Mikhed and M. Vogan, "How data breaches affect consumer credit," *Journal of Banking and Finance,* vol. 88, no. 3, 2018, pp. 192-207.

[16] Y. Zou and F. Schaub, "Beyond Mandatory: Making Data Breach Notifications Useful for Consumers", *IEEE Secur. Privacy,* Article, vol. 17, no. 2, 2019, pp. 67-72, Art no. 8677354.

[17] T. Caldwell, "Reporting data breaches," *Computer Fraud & Security,* vol. 2012, no. 7, 2012, pp. 5-10.

[18] A. Daly, "The introduction of data breach notification legislation in Australia: A comparative view," (in English), *Computer Law & Security Review,* Article vol. 34, no. 3, 2018, pp. 477-495.

[19] J. R. Veltsos, "An Analysis of Data Breach Notifications as Negative News," *Bus. Commun. Q.,* Article vol. 75, no. 2, 2012, pp. 192-207.

[20] S. Goode, H. Hoehle, V. Venkatesh, and S. A. Brown, "User compensation as a data breach recovery action: An investigation of the Sony PlayStation network breach," *MIS Quarterly,* vol. 41, no. 3, 2017, pp. 703-A16.

[21] L. Bonner, "Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches," *Washington University Journal of Law & Policy,* vol. 40, 2012, pp. 257-278.

[22] C. Cachin and M. Schunter, "A cloud you can trust," *Spectrum, IEEE,* vol. 48, no. 12, 2011, pp. 28-51, doi: 10.1109/ MSPEC.2011.6085778.

[23] E. M. Kass, "Do federal regulations help or hinder patient data security?", *Health Data Management,* vol. 23, no. 4, April 2015, pp. 24, 26, 28.

[24] B. V. Newman, "Hacking the current system: Congress' attempt to pass data security and breach notification legislation," *University of Illinois Journal of Law, Technology & Policy,* vol. 2015, no. 2, 2015, pp. 437-460.

[25] R. L. Garner, "Evaluating solutions to cyber attack breaches of health data: How enacting a private right of action for breach victims would lower costs," *Indiana Health Law Review,* vol. 14, no. 2, 2017, pp. 127-172.

[26] C. Kenny, "The Equifax data breach and the resulting legal recourse," *Brooklyn Journal of Corporate, Financial & Commercial Law,* vol. 13, no. 1, 2018, pp. 215-238.

[27] H. Berghel, "Equifax and the Latest Round of Identity Theft Roulette," *Computer,* vol. 50, no. 12, 2017, pp. 72-76.

[28] T. G. Siracusa Jr., "The Equifax breach: What we learned and how we can protect consumer data," *Loyola Consumer Law review,* vol. 30, no. 3, 2018, pp. 460-473.

[29] J. L. Mills and K. Harclerode, "Privacy, mass intrusion, and the modern data breach," *Florida Law Review,* vol. 69, no. 3, 2017, pp. 771-830.

[30] Y. Rahulamathavan, M. Rajarajan, O. F. Rana, M. S. Awan, P. Burnap and S. K. Das, "Assessing Data Breach Risk in Cloud Systems," 2015 *IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom)*, 2015, pp. 363-370.

[31] C. Wang, S.T.K. Jan, H. Hu, D. Bossart, G. Wang, "The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services", *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, Tempe, AZ, USA, 2018, pp. 196–203.

[32] P.R. Kumar, P.H. Raj, P. Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing", *Procedia Computer Science*, vol. 125, 2018, pp. 691-697.

[33] S. Logesswari, S. Jayanthi, D. KalaiSelvi, S. Muthusundari, V. Aswin, "A study on cloud computing challenges and its mitigations", *Materials Today: Proceedings*, 2020.

[34] S. Mandal, D.A. Khan, "A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic", *2020 International Conference on Smart Electronics and Communication (ICOSEC)*, 2020, pp. 837-842.

[35] FTC. "Equifax Data Breach Settlement", *Federal Trade Commission: protecting America's Consumers*, January 2020, www.ftc.gov/enforcement/cases-proceedings/ refunds/equifax-data-breach-settlement

[36] G. E. Marchant, "The growing gap between emerging technologies and the law", *The growing gap between emerging technologies and legal-ethical oversight*, 2011, pp. 19-33, Springer, Dordrecht.

[37] G.E. Marchant, “Addressing the pacing problem”, *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight*, 2011, pp. 199-205, Springer, Dordrecht.
[38] G. E. Marchant, ““Soft Law” Governance Of Artificial Intelligence”, *Pulse*, January 25, 2019, aipulse.org/soft-law-governance-of-artificial-intelligence/
[39] J. Lee, K. Kapitanova, S. H. Son, “The price of security in wireless sensor networks”, *Computer Networks*, vol. 54, no. 17, 2010, pp. 2967-2978.
[40] K. Alspach and W.T. Millward, “Partners: Demand For Cloud Services Is ‘Up Significantly’ For 2021”, *CRN*, 26 February 2021, www.crn.com/news/cloud/partners-demand-for-cloud-services-is-up-significantly-for-2021
[41] K. Blind, "The influence of regulations on innovation: A quantitative assessment for OECD countries", *Research Policy*, vol. 41, no. 2, 2012: pp. 391-400.