Cost Of Privacy

Abdulhadi Alalmai,
Chidera A. Eluwa
Cybersecurity of Computer Science
St. Mary's University
San Antonio, Texas USA
aalalmai@mail.stmarytx.edu
celuwa@mail.stmarytx.edu

ABSTRACT

Privacy is the right to be let alone. The control that a person has over how personal information is shared and received. The cost of privacy is usually a burden for data processors or owners. But what is the cost of not protecting it? The consequences of not protecting it has a ripple and adverse effect on the same data owners and consumers. Big organizations and large-scale companies invest a lot of funds in ensuring that privacy is maintained. They perform a risk analysis to identify the possible impact that might occur when privacy has been breached. With this, a budget is planned and set aside for this proactive measure. A big organization like Apple has been very meticulous with the privacy of their consumers and themselves. However, there was a recent privacy violation that affected IOS users. This spyware called Pegasus attacks its users without the users clicking on it. This attack then raises a lot of concerns and questions. What kind of budget do large scale companies set aside to protect the privacy of their consumers? How much do corporate privacy programs cost? What kinds of industries are developing around corporate privacy-related services? What kinds of companies seem to benefit most from proactive privacy efforts? This project will analyze how these questions are answered, evaluate the economics of privacy, and highlight some of the factors that affect the cost of privacy.

Keywords
Privacy, Economics of Privacy, Security, Security Breaches, Cyber-attack, Spyware, Compliance, Personal Identifiable Information (PII)

1. INTRODUCTION

The constitutional Law defines privacy as the right to make certain fundamental decisions concerning deeply personal matters free from government coercion, intimidation, or regulation. Under the common law, privacy generally means the right to be let alone. In this sense, privacy is associated with seclusion. Alan Westin defines privacy as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others [1]. Privacy is often mistaken for security. Although they are related and work well with each other, they have different meanings and serve different purposes. Security protects unauthorized users from gaining access to an individual's personal information, while privacy protects the right of the individual to control how personal information is disclosed and shared. No one in this age of hackers and identity theft questions whether privacy and data security should be a priority. But many privacy efforts are proving counterproductive. Security "breach notices" are an example. First required by the state of California in 2003 but now widespread, these are the letters sent by companies to their customers letting them know about problems connected with their data [2]. Companies are collecting all kinds of data from consumers about online activities, whether the users are browsing the Internet, watching online content, or posting on social media. Together, these records of data make up each user's digital identity. These consumers trust most companies with their information and use their services. But still, on from different companies. Data

aggregators link information coming from different sources to compose individual profiles.

The more organizations and individuals embrace digital technologies, the cheaper and faster become the production and processing of personal, and potentially sensitive, data. Thus, privacy concerns grow as well [5].

Economics of privacy highlights the costs and benefits linked with the changing boundaries between public and private spheres and, with the protection and revelation of personal information. Economics helps us understand how individuals and organizations make decisions about the protection and usage of individuals' data, and what the consequences of those decisions are.

The rest of the paper is organized as follows. In Section 2, we highlight different related works on the cost of privacy from different aspects and the impact on companies. In Section 3, we lay out the present problem that drives our research and focuses on a particular form of privacy incident, consisting of breaches of consumers' privacy. In Section 4, we analyze our research questions and provide insights on the impact on organizations. In Section 5, we discuss some factors that affect the cost of privacy in organizations.

1.1. Background and Motivation

An attack called zero-day is a cyber-attack that hackers use to exploit a system. This attack is hardly noticed by the developers of a system because it is almost invisible. This was the same strategy that "Pegasus" also known as a "zero-click attack" used to exploit iOS and Android users. Pegasus is a spyware. Spyware is a software that obtains information from a user's computer or device without the user's knowledge or consent. This spyware was developed by an Israeli company called NSO group and was first discovered in 2016. In 2019, WhatsApp revealed that NSO's software had been used to send malware to more than 1,400 phones by exploiting a zero-day vulnerability. A group of Canadian researchers discovered this spyware on Apple's iMessage. This spyware has the capacity of turning a phone into a 24-hour surveillance device. It can copy messages sent or received, harvest photos and record users' calls. It can secretly film a user through his/her phone's camera or activate the microphone to record conversations. It can potentially pinpoint a user's location, where you've been, and who you've met. Looking at the capabilities of this spyware and how dangerous it is, it raises a serious privacy and security alarm. For a multinational company like Apple to become susceptible and vulnerable to such an attack, its users are concerned about this privacy breach and exposure. There was also a recent cyber-attack on T-Mobile where thousands of customers personal information had a potential exposure scare. What kind of budget do large scale companies set aside to protect the privacy of their consumers? How much do corporate privacy programs cost? What kinds of industries are developing around corporate privacy-related services? What kinds of companies seem to benefit most from proactive privacy efforts? Every day we hear of different breaches of information. This raises the questions mentioned above and keeps consumers wondering if these big scale organizations spend enough money to keep their information safe. The cost of privacy can be measured from different aspects. In our related works, we will see how different organizations have measured privacy for different purposes and from different aspects.

2. RELATED WORKS

There has been some surveys and analysis on the cost of privacy and the impact of what a security breach can incur. A common motivation for organizations to invest in information security is to safeguard their confidential data as well as their customers' personal information. Over the past few years, privacy incidents have been announced frequently enough to question whether organizations have the necessary incentives to safeguard consumer information [3]. Acquisti et al. presents a comprehensive analysis of the impact of a company's privacy incidents on its market value. A broad data set of instances is compiled of exposures of personal information due to failures of some security mechanism (hacking, stolen or lost equipment, poor data handling processes, and others) and they present the results of various empirical analyses, including event study analysis [3]. Regression analysis is used to show the negative and statistically significant impact on a company when a breach occurs. There is however no solid evidence

that shows how much companies pay to keep their privacy safe, but the results show that larger reputable firms have higher risks and impacts when a privacy breach occurs.

IBM security sponsors a cost of data breach research conducted by Ponemon Institute in 2019. Based on in-depth interviews with more than 500 companies around the world who experienced a data breach between July 2018 and April 2019, the analysis in this research study considers hundreds of cost factors, from legal, regulatory, and technical activities to loss of brand equity, customer turnover, and the drain on employee productivity [4]. The analysis shows that malicious attacks are the most expensive root cause of breaches and small businesses face larger costs relative to organizations. Encryption is the highest cost mitigator reducing breach cost by an average of $360,000. Companies with an incident response team extensive testing were able to save over $1.2 million. Automation of security along with encryption is recommended as concrete ways that organizations can mitigate costs and improve overall security posture.

In modern information economies, the reduction of the cost of storing information has made it possible to capture, save, and analyze increasing amounts of information about the individual and companies record details of each customer transaction [5]. Alessandro Acquisti reports on the economic implications of the protection and revelation of personal data by measuring the data from the consumer's view and the organization's view. This analysis also examines the privacy-related trade-offs for data subjects (the consumers) and data holders (the organization). The recommendation provided for solving this privacy economics issue is to find a balance between information sharing and information hiding that is in the best interest of data subjects but also of society.

Robert Gellman analyzes the costs to businesses of not protecting the privacy and costs consumers incur when privacy is not protected. The absence of privacy rules imposes expenses on businesses that many industry-sponsored studies ignore when calculating the costs of privacy and when laws and practices do not provide adequate protection for personal information, individuals act to protect themselves and their privacy [6]. Sales Losses, Lost International Opportunities, Increased Legal Costs, and Investor Losses are some of the consequences highlighted in this analysis that businesses face when they fail to protect their consumer's personal information. The author Gellman points out that measuring costs must be fair and not biased or one sided and privacy is not measured solely with a financial yardstick. This research is however not an academic study of the issue of privacy costs but identifies the types of costs that are ignored in business - sponsored studies.

Michael A. Turner publishes a rebuttal to Robert Gellman's debate on measuring the true cost of privacy. Gellman's failure to disaggregate business processes ed him to assume without proving, that information sharing is part of an old and now discredited business model [7]. Turner argues that Gellman's research is without a quantitative analysis and the costs identified are poorly calculated without including economic models. The author recommends that future research should be built upon the first generation of quantitative data restriction when measuring privacy costs.

Taylor et al. draw empirical research on the economic value and consequences of protecting and disclosing personal information, and on consumers' understanding and decisions regarding the trade-offs associated with the privacy and the sharing of personal data [8]. This survey delves into numerous kinds of literature across a variety of disciplines and fields, from marketing to economics to computer science highlighting that personal information has both private and commercial value and that the sharing and protection of personal data can have both positive and negative impacts on the economic market.

While privacy and security of personal information remain a concern for many, the economic incentives have not generated widespread adoption, and government intervention has increased the responsibilities for companies to collect personal information, without determining their liabilities for misuses of those data [9]. The author of this research distinguishes between on-line and off-line identities of an individual and each type of identity raise different privacy concerns and economic implications and highlights those generating incentives to handle personal information in a new way, appropriate legal

intervention can allow the growth of the market for third parties providing solutions that anonymize off-line information but make it possible to share on-line profiles.

John et al. use a field experiment informed by behavioral economics and decision research to investigate individual privacy valuations and find evidence of endowment and order effects [10]. Individuals assigned markedly different values to the privacy of their data depending on (1) whether they were asked to consider how much money they would accept to disclose otherwise private information or how much they would pay to protect otherwise public information and (2) the order in which they considered different offers for their data. The gap between such values is large compared with that observed in comparable studies of consumer goods [10].

3. PEGASUS DATA BREACH AND THE COST OF ITS EFFECT

In this section, our focus is on a particular privacy breach called “Pegasus” and the cost of its effect on the affected users and companies. As mentioned in the introduction, Pegasus is a spyware, and a spyware is any software that installs itself on your computer and starts covertly monitoring your online behavior without your knowledge or permission. Spyware is a kind of malware that secretly gathers information about a person or organization and relays this data to other parties. Pegasus was first developed by an Israeli NSO group. It runs mostly on iOS and some Android operating systems. Its iOS exploitation was first identified in August 2016 by some Canadian citizen lab researchers in the University of Toronto when a failed installation attempt on the iPhone of a human rights activist led to an investigation revealing details about the spyware, its abilities, and the security vulnerabilities it exploited. News of the spyware caused significant media coverage. It was called the "most sophisticated" smartphone attack ever and was the first time that a malicious remote exploit used jailbreaking to gain unrestricted access to an iPhone [11]. Rather than being a specific exploit, Pegasus is a suite of exploits that uses many vulnerabilities in the system. Infection vectors include clicking links, the Photos app, the Apple Music app, and iMessage. Some of the exploits Pegasus uses are zero-click—that is, they can run without any interaction from the victim. Once installed, Pegasus has been reported to be able to run arbitrary code, extract contacts, call logs, messages, photos, web browsing history, settings [12]. Although the NSO group claims that this spyware was developed to track and identify criminals, it has caused a lot of privacy violations and breaches to unintended users and organizations.

Figure 1.0: An illustration of the data collected by Pegasus
Source: Hacking Team Emails

The above figure shows some of the information that Pegasus collects from its target iOS system. For example, customers can request the spyware to send an alert and record information only when the target is communicating with a specific phone, or the target arrives at a specific location or travels to a geographical area.

3.1 Cost of The Effect of This Breach

Security researchers confirmed that thousands of iPhones were compromised and unfortunately because the attack is a zero-day attack, it is very challenging for security experts to identify and retrieve the compromised information of the affected users. NSO reported $240 million in revenue in 2021 and this questions the security reputation of a big technology company like Apple.

Apple was hit with different lawsuits regarding this breach as it violated the privacy of thousands of its consumers. While facing these violation lawsuits, they presented ways to mitigate this issue and protect their system from subsequent and frequent attacks.

One of the ways Apple tried to curb this issue is to introduce new iOS frequently for updates and patching. These updates and patches help to eliminate or reduce the present spyware in the device.

Figure 2.0: Target of Pegasus
Source: Pegasus Project

4. RESEARCH QUESTIONS

In this section, we are going to highlight the research questions and its impact on organizations.

4.1 *What kind of budget do large scale companies set aside for the privacy of their consumers?*

This question is one of the most important questions in evaluating the cost of privacy. There have been so many cases of data breaches in different organizations. It leaves its consumers extremely worried because these companies are expected to protect the information of their users and employees. A quantitative research carried out by the International Association of Privacy Professionals (IAPP) in 2014 reports that the Fortune 1000 spends roughly $2.4 billion on managing privacy, a number referred to as the Privacy Industry Index and an approximate average of $76 per employee on privacy, or $204 per $1 million in revenue, while the smallest company does about $2.5 billion in revenue [13].

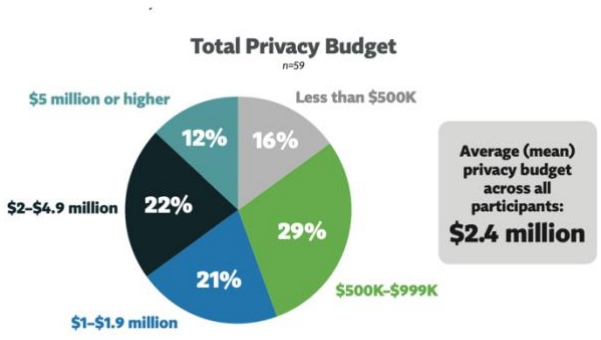

Figure 3.0: Total Privacy Budget
Source: IAPP Report

The above image shows the total percentage of the privacy budget and the average mean across all participants. 12% confirmed investing $5 million or higher on privacy, 16% confirmed investing less than $500k, 29% confirmed investing between $500k - $999k, 21% confirmed investing between $1–$1.9 million and 22% confirmed investing $2-$4.9 million.

4.2 *How much do corporate privacy programs cost?*

Corporate businesses have an obligation to protect the privacy of all employees and ensure their security on the job and publicly traded companies can also benefit from putting policies in place to protect their private information and assets. Costs may vary greatly depending on the nature of the business, the demographics of users, and the laws governing the private information collected. There are different bodies and compliance regulations that companies must comply with. The GDPR (General Data Protection Regulation) for the European Union and CCPA (California Consumer Privacy Act) have specific procedures put in place for handling private consumer information that must be complied with. All the data collected by an organization is included in their privacy policy as well as any third party involved in the collection of the data. This compliance comes with a cost.

While European companies are already facing the unpleasant costs of GDPR, among Fortune 500 firms the costs are soaring even higher. GDPR is costing the average Fortune 500 company a whopping $16 million.

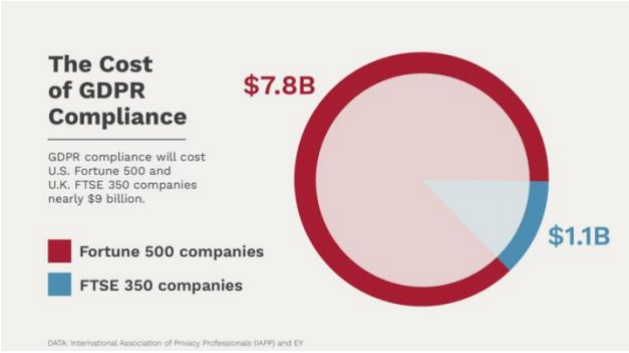

Figure 4.0: Cost of GDPR Compliance
Source: Forbes

The above pie chart shows the cost of GDPR compliance between Fortune 500 and Financial Times-Stock Exchange (FTSE) 350 companies. It costs Fortune 100 companies approximately $7.8 billion to comply with the GDPR laws and regulations and FTSE approximately $1.1 billion to comply. As corporate organizations face challenges with compliance, it is the law and must be obeyed. The organizations that do not comply spend more money to remediate when privacy is violated or when data has been breached.

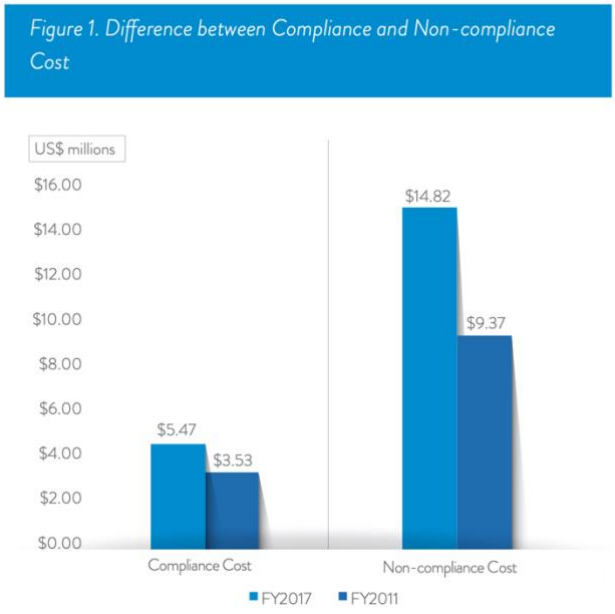

Figure 5.0: Cost of Compliance and Non-Compliance
Source: Ponemon Institute

The above figure shows an estimate of how much compliance costs against non-compliance. As we can see from the chart, compliance costs approximately $5.47 million in 2017 and non-compliance costs $14.82 million in 2017, which leaves a difference of $9.35 million.

4.3 *What kinds of industries are developing around corporate privacy-related services?*

The technology industry and the precipitous growth of the IoT and the frequently reported data leaks suffered by large companies will likely contribute to an environment in which consumer demands for privacy and data security rise along with increases in the quantity and types of consumer data. This presents various opportunities for companies to monetize consumer privacy [14]. These companies are using IoT devices to collect information from their consumers.

4.4 *What kinds of companies seem to benefit most from proactive privacy efforts?*

Adhering to corporate privacy and its policies can be beneficial to organizations in many ways. A legislation in GDPR mandates that each organization have a Data Protection Officer (DPO) that ensures that the data of the consumers, as well as staff of the organization, is secure and organizations will have to comply with a set of data protection principles under the GDPR, ensuring that the necessary framework is in place to keep data subjects' personally identifiable information secure. The companies or organizations (in the IT industry to be precise) that communicate and provide services to consumers stand a better advantage from proactive privacy efforts. These proactive efforts save the organizations from a lot of things. It reduces maintenance costs. For example, following a GDPR's mandate to keep data inventory up to date prompts the organization to retire any data inventory software and legacy applications that are no longer relevant to your business. It also provides improved consumer confidence. When the consumers are certain that their PII is safe and secure, they will stick to that company and keep patronizing them, yielding more money and business opportunities for the company.

Also, organizations will have to move towards improving their network, endpoint, and application security. Migrating towards the latest technologies – virtualization, cloud computing, BYOD and The Internet of Things (IoT) – can serve two purposes: one, giving you a way to manage the growing demand for data more effectively and two, allowing the opportunity to offer end users augmented products, services, and processes.

5. DISCUSSION

We have seen the outline of the research questions of the paper in the previous section 4. Some organizations take the privacy of their consumers as a priority and budget a lot of funds to protect their personal information. According to research and frequent evaluations and analysis, the bigger the organization, the more money is spent. This is

because larger organizations have a wider market and consumers. A company like Apple with thousands of staff need to protect millions of customers' information. This automatically triples the number of funds spent for their protection. However, there are a lot of factors that affect the cost of privacy and factors that affect why some organizations can't afford to spend so much to protect their customer's information.

5.1 Factors that Affect the Cost of Privacy

There are a lot of factors that affect how organizations plan to budget for privacy. We're however going to highlight the major factors that affect this cost.

5.11 *Value of Personal Data*

One of the major factors that affect the cost of privacy is the value of the personal data being collected. Organizations who hold personal identifiable information of consumers spend the highest amount of money on the protection of the data because such kind of sensitive information collected has substantial economic value.

5.12 *The Population of The Market (Supply and Demand)*

The population of the market to which services are rendered is another factor that affects the cost of privacy. As mentioned earlier, larger, and high-end organizations that have larger consumers must spend more money on privacy compared to smaller organizations with smaller users. It is however more difficult trying or attempting to protect large masses of people because when a violation occurs, it affects the whole crowd and curbing or remediating such issues isn't the easiest.

5.13 *Security and Privacy Awareness and Training*

Organizations require security and privacy expertise when protecting data. With this, frequent training and risk assessments are carried out on the team responsible for the protection of data. Some organizations also must carry out third party and vendor risk assessments to confirm that their vendors are also complying with the privacy regulations and that their assets are in safe hands. Carrying out such assessments and training costs the organizations a token. And because security and privacy need to be monitored frequently, these training and assessments need to be continuous.

5.14 *Compliance Cost*

As mentioned earlier in the previous section, every company or organization is required to have a Data Protection Officer (DPO) mandated by the GDPR to oversee that privacy compliance is met. Compliance cost is associated with several components of data privacy legislation: data protection officers; privacy audits, improving data quality to facilitate subject requests, costs associated with four types of potential user rights (access, data portability, deletion requests, and data correction also called data rectification), the costs of increased legal risk and duplicative enforcement, and productivity costs for consumers because of pop-up consent notices. Some organizations may hire consultants to help manage their requirements under the law. Others, especially those with many complex systems that handle personal data may hire several internal data protection officers to solely handle compliance. Some organizations especially those with a small amount of personal information may simply delegate the task to current employees.

5.14 *Privacy Audit*

Some privacy laws require organizations to submit to periodic compliance audits, administered by either their organization or a third party [15]. Audit requirements will likely affect different types of businesses in different ways, based on the types of data they collect, and the protections required in the law. Audits will likely be required, for example, after a data breach, series of complaints, or random inquiry from a regulator. To estimate this cost, we used HIPAA compliance as a benchmark. According to the health care compliance company Datica, a full HIPAA audit costs between $30,000 and $60,000 for both employee and direct costs [16]. And if for example, small-sized businesses spend $10,000 per audit, the cost will go up as the size of the businesses increase.

6. CONCLUSION

Although estimating the economic value of privacy is challenging, it is not impossible to estimate the social costs of implementing privacy regulations and the estimate of social costs in other policy areas [17]. The benefits of privacy must also be fairly assessed because privacy saves money and If privacy rules force record keepers to keep fewer records or to maintain records for a shorter period, the costs of record maintenance will be reduced [18].

ACKNOWLEDGEMENTS

We would like to thank our professor Dr Bokaei Mitra Hosseini for giving us the opportunity to thoroughly understand privacy and everything that it entails. We have been able to learn the rights that humans have as well as the regulations and standards that the federal government has set concerning privacy protection and compliance. This research has really broadened our knowledge and has given us the courage to face real-world problems in cybersecurity. Lastly, we would like to thank our professor for the feedback on our draft and the final presentation that helped with the improvement of this paper.

REFERENCES

[1] A. F. Westin, "Privacy And Freedom," *Washington and Lee Law Review*, vol. 25, no. 1, pp. 167-170, 1968.

[2] L. Gomes, "The Hidden Cost of Privacy," 21 May 2009.

[3] A. Acquisti, A. Friedman and R. Telang, "IS THERE A COST TO PRIVACY BREACHES? AN EVENT STUDY," *ICIS 2006 proceedings*, p. 94, 2006.

[4] I. S. a. P. Institute, "Cost of a Data Breach Report," IBM Security, 2019.

[5] A. Acquisti, "The Economics of Personal Data and the Economics of Privacy," 2010.

[6] R. Gellman, "Privacy, Consumers, and Costs," vol. 6, no. 2, p. 02, 2002.

[7] M. A. Turner, "Measuring the True Cost of Privacy: A Rebuttal to “Privacy, Consumers, and Costs”," pp. 1-19, 2002.

[8] C. Taylor, A. Acquisti and L. Wagman, " The Economics of Privacy," *Journal of Economic Literature*, vol. 54, no. 2, pp. 442-92, 2016.

[9] A. Acquisti, "PRIVACY AND SECURITY OF PERSONAL INFORMATION : Economic Incentives and Technological Solutions," pp. 179-186, 2004.

[10] L. K. John, A. Acquisti and G. Loewenstein, "What Is Privacy Worth?," *The Journal of Legal Studies*, vol. 42, no. 2, pp. 249-274, 2013.

[11] L. Franceschi-Bicchierai, "Government Hackers Caught Using Unprecedented iPhone Spy Tool," *Vice Media*, 2016.

[12] N. Perlroth, "IPhone Users Urged to Update Software After Security Flaws Are Found," *The New York Times*, 2016.

[13] IAPP, "Benchmarking Privacy Management and Investments of the Fortune 1000," 2014.

[14] S.-A. Elvy, "PAYING FOR PRIVACY AND THE PERSONAL DATA ECONOMY," *COLUMBIA LAW REVIEW*, vol. 117, no. 6, pp. 1369-1459, 2017.

[15] A. McQuinn and D. Castro, "Law, The Costs of an Unnecessarily Stringent Federal Data Privacy," in *Information Technology & Innovation Foundation*, Washington DC, 2019.

[16] T. Good, "What is the Cost of a HIPAA Audit?," in *Datica*, 2019.

[17] J. J. Cordes and D. R. Pérez, "Measuring Costs and Benefits of Privacy Controls," *The George Washington University Regulatory Studies Center*, pp. 1-15, 2017.

[18] R. Gellman, "Privacy, Consumers, and Costs," *How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete*, pp. 3-36, 2002.