CYBER SECURITY AND ITS EFFECT ON PERSONAL PRIVACY

Dylan W., Mark F., Oon C. L., Phillip K.
University of British Columbia
Contact emails redacted for privacy

Abstract – *Due to the rapid growth of online connectivity, the internet has sparked discussions regarding the privacy and security of digital information. Cybersecurity is becoming crucial due to the entangled nature of society and technology; user data that would previously have been stored offline is now being processed in cloud servers and is vulnerable to attack. Individuals are often forced to interact with cloud services (lacking reasonable alternatives); they are coerced into risking their privacy.*

To suitably address cybersecurity and data privacy, increased regulation is required to protect consumers. The ethical implications of cybersecurity and data collection must be carefully considered; the repercussions of postponing these discussions are severe as irremediable losses can directly impact millions of individuals. Proposed solutions focus on improved transparency and legislation; these policies will lay the foundation for security in a tightly interconnected society.

Keywords: cybersecurity, privacy, legislation, user data

1. INTRODUCTION

In the United States, 157 data breaches were recorded in 2005. By 2020 that number rose almost an order of magnitude to 1001 breaches in 2020.[1]

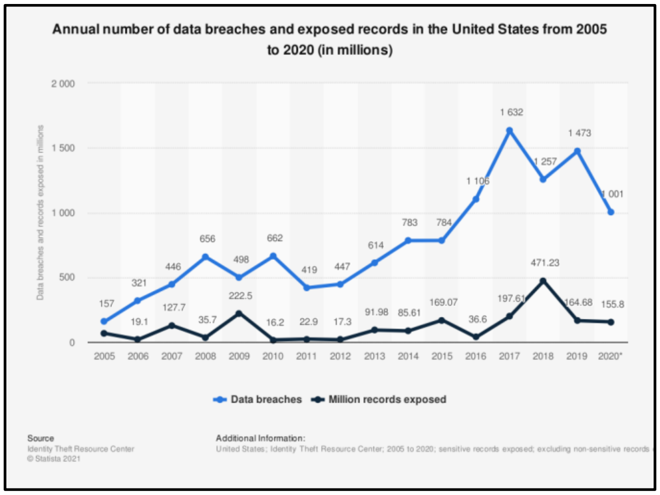


Fig. 1.0.1 – Data breaches 2005-2020.[1]

Online service providers have been collecting user data since the creation of web-based services, but the recent, massive shift towards digital operations in all sectors of the economy has created an enticing target for cyber-criminals. This paper intends to highlight the importance of cybersecurity with respect to personal data and privacy.

Section two discusses the entangled nature of modern society and internet technologies. It is becoming increasingly difficult for a person to contribute as a functioning member of society without having an online presence (for instance, using direct deposit from employers). The internet is also critical for day-to-day communication; users who are simply trying to stay connected with friends and family are unwitting targets of tech giants harvesting data for advertising purposes. Even professional services like computer operating systems and the Microsoft Office suite are now offered as subscription-based services, continually transmitting telemetry user data to the corporation.[12]

Section three explores the cost of ineffective cybersecurity measures. Due to the sensitive nature and resulting value of affiliated user data, the finance and healthcare sectors consistently comprise the majority of data breaches every year.[18] Various data breaches throughout 2015 cost the finance and healthcare sectors an estimated $3 billion in economic losses.[2] A case study analysis of the Equifax and AMCA Healthcare data breaches in section three illustrate the destructive and costly potential of inadequate cybersecurity measures.[3] The financial fallout of data breaches can be quantitatively estimated. Other damages such as identity theft and loss/destruction of personal property are more difficult to calculate, but are of equal significance.

Section four explores established government legislation regarding personal data protection and data collection regulations. A comprehensive history of legislation is covered, including the PDP, PIPEDA, GDPR, and CCPA. The unintended consequences of these pieces of legislation are also discussed, encompassing both the positive and negative aspects. The section concludes with a critical analysis of the historical legislation, and highlights key areas that should be considered when introducing future legislation.

Section five discusses the social responsibility of online service providers to maintain adequate cybersecurity measures for the benefit and protection of end users. Specific, easily employable mechanisms to address the obligation of cybersecurity are discussed in subsections 5.2, and 5.3. Lastly, the role of user awareness is considered in 5.4.

2.0 NECESSITY OF CYBERSECURITY

2.1 Entanglement of Technology and Society

Since the beginning of the digital revolution in the late 20th century, society has rapidly become more closely linked through the use of digital computing and communication technologies.[4] People have grown dependent upon this connectivity; in a 2013 Qualcomm poll, 84% of respondents said they could not live without their smartphone for more than one day.[5] Since smartphones and computers are now ubiquitous, online connectivity has essentially become a requirement for many critical areas of civic life including bill payments, taxes, and education. For example, RBC charges fees for monthly paper statements[6], and the CRA urged all Canadians to use their electronic services to avoid mail service delays during the coronavirus pandemic.[7]

As the use of smartphones and internet messaging increases, traditional communication services such as landline telephones and even the postal service are becoming obsolete as methods for distributing information.[8] There is societal pressure, fueled by the convenience and speed with which information can move online, which compels individuals to use technology to remain connected. Communication was historically handled by government services (like the postal service) and highly regulated telecommunications companies, but now larger volumes of communication are routed through social media.[8] This means that large tech companies now have the power to facilitate or hinder communication between individuals. Telecommunications regulation began with the Communications Act of 1934 (a document still relevant today regarding the debate around net neutrality)[9]; similar data privacy legislation must be established to ensure equitable and secure service – examples of historical attempts at data privacy legislation are presented in section 4.1.

Recently, there has been a shift towards offering software as a service (SaaS) by software developers such as Microsoft.[10] Compared to selling software distributions, SaaS is a more profitable business model, partly because of the potential to collect and monetize user data.[11] This issue is prevalent to the level of operating systems; even the Microsoft Office suite has been harvesting user data in violation of GDPR regulations.[12] As society continues down the path of technological entanglement and Internet of Things (IoT) devices, it is critical to establish strong cybersecurity legislation today to prevent future digital capitalists from profiting through the sale and exploitation of private user data.

2.2 Individuals Privacy Rights

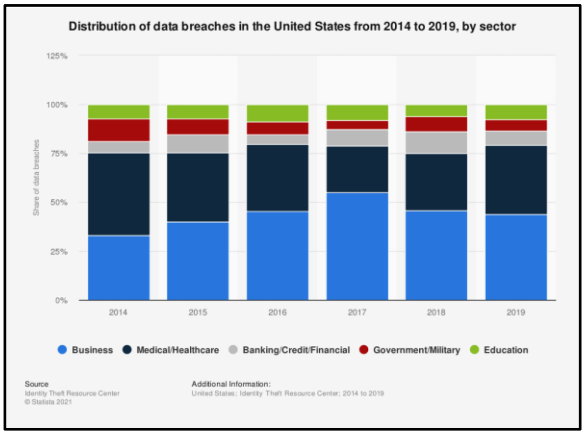
A study investigating students' use of social network sites concluded that "Students... expressed greater concerns about social privacy than institutional privacy". And continued that "they adopted privacy protection strategies that would allow them to better control who in the Facebook network would have access to their personal information, rather than strategies that would enable them to restrict third parties from using their information."[13] This shows that students will take measures to protect their social privacy, but are less concerned about protecting their personal information from corporations. One must conclude that users either implicitly trust corporate data handlers, do not know how to protect their information, or value using the internet over the risk of losing personal privacy.

To evaluate risk, individuals must first understand the importance of privacy and consequences of breaches. A paper investigating users' disclosure of information online explained that "a past medical condition, if disclosed, may preclude future medical insurance coverage or even employment that could lead to a negative impact on an individual's health and/or financial status."[14] Examples of the data revealed during breaches include social security numbers, credit card numbers, home addresses, and birth dates.[15] The loss of this data is irreversible and provides an opportunity for mass fraud to occur, costing both individuals and governments.[3]

3.0 COST OF INEFFECTIVE CYBERSECURITY

3.1 Prevalence of Data Breaches

As more people become comfortable divulging their personal information to online service providers, these same service providers become a more tempting target for cyber attacks. The potential to acquire a greater volume of user data entices criminals with larger profits, obtained by selling the data on the dark web.[16] According to Statista[17], the number of data breaches in the United States skyrocketed almost an order of magnitude between 2005 and 2020. The business and medical sectors are consistently targeted due to the nature of data (financial, personal medical history, etc…) that is collected.[18]


Distribution of data breaches in the United States from 2014 to 2019, by sector

Source
Identity Theft Resource Center
© Statista 2021

Additional Information:
United States; Identity Theft Resource Center; 2014 to 2019

Figure 3.1.1 – US data breaches by sector[18]

A handful of examples of data breaches include the iCloud accounts of countless celebrities, Equifax, one of the largest credit reporting agencies, and Cambridge Analytica.[19] Moreover, the cyber-attack which targeted Yahoo revealed "the issue of latency in discovering that an attack has occurred." The attack was only identified after two years, which raises concern regarding whether companies with fewer resources are even detecting data breach events.[20]

Furthermore, ransomware attacks successfully targeted the British health sector and the Danish A.P. Moller – Maersk Group.[21] An American journal indicated that "healthcare data breach statistics clearly show there has been an upward trend in data breaches over the past 10 years."[22] These examples of the exploitation of vulnerable data systems highlight that concerns encompass personal privacy and extend into the safety and operation of society.

3.2 2017 Equifax Data Breach

The credit bureau Equifax was breached in 2017, revealing private information of over a third of American citizens. Hackers collected full names, social security numbers, birth dates, addresses, and even driver's license numbers.[23]

Equifax was using the open-source software Apache Struts as a framework for its credit-dispute handling systems. On March 7th, a security vulnerability was discovered in the Apache Struts systems, and all users were encouraged to update immediately. Hacking groups were found searching for websites to exploit as early as March 10th.[23]

By May 12th, Equifax had yet to update their framework and hackers gained access to Equifax internal servers using the framework exploit. The hackers gathered internal credentials for Equifax employees, allowing them to access credit monitoring databases as though they were a fully authorized user. They gathered information for 76 days until Equifax discovered the breach on July 29th. The breach affected over 15 million British citizens, and almost 20 000 Canadian citizens.[23]

The failure to update the Apache Struts framework was critical for enabling the breach, but later analysis of the breach determined that Equifax's systems were inherently insecure, with inadequate encryption of Personally Identifying Information (PII), ineffective breach detection mechanisms, and insufficient segmentation.[23]

Disturbingly, Equifax did not publicly reveal any knowledge of the data breach until September of 2017 - 40 days after the exploit was initially discovered and locked down. It is unclear why Equifax waited so long before revealing the breach, but their actions would have been considered criminal under the GDPR act which came into effect only three months later. The GDPR stipulates that online service providers must release a data breach notification no later than 72 hours after a breach has been discovered, or risk stiff fines from data watchdogs.[24]

3.3 2018 AMCA Data Breach

American Medical Collection Agency (AMCA) is a US medical bill and debt collector which suffered a major data breach between August 2018 and March 2019. Information was stolen from corporate clients such as Quest Diagnostics and LabCorp which used AMCA's payment portal to bill the customers. At least 20 million US citizens have been impacted by this security incident in which sensitive personal information such as names, social security numbers, addresses, dates of birth, and payment card information were stolen and advertised for sale on deep web forums.[25]

The company first became aware of the data breach when a disproportionate number of credit cards processed in their system were linked with fraudulent transactions. Victims of the breach also claim there was an excessive delay in releasing information about the breach, Health Information Privacy (HIPPA) standards were disregarded throughout the incident, and the system itself employed inadequate security measures to protect PII. This data breach caused a severe drop in business for AMCA and ultimately led to its parent company, Retrieval-Masters Creditors Bureau Inc. to file for Chapter 11 bankruptcy protection.[25]

4.0 CYBERSECURITY LEGISLATION

4.1 Established Government Legislation

4.1.1 DPD. To regulate the processing and movement of data within the EU, the Data Protection Directive (DPD) was enacted by the European Union in 1995.[26] Prior to this, data privacy laws were region-dependent, creating an inefficient flow of data through a rapidly digitizing private sector. The DPD was one of the first attempts to create a cohesive set of regulations governing the collection, use, and transmission of personal data. It was composed in accordance with the seven Organisation for Economic Cooperation and Development (OECD) guidelines established in 1980[27]:

(i) Notice: Data collectors must notify users when collecting personal data.
(ii) Purpose: Personal data must only be used for it's express purpose of collection
(iii) Consent: Data collectors must garner consent from users before sharing personal data with third parties
(iv) Security: Data collectors should implement security measures to protect stored data from abuse or compromise
(v) Disclosure: Data collectors should notify users whenever personal data is collected
(vi) Access: Personal data should be accessible to users so they can correct inaccuracies
(vii) Accountability: Users should have a method to ensure data collectors adhere to aforementioned principles

4.1.2 PIPEDA. In 2000, Canada passed the Personal Information Protection and Electronic Documents Act (PIPEDA) to better align with EU privacy legislation.[28] PIPEDA established laws for data privacy within the private sector; it was meant to create consumer trust in e-commerce and demonstrate that Canadian privacy legislation was adequate to protect the personal information of EU citizens doing business in Canada. Seven provinces amended PIPEDA by adjusting its clauses, although regulators consider the resulting legislation to be "substantially similar" to PIPEDA. In British Columbia the legislation is called PIPA; it includes several notable provisions:

(i) Data controllers must obtain user consent prior to collecting personal data
(ii) Data controllers may only collect personal information for "reasonable purposes"
(iii) Specific policies and procedures are designated for managing breaches of privacy

4.1.3 GDPR. The European Commission submitted a draft proposal for an exhaustive reform of the DPD. It was an attempt to further compose regional data privacy laws into a cohesive piece of legislation demanding cross-border cooperation.[27] The General Data Protection Regulation (GDPR) was created by the European Parliament, Council, and Commission in 2015, and approved by European Parliament the following year. It superseded the DPD as national law for European states in 2018, giving individuals more control over their personal data.

4.1.4 CCPA. The California Consumer Privacy Act (CCPA) was proposed by the privacy group Californians for Consumer Privacy in December 2018, and it was passed by the state legislature on June 28, 2018.[29] CCPA empowers consumers with the right to know what information is being collected from them, and to whom said information is being disclosed. From here, consumers can also deny the sale of this information to third parties, and request to delete their personal information from the cloud. Even if their privacy right is exercised, equal service and price must be granted to the consumers.[30]

4.1.5 Unintended Consequences of Existing Legislation. The online environment is a new domain for regulators who are not necessarily aware of all the particular risks and vulnerabilities associated with software. To address this, legislation must be carefully reviewed by technical experts before implementation to ensure that it has the intended effect. For example, most websites now provide pop-up messages informing users of cookie usage and soliciting cookie preferences, in a direct attempt to maintain GDPR compliance. A better system should be established such as a "cookie preference" configuration file in the browser, allowing sites to automatically respond according to user cookie preferences. Moreover, there is a possibility that "GDPR compliance could paint companies in a better light than they really deserve, blinding unsuspecting consumers to instances where privacy and security measures are weaker."[31]

There have also been some positive unintended consequences of the GDPR regulation. Users located outside of Europe and California also stand to benefit from the GDPR and CCPA policies as it is cheaper for companies to provide a single webpage to all users rather than discriminate based on their location. Moreover, companies seek to maintain a good public image by providing privacy-enhanced services to all users. Large corporations such as Microsoft, Starbucks and Netflix already extend these CCPA rights to America.[32],[33]

4.2 Considerations for Future Legislation

Only 9 months after its induction on 25 May, 2018, European Commission officials had received over 95 000 privacy and data breach complaints from European citizens.[34] GDPR forced many organizations and online service providers to re-evaluate their data management systems to ensure compliance with the improved standards.[35] To address the historical prevalence of data breaches in the private sector, the GDPR requires that data controllers give notice of any data breaches "not later than 72 hours after having become aware of it."[24] Again, this encourages data controllers to refine their cybersecurity methods for the purpose of minimizing liability in the case of a data breach. The legislation has been fairly well received by the private sector; 92% of businesses surveyed agreed that compliance with GDPR legislation would be non-problematic.[37]

Much of the GDPR legislation is based around the concept of consent during collection of user data. Most critically, GDPR includes the concept that "Consent must be freely given."[38] Nevertheless, it does not directly address the complication of dark patterns. A dark pattern is a trick of misdirection[39] employed by websites and online service providers to deceive users into surrendering more data than they originally intended. A notable example is in the ubiquitous cookies pop-up, where the "Accept All" button is very easy to click, while the "Accept Only Necessary" button is often hidden behind several menu layers. Future regulations should include clauses to directly address dark patterns because it will promote integrity on behalf of online service providers, improving user experience across the web.

Data portability is the concept that individuals should be able to easily transfer their online personal data from one service provider to another. Unfortunately, the GDPR regulation fails to adequately address this issue. The EU's recently introduced "Right to Data Portability" essentially means that European citizens can choose to download a copy of their personal data, or transfer it to another online service provider. However, the GDPR fails to fully meet this right, and more legislation may be required to lower switching costs for end users.[40]

Unfortunately, not all corporations are in favour of data portability legislation; "Corporations frequently ignored or declined requests of individuals for information access or corporate information sharing practices."[40] Data portability rights will give users greater mobility between service providers, and assist users who are concerned about data security to transition to competing, more secure platforms. Consequently, regulators should establish rigorous data portability legislation to incentivise current leading corporations to improve their security, and data sharing practices to retain users.

Another insidious behaviour (primarily employed by social media companies) involves the collection of behavioural data.[31] Behavioural data is not currently subject to the same legal constraints as personal data under the GDPR, but behavioural data creates a "digital fingerprint" that can be used to identify unique individuals almost 99% of the time.[42] Behavioural data is most commonly collected by social media and online shopping websites, where demographics such as age, gender, and personal interests can be used for targeted advertising purposes. It is important to realize that "Just like any law, GDPR isn't watertight. Tech giants could very well find loopholes" – behavioural data is one such example.[31] Specific legislation to address the loophole of behavioral data and digital fingerprinting is required because it will "help keep tech giants in check, making it harder for them to abuse their users' personal information."[31]

5.0 SOCIAL AND MORAL RESPONSIBILITY OF ONLINE SERVICE PROVIDERS

5.1 Social Responsibility

With online services becoming increasingly prevalent in society, online service providers and data controllers are morally and socially obligated to ensure a safe and secure user experience. Individuals with limited understanding of the systems and potential risks (such as elderly or young children) should be informed and protected. Providers should implement default settings which maximize the privacy of users who may not be aware of available options. However, this reduces the data that companies are able to collect and interferes with their interest to "maximize and then leverage the value of consumer information."[44] Therefore, the obligation for ensuring protective measures are implemented falls onto the regulators, who ought to act according to public interest.

5.2 Design of Login Systems

Whenever possible, service providers should design their login systems to be compatible with modern security systems. Common examples are password managers and Time-Based One Time Password (TOTP) systems. If the login page is incompatible with a password manager (i.e. the password manager cannot auto-fill credentials), then users will be less likely to store their credentials for that specific site in a password manager; this compromises security because users may reuse passwords, or use weak passwords.

Users should always be given the option to employ up to three methods of two factor authentication (2FA) for their accounts. Email 2FA is the most basic and least secure method. SMS verification with a mobile telephone number is more secure, but has associated vulnerabilities (e.g. SIM spoofing). TOTP is one of the most secure methods, because verification codes are generated according to a pseudo-random algorithm. The device generating the verification code does not even need to be connected to the internet, making it impervious to direct cyber attacks.[45],[46]

5.3 Design of Passwords

A popular XKCD comic states that "through 20 years of effort we've successfully trained everyone to use passwords that are hard for humans to remember and easy for computers to guess". The comic is presented below for convenience; its main point is that many service providers require users to create passwords with certain characteristics (e.g. one number, one capital letter and one special character). Rather than improving security, this practice only encourages users to create short, lazy passwords (e.g. P@55word).

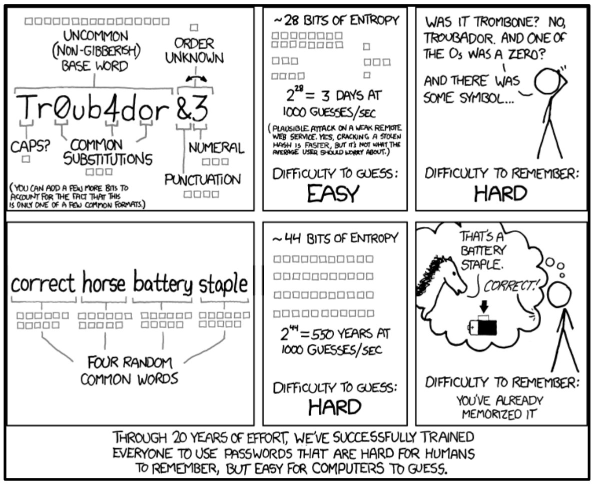

UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Figure 5.3.1 – Password Security[47]

The XKCD four english word format is much more secure than traditional password formats, and service providers should always program their systems to accept suitable XKCD style passwords.

Service providers should also routinely provide users with the ability to create an anti-phishing phrase. The anti-phishing phrase is a random word (or series of words) that the user can specify in their account settings. Any legitimate email correspondence from the service provider would include the anti-phishing phrase, while it would be absent from phishing attempts. This is a basic feature that allows users to quickly identify phishing attacks, rendering them ineffective.[48]

5.4 User Awareness

Although government legislation and corporations can work to keep users safe online, the end user still bears an amount of personal responsibility to support the systems keeping their data safe. Users must take some amount of initiative to inform and protect themselves from potential risks. For instance, users can back up their personal data to reduce impacts of ransomware attacks and take care when pressing on links or downloads in their email.[49] Users should always use unique passwords for their accounts (it is preferable to store login information in a password manager), enable two factor authentication, and never share their credentials.[50] However, these measures should be considered the last line of defence for users. Service providers must inform users of their responsibilities, and recommend users employ the most secure methods available.

6.0 CONCLUSION

The importance of privacy has been established by outlining society's dependence on technology and the consequences of data becoming available, including fraud and identity theft. The prevalence and continually increasing rates of data breaches highlight inadequate development of cybersecurity protocols and legislation; user data and personal privacy is not being respected. This is clearly shown in the investigation of two case studies, the Equifax breach of 2017 and the AMCA data breach of 2018. Consequently, action must be taken to prevent data breaches and protect user privacy in the future.

Although existing legislation such as the GDPR and CCPA was a step in the right direction towards creating comprehensive cybersecurity and data privacy regulations, there is still work to be done. Future legislation must be introduced to address specific areas of data privacy; these include data portability, regulations of dark patterns when garnering consent, and the collection of behavioural data.

Although companies have a social responsibility to provide adequate cybersecurity and data protection methods for end users, more legislation should be introduced to address specific protocols for login and authentication systems. Specifically, proper encryption methods must always be employed, login systems should be compatible with password manager systems, and multiple levels of two factor authentication should be offered. This would decrease incidences of account hijacking by encouraging users to employ proper security measures when creating/accessing accounts, rather than using weak passwords, or reusing passwords.[50]

Although there are certain steps individuals can take to protect themselves online, it is the duty of regulators to legislate cybersecurity and data privacy for online service providers and data controllers. Unfortunately, regulators will likely face opposition from the private sector (especially social media and online shopping retailers) who monetize user data to generate vast wealth. There may be fearsome opposition from large tech companies who can hire lobbyists to oppose data protection legislation (this precedent was set as the right to repair movement gained traction in the United States). Nevertheless, public awareness about the issue of personal privacy and cybersecurity is continuing to improve.[34] As individuals are educated to make better informed decisions, data controllers will be forced to integrate better security measures by the processes of the free market.

References

[1] U.S. Data Breaches and Exposed Records 2020. (n.d.). Statista. Retrieved 20 August 2021. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

[2] Samhan, B. (2020). Can cyber risk management insurance mitigate healthcare providers' intentions to resist electronic medical records? International Journal of Healthcare Management, 13(1), 12-21. https://doi.org/10.1080/20479700.2017.1412558

[3] Moore, T. (2017). On the harms arising from the Equifax data breach of 2017. International Journal of Critical Infrastructure Protection, 19, 47-48. https://doi.org/10.1016/j.ijcip.2017.10.004

[4] Wikipedia contributors. (2021, July 27). Digital Revolution. In Wikipedia, The Free Encyclopedia. Retrieved 11:38, August 18, 2021. https://en.wikipedia.org/w/index.php?title=Digital_Revolution&oldid=1035664087

[5] TIME Mobility Poll, in cooperation with. (2014, May 21). Qualcomm. https://www.qualcomm.com/documents/time-mobility-poll-cooperation-qualcomm

[6] View Account Information with eStatements. (n.d.). RBC Royal Bank. Retrieved August 18, 2021. https://www.rbcroyalbank.com/banking-services/estatements.html

[7] Canada Revenue Agency. (n.d.). Filing an income tax and benefit return on paper - Canada.ca. Government of Canada. Retrieved August 18, 2021. https://www.canada.ca/en/revenue-agency/campaigns/income-tax-benefit-return-paper.html

[8] Robbins-Tiscione, K. K. (2008). From snail mail to E-mail: The traditional legal memorandum in the twenty-first century. Journal of Legal Education, 58(1), 32-60

[9] Wikipedia contributors. (2021, June 20). Communications Act of 1934. In Wikipedia, The Free Encyclopedia. Retrieved 11:52, August 18, 2021. https://en.wikipedia.org/w/index.php?title=Communications_Act_of_1934&oldid=1029489162

[10] Wikipedia contributors. (2021, August 17). Software as a service. In Wikipedia, The Free Encyclopedia. Retrieved 11:53, August 18, 2021. https://en.wikipedia.org/w/index.php?title=Software_as_a_service&oldid=1039250238

[11] Du, J., Dean, D. J., Tan, Y., Gu, X., & Yu, T. (2014). Scalable distributed service integrity attestation for software-as-a-service clouds. IEEE Transactions on Parallel and Distributed Systems, 25(3), 730-739. https://doi.org/10.1109/TPDS.2013.62

[12] Spadafora, A. (2018, November 16). Users warned of Microsoft data harvesting. TechRadar. https://www.techradar.com/news/users-warned-of-microsoft-data-harvesting

[13] Alyson Leigh Young & Anabel Quan-Haase (2013) PRIVACY PROTECTION STRATEGIES ON FACEBOOK, Information, Communication & Society, 16:4, 479-500, DOI: 10.1080/1369118X.2013.777757

[14] Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. The Journal of Consumer Affairs, 41(1), 100-126. doi:http://dx.doi.org/10.1111/j.1745-6606.2006.00070.x

[15] Durnell, E., Okabe-Miyamoto, K., Howell, R. T., & Zizi, M. (2020). Online privacy breaches, offline consequences: Construction and validation of the concerns with the protection of informational privacy scale. International Journal of Human-Computer Interaction, 36(19), 1834-1848. https://doi.org/10.1080/10447318.2020.1794626

[16] Wilson, E. (2019). Disrupting dark web supply chains to protect precious data. Computer Fraud & Security, 2019(4), 6-9. https://doi.org/10.1016/S1361-3723(19)30039-9

[17] Statista. (2021, March 3). Cyber crime: number of breaches and records exposed 2005–2020. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

[18] Statista. (2021a, January 25). Cyber crime: distribution of breaches 2014–2019, by sector. https://www.statista.com/statistics/422115/distribution-of-data-breaches-usa-by-sector/

[19] Durnell, E., Okabe-Miyamoto, K., Howell, R. T., & Zizi, M. (2020). Online privacy breaches, offline consequences: Construction and validation of the concerns with the protection of informational privacy scale. International Journal of Human-Computer Interaction, 36(19), 1834-1848. https://doi.org/10.1080/10447318.2020.1794626

[20] Benyon, D. (2016). Yahoo blames breach on state-sponsored hackers - FREE. ReActions (London)

[21] Vaczi, D., & Szadeczky, T. (2019). A threat for the trains: Ransomware as a new risk. Interdisciplinary Description of Complex Systems, 17(1), 1-6. https://doi.org/10.7906/indecs.17.1.1

[22] Healthcare Data Breach Statistics. (2021, January 22). HIPAA Journal. https://www.hipaajournal.com/healthcare-data-breach-statistics/

[23] Wikipedia contributors. (2021, July 10). 2017 Equifax data breach. In Wikipedia, The Free Encyclopedia. Retrieved 12:11, August 18, 2021. https://en.wikipedia.org/w/index.php?title=2017_Equifax_data_breach&oldid=1032862758

[24] Lomas, N. (2017a, September 8). Equifax breach disclosure would have failed Europe’s tough new rules. Tech Crunsh. https://techcrunch.com/2017/09/08/equifax-breach-disclosure-would-have-failed-europes-tough-new-rules/

[25] Osborne, C. (2019, June 19). Data breach forces medical debt collector AMCA to file for bankruptcy protection. ZDNet. https://www.zdnet.com/article/medical-debt-collector-amca-files-for-bankruptcy-protection-after-data-breach/

[26] Wikipedia contributors. (2021, July 30). Data Protection Directive. In Wikipedia, The Free Encyclopedia. Retrieved 12:16, August 18, 2021. https://en.wikipedia.org/w/index.php?title=Data_Protection_Directive&oldid=1036252262

[27] Lord, N. (2018, September 12). What is the Data Protection Directive? The Predecessor to the GDPR. Digital Guardian. https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr

[28] Wikipedia contributors. (2021, May 26). Personal Information Protection and Electronic Documents Act. In Wikipedia, The Free Encyclopedia. Retrieved 12:21, August 18, 2021.
https://en.wikipedia.org/w/index.php?title=Personal_Information_Protection_and_Electronic_Documents_Act&oldid=1025318705

[29] Wikipedia contributors. (2021, August 18). California Consumer Privacy Act. In Wikipedia, The Free Encyclopedia. Retrieved 12:23, August 18, 2021. https://en.wikipedia.org/w/index.php?title=California_Consumer_Privacy_Act&oldid=1039313091

[30] Morrison, S. (2019, December 31). CCPA, California's new privacy law, explained. Vox. https://www.vox.com/recode/2019/12/30/21030754/ccpa-2020-california-privacy-law-rights-explained

[31] Shamir, S. (2018, August 13). The GDPR Aftermath: What Else Can be Done to Improve Data Security. Infosecurity Magazine. https://www.infosecurity-magazine.com/opinions/gdpr-aftermath-improve-data/

[32] Fowler, G. A. (2020, February 19). Perspective | Don't sell my data! We finally have a law for that. Washington Post. https://www.washingtonpost.com/technology/2020/02/06/ccpa-faq/

[33] Barrett, C. (2019). Rre the EU GDPR and the California CCPA Becoming the De Facto Global Standards for Data Privacy and Protection?. American Bar Association.

[34] Weber, R. (2019). EU officials say voluminous data-breach complaints reflect GDPR's effectiveness. Inside Cybersecurity,

[35] Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. Journal of Global Information Technology Management : JGITM, 22(1), 1-6. https://doi.org/10.1080/1097198X.2019.1569186

[37] A new year for privacy GDPR six months on. (n.d.). Deloitte. Retrieved August 18, 2021. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf

[38] Wolford, B. (2019, February 13). What are the GDPR consent requirements? gdpr.eu https://gdpr.eu/gdpr-consent-requirements/

[39] Dark Patterns. (n.d.). Dark Patterns. Retrieved August 18, 2021.
https://www.darkpatterns.org/

[40] Syrmoudis, E., Mager, S., Kuebler-Wachendorff, S., Pizzinini, P., Grossklags, J., & Kranz, J. (2021). Data Portability between Online Services: An Empirical Analysis on the Effectiveness of GDPR Art. 20. Proceedings on Privacy Enhancing Technologies, 2021(3), 351–372. https://doi.org/10.2478/popets-2021-0051

[42] Kessler, D. (2021, February 3). This is Your Digital Fingerprint. The Mozilla Blog. https://blog.mozilla.org/en/privacy-security/this-is-your-digital-fingerprint/

[44] NORBERG, P. A., HORNE, D. R., & HORNE, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. The Journal of Consumer Affairs, 41(1), 100-126.
https://doi.org/10.1111/j.1745-6606.2006.00070.x

[45] Wikipedia contributors. (2021, August 14). Multi-factor authentication. In Wikipedia, The Free Encyclopedia. Retrieved 13:53, August 18, 2021. https://en.wikipedia.org/w/index.php?title=Multi-factor_authentication&oldid=1038735365

[46] Drozhzhin, A. (2019, November 15). SMS-based two-factor authentication is not safe — consider these alternative 2FA methods instead. Kaspersky. https://www.kaspersky.com/blog/2fa-practical-guide/24219/

[47] A. (n.d.). Password Strength. Xkcd. Retrieved August 18, 2021.
https://xkcd.com/936/

[48] Rahman, Sheikh Shah Mohammad Motiur, Gope, L., Islam, T., & Alazab, M. (2020). IntAnti-phish: An intelligent anti-phishing framework using backpropagation neural network. (pp. 217-230). Springer International Publishing. https://doi.org/10.1007/978-3-030-57024-8_9

[49] Szücs, V., Arányi, G., & Dávid, Á. (2021). Introduction of the ARDS—Anti-ransomware defense system Model—Based on the systematic review of worldwide ransomware attacks. Applied Sciences, 11(13), 6070. https://doi.org/10.3390/app11136070

[50] Gasti, P., & Rasmussen, K. B.On the security of password manager database formats. (pp. 770-787). Springer Berlin Heidelberg.
https://doi.org/10.1007/978-3-642-33167-1_44

[51] Alodhyani, F., Theodorakopoulos, G., & Reinecke, P. (2020). Password managers--it's all about trust and transparency. Future Internet, 12(11), 1.
https://doi.org/10.3390/fi12110189

Revision Notice

This paper originally published 2021-08-19
Revision 1 to redact personal information 2024-08-07