Chapter 5
An Overview of Recent Development in Privacy Regulations and Future Research Opportunities

Tawei Wang
DePaul University, USA

Yen-Yao Wang
Auburn University, USA

ABSTRACT

This chapter provides an overview of several recently proposed or passed privacy-related regulations, including General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Illinois Video Interview Act, Data Broker Regulations in Vermont, and Privacy Bill of Rights Act, and related but very limited studies. Toward the end, several research opportunities are discussed. These research opportunities include (1) economic consequences of these new regulations and (2) the new research framework to capture novel features of these regulations to explain security compliance. The authors further discuss possible research designs to address the proposed research opportunities. This chapter provides both professionals and researchers additional insights on the regulation of privacy issues.

INTRODUCTION

With the advance in information technology, companies are capable of collecting much more information with a faster and cheaper manner. These pieces of information ranges from basic personal information to behavioral information such as social media activities and preferences or the way we talk and walk. Though such information helps companies better understand their customers and potentially provide more customized services, it does raise concerns about the collection, the use and share of personal information. For example, the Facebook scandal shows that about 87 million users' information has

DOI: 10.4018/978-1-7998-5728-0.ch005

been inappropriately shared with Cambridge Analytica (Newcomb, 2018), which resulted in a $5 billion fine by Federal Trade Commission (Snider & Baig, 2019) and the change of Facebook's privacy policies (Corcoran, 2018). Not just Facebook, Google is also facing privacy challenges, including censored search engine service in China (Tiku, 2018), exposed user information (MacMillan & McMillan, 2018) and Nest spycam problem (Winder, 2019).

In addition to the collection and use/share of personal information, several recent high-profile cybersecurity breaches, such as Equifax and Marriott, all involve the loss of personal information. For example, the Marriott breach involves about 5 million users' information (Fruhlinger, 2020) while Equifax lost personal information of about 150 million individuals due to an unpatched software (Andriotis, Rapoport & McMillan, 2017). These data breaches have further attracted the public's and regulators' attention regarding the protection of privacy.

In this book chapter, we will provide an overview of several recent development of privacy regulations. These regulations are: General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Illinois Video Interview Act, Data Broker Regulations in Vermont, and Privacy Bill of Rights Act. We select these five regulations because of the following reasons. First, these five regulations demonstrate a change in privacy concerns. That is, the privacy concern is not just about collecting personal information but also about the share, the use and the deletion of information. These five regulations also cover a wide variety of issues from personally identifiable information, behavioral information to data broker issues. Last, these five regulations range from a State-wide legislation (e.g., Illinois Video Interview Act) to a regional privacy act with a global impact (e.g., GDPR).

Existing research centered around this new development in privacy regulation is very limited with only a few exceptions. Accordingly, in this study, we highlight major areas that researchers can contribute to the understanding of privacy issues and provide policy implications for regulators. These research directions are: (1) economic consequences of these new regulations and (2) new research framework to capture novel features of these regulations to better explain security compliance. In addition to these research directions, we also discuss several research designs for scholars to consider in order to leverage this new stream of research opportunities.

In the following book chapter, we will first provide an overview of these five different regulations and discussed related available studies in the business field in Section 2. Following that, five future research directions are highlighted in Section 3. We conclude in Section 4.

OVERVIEW OF RECENT DEVELOPMENT IN PRIVACY REGULATIONS AND RELATED STUDIES

General Data Protection Regulation (GDPR)

As the data privacy protection issues have become serious in recent year, the General Data Protection Regulation (GDPR) was passed in 2017 and implemented in the European Union (EU) in May 2018. The implementation of the GDPR is expected to deal with concerns and challenges related to the collection of customer information. It has the following general data protection principles: (1) fairness and lawfulness: personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. (2) purpose limitation: personal data needs to be collected for specified, explicit and legitimate purposes (i.e., purpose limitation). (3) data minimization: data minimization is designed to ensure that organizations do not overreach with the type of data they collect about people. (4) storage limitation: storage limitation is designed to keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purpose for which personal data are processed. (5) accuracy, integrity and confidentiality: personal data should be accurate and, where necessary, kept up to date (i.e., accuracy). Integrity and confidentiality (security) states that personal data should be processed in a manner that ensures appropriate security of personal data. (6) accountability: accountability is designed to ensure that companies can prove they are working to comply with the other principles that form GDPR (European Commission, 2019; Goddard, 2017).

The GDPR has 99 articles and includes many different aspects (European Commission, 2019). The extensive aspects of the GDPR has made it receive praise as "a game changer" (Goodman, 2018) and criticism as both a "property regime" (Victor, 2013) and a stifling force for innovation and technological development (Zarsky, 2016). Here we will only discuss several major features in GDPR.

It is worth noting that though it focuses on organizational practices for collecting and handling European Union residents' information, it does not limit to a company's physical present in Europe (i.e., the extraterritoriality requirement). Accordingly, before the GDPR went in effective in May 2018, many US companies were also busy preparing for compliance as in today's global business operations, it is likely to gather or process information from European Union residents. The GDPR also requires companies that process a lot of sensitive personal information to have a data protection officer (DPO). Data protection officers are responsible for training employees, perform regular assessments, and being the communication channel between the company and the data subjects. More importantly, the GDPR allows users to request to access the data collected by companies and can request her/his data to be deleted (i.e., the right to be forgotten). The non-compliance penalty can up to €20 million or 4 percent of a company's global turnover (whichever is greater). For instance, Google was fined 50 million Euros by the French data regulator due to the lack of transparency (Fox, 2019).

Since the implementation of the GDPR, we have noticed some but very limited studies discussing the impact of the GDPR in various settings. In addition, although the GDPR claims to cover 'a right to explanation' of all decisions made by automated or artificially intelligence algorithmic systems, some scholars still debate on this issue due to the lack of precise language and well-defined rights, thereby running the risk of being not too meaningful. For example, Wachter, Mittelstadt, and Floridi (2017), one example of arguing the lack of well-defined rights in the GDPR, explicitly discuss the meaning of a right to explanation and point out that a meaningful right to explanation is not legally mandated by GDPR.

Most of existing studies tend to focus on the viewpoint with respect to the impact of the GDPR instead of empirically examining its impact with few exceptions. Goddard (2017) discusses data protection principles of the GDPR and the potentially global impact of the GDPR. To implement these principles, researcher require proactive design and conceptualization of privacy as the default for any data collection exercise. He further emphasizes the importance of embedding these principles in the design system of IT architecture to operate these principles. Rumbold and Pierscionek (2017) explain the changes in data protection laws that apply to medical research and discuss how the GDPR may affect medical research. Particularly, they pay more attention on consent requirements based on the GDPR that would severely restrict medial data research. Their discussion concludes that the proposed changes due to the GDPR will make little impact on biomedical data research. As another attempt examining the potential impact of the GDPR on scientific research, Chassang (2017) provides an overview of the GDPR and discusses how the GDPR would change practices on processing personal health data, genetic data or other kinds of sensitive information. The study concludes with key facts to scientific researchers to adapt their practices and to ensure to GDPR compliance. In addition, Wachter (2018) discusses the inherit tension between privacy and identifiability in the setting of the Internet of Things (IoT) and examines how the GDPR will provide meaningful protection for privacy and control over identity for users of IoT.

In addition to the above-mentioned studies, many other studies also focus specifically on the GDPR implications from the healthcare perspective. For example, Marelli, Livevrouw, and Van Hoyweghen (2020) discuss the tension emerging between the current GDPR-based data governance regime and the broader societal shifts coming along with the expansion of digital health. Their discussion leads into doubt whether the GDPR is a fit for the purpose of governing current development in healthcare, while also calling for swift and adequate policy responses. Finally, Marovic and Curcin (2020) explore the impact of the GDPR on health data management in Serbia. Their findings suggest that given the current limitation and potential issues with the legislation, it still remains to be seen whether the move toward the GDPR will be beneficial for the Serbian health system. Therefore, a strategic approach is needed at the national level to address insufficient resources to develop the personal data protection environment further.

Two recent studies emphasize on consumers' responses to GDPR. Aridor et al. (2020) study the economic consequences of data privacy regulation, which is one of the few exceptions empirically examining the effect of the GDPR. They find a 12.5% drop in the intermediary observed consumers as a result of the GDPR, suggesting a non-negligible number of consumers exercised the opt-out right enabled by the GDPR. Zhang, Wang and Hsu (2020), from a different viewpoint, investigate the relationship between voluntary adoption of GDPR and readability of privacy statement on consumers' intention to disclose information. The adoption of GDPR is a major factor that affects consumers' intention to disclose information and trust towards the company. The study demonstrates the potential benefits that can be brought by the adoption of GDPR.

Although the GDPR attempts to benefit companies by providing a guidance for data protection activities, it also posts new challenges on the existing operation practices. We observe a handful of research with respect to this topic. For example, Tikkinen-Piri, Rohunen and Markkula (2018) focus on the GDPR implications on firms' operation practices. They further present 12 aspects of implications such as business strategies, organizational, and technical measures and offer the corresponding guidance on how to better prepare companies for the new GDPR requirements.

California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) is the new consumer privacy rights regulation in California which was in effect on January 1, 2020 (State of California Department of Justice, 2020). CCPA has a similar spirit compared to the GDPR. It is perhaps the most influential state-level privacy law in the U.S. and is the first of its kind to provide significant privacy rights to consumers (Stallings, 2020). It is about the access, the deletion and sharing of individual's information that is collected by companies. In other words, it gives consumers a great deal of control over their personal information. This law applies to any business in the State of California that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information (State of California Department of Justice, 2020). Companies operate in California with the following conditions are under the regulation of the CCPA: (1) has gross annual revenues more than $25 million; (2) buys, receives, or sells personal information of 50,000 or more consumers, households, or devices; (3) derives 50 percent or more of annual revenues from selling consumers' personal information (State of California Department of Justice, 2020). One of the key characteristics of the CCPA is its extremely broad and comprehensive definition of personal information (PI). Under the CCPA, PI is anything that is capable of being associated, or could reasonably be directly or indirectly linked with a particular consumer or household. Therefore, PI could include identifiers such as a name, alias, postal address, unique personal identifier, email address, account name, social security name, driver's license number, or passport number. The CCPA also allows California customers to request to see the information a company has about them (i.e., the right to know). Regarding the categories that companies need to disclose to California residents, companies must disclose the sources from which that PI is collected, the purpose for collecting or selling PI, the categories of PI sold, and the categories of third parties with whom PI is shared. In addition, companies must allow customer to choose whether or not to share their information with third parties (i.e., the right to opt-out). Customers also have the right to request to delete their information collected by the companies (i.e., the right to delete) and not to be discriminated by the data (i.e., the right to non-discrimination). Finally, compared to the GDPR that fines up to €20 million or 4 percent of a company's global turnover, the CCPA does not impose monumental fines. It only permits consumers to recover the greater of up to $750 per violation or their actual damages. When a business has intentionally violated the law, the attorney general can also recover a civil penalty of up to $7,500 per violation.

Given the fact that the CCPA was effective in 2020, most of studies from different fields such as law, accounting, or information technology tend to discuss what the CCPA is and how it may affect the corresponding field. A number of studies also examine the similarities and the differences between the GDPR and the CCPA. For example, Myers, Lively, & Andrews (2019) compare the CCPA and the GDPR and offer the recommendations for public accountants and consultants in response to these new laws. Thomas (2020) compares some of the ways that the CCPA is similar to and different from the GDPR and discuss how this affects the way that businesses should prepare.

Similar to the trend of the GDPR, we notice very limited studies from different fields empirically examining the impact of the CCPA. For example, Stallings (2020) discusses how IT practitioners may deal with obfuscation algorithms that can protect privacy, including deidentification, aggregation, and pseudonymization. The author further considers whether those technical protections are sufficiently well defined in the CCPA and whether they are likely to be effective in practice. Finally, motivated by the implementation of privacy regulations (e.g., the GDPR and the CCPA), Winegar and Sunstein (2019) examine how consumers value data privacy by conducting a survey. They find that the median consumer is willing to pay just $5 per month to maintain data privacy but would demand $80 to allow access to personal data. They conclude that because of a lack of information and behavioral biases both willingness to pay and willingness to accept measures are highly unreliable guides to the welfare effects of retaining or giving up data privacy. Although their study represents one empirical setting with respect to consumer privacy, their study still does not the examine the impact of the CCPA or the GDPR in essence.

Illinois Video Interview Act

The big hotel chain, Hilton, used an artificial intelligence (AI) software, HireVue, for its hiring initiatives (Halzack, 2014). The software may help a company reach more candidates and allow potential candidates to be seen as the company now has the capability to process more candidates initially. When the company uses the software, it is possible that the assessment results are more consistent and independent from the interviewers' opinions. However, it at the same time raises privacy concerns about the collection of behavioral information (i.e., how a candidate talks, how a candidate explains things, and facial expressions as well as body languages) and the use or share such information for different purposes.

The Illinois Video Interview Act or AI Video Interview Act (Illinois General Assembly, 2020) aims to address this emerging issue and was enacted in January 1, 2020. It is the first U.S. law that specifically regulates artificial intelligence as an evaluation tool on applicant videos. This legislation has the following several key features. First, companies who plan to use AI for interview purposes must explain how the tools work and how they are used for evaluations. Second, companies need to have applicants' consent in order to use artificial intelligence to assess the applicants' interview videos. Third, employers will be permitted to share the videos only with persons whose expertise or technology is necessary to evaluate an applicant's fitness for a position. Finally, employers must destroy both the video and all copies within 30 days after an applicant requests such destruction. Although this law attempts to protect job candidates' right during the interview process, some of its requirements are quite vague. For example, this law does not define AI, nor does it provide specific guidance about what the employer's explanation of AI used in connection with video interviews should contain. Moreover, although this law provides the right for candidates to decline to have the video interview, it does not require employers to provide an alternative. Therefore, a lot of the responsibility is being put on the candidate, leading job applicants feel obligated to do the video to avoid losing out an employment opportunity. Finally, compared to the GDPR and the CCPA, this law is also silent on enforcement, remedies, and penalties for violations.

Despite of the potential benefits and issues brought by using AI to perform interviews, we notice very few studies examining the effect of AI for facilitating the recruiting process. For example, Suen, Chen, & Lu (2019) explore the social impacts of synchronous video interviews, asynchronous video interviews, and asynchronous video interviews with the AI aid. Interestingly, they find that applicants did not perceive differences in procedural fairness between the interviews with and without the AI aid. However, no studies have attempted to address related issues under the framework of the Illinois AI video interview act.

Data Broker Regulations in Vermont

With the advance in information technology, we have seen a new business model as a data broker. A data broker[1] collects information and sells useful information about customers to companies. For example, in a Forbes article in 2018, it states that "Facebook's Partner Categories program, in which as far back as 2013 it began licensing information from companies like Acxiom, Epsilon and Oracle Data Cloud to allow precision advertising targeting of its users based on the activities they perform offline or online outside of its walled garden" (Leetaru, 2018). Specifically, a wide range of personal information may not be collected directly through the companies that customers have relationships with. Instead, companies may obtain information regarding its customers through data brokers, which is the focus of this legislation.

The Data Broker Regulation (Vermont Office of the Attorney General, 2018) in Vermont effective in January 1, 2019 specifically regulate data brokers in the following ways. First, this law defines data brokers as a business or business unit that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship. This law further defines brokered personal information as one or more of a list of computerized data elements about a consumer if categorized or organized for dissemination to third parties, as well as other information that allows a reasonable person to identify the consumer with reasonable certainty. The definition of brokered personal information in this law leads to some vague area, especially for internal use of data. For example, given the fact that brokered personal information must be categorized or organized for dissemination, the business must have done something to the data to prepare it for dissemination to be implicated under the law. Therefore, data that is stored in a business's internal database for internal use with no intention for dissemination outside the business does not consider as brokered personal information, leading to some vague area to be regulated by the law. Under this regulation, data brokers are required to register through the Vermont Secretary of State annually. Data brokers are also required to maintain security standards. This law lists the detailed data security as the followings. For example, data brokers need to have a comprehensive security program, perform risk assessment, train employees to compliance with policies and procedures, implement measures that prevent terminated employees from accessing personally identifiable information, and review the scope of security measures at least annually. Finally, the legislation explicitly state that it is illegal to obtain an individual's information through fraudulent activities and for the purpose of, for example, fraud or discrimination. Though this regulation has attracted a lot of attention, no business-related studies have emphasized on this issue.

Privacy Bill of Rights Act

In the US, privacy notification laws or related privacy legislations are at the state level. Senator Edward J. Markey in 2019 proposes a new regulation entitled "Privacy Bill of Rights Act" that is the first privacy regulation in the US at the federal level (Congress, 2020). The bill considers several aspects in GDPR and CCPA, such as data portability, deletion and access to the collected personal information. The bill defines personal broadly to include biometric information (but not those collected by a covered entity about an individual without the individual's knowledge), pass code, and individual preferences or characteristics. It also attempts to maintain a centralized database that lists all data brokers in the United States.

This bill has several main components. First, it requires companies to protect the personal information they have. Second, companies can only collect the information needed to provide the service with easy to read short privacy notices and are not allowed to use collected personal information for discrimination. Third, it proposes of using a centralized Federal Trade Commission website to provide information to customers about their privacy rights. Last, the proposed bill will enable State Attorneys General to bring actions against companies that violate the privacy rights. Given that this is still at the proposal stage, changes may also be made in later stages, no studies have attempted to address related issues in this context.

FUTURE RESEARCH OPPORTUNITIES

Our literature review suggests that the current discussions on policies above are still relatively few with most of exceptions on the viewpoint of the general impact. In this section, we offer few research opportunities for this particular research stream.

Economic Consequences

We observe that most of current studies focus on discussing what these regulations are and what potential impacts these regulations may create in the corresponding field such as law, information technology (IT), or accounting. However, our understanding regarding the economic consequences is still very limited.

Empirically, after the adoption of the new regulation, it will provide a good setting to conduct the natural experiment by treating the adoption of new regulation as exogenous variation (i.e., the shock), followed the difference-in-differences approach to show the effect. We, therefore, call for more studies on the economic effects of these new regulations and suggest that a natural experiment could be one of the appropriate research designs for this matter.

For instance, as discussed earlier, Aridor et al. (2020) represents one of few examples empirically examining the economic consequences of the GDPR in the online travel industry. They show that after adopting the GDPR privacy-conscious consumers substitute away from less efficient privacy protection to explicit opt out. However, the average value of the remaining consumers to advertisers has increased, offsetting most of the losses from consumers that opt-out. Therefore, their study shows great implications for practitioners to consider the costs and benefits of adopting a new policy such as the GDPR.

Specifically, we highlight several possible research questions from both the company's and the consumers' perspectives in the context of the above-mentioned new regulations.

First, in the context of GDPR and CCPA, what is GDPR or CCPA ready? It is still not clear how GDPR and CCPA may fundamentally change how organizations deal with privacy or how these new regulations may change how companies collect user information. The GDPR states that the non-compliance penalty can up to €20 million or 4 percent of a company's global turnover. This high amount of the non-compliance penalty, on the one hand, may give the companies incentives to revisit their current policies and operations to avoid the penalty. On the other hand, for compliance purpose, there are extra efforts or resources that need to be devoted to the change in business processes, IT infrastructure or data arrangement. Recently, we have already observed that users are allowed to change cookie settings when visiting specific websites. Nevertheless, some website simply asks the viewers to select "I accept" without any additional options, which basically forces users to accept the proposed privacy policy set by the company if a user chooses to continue with the service/purchase. However, this is not aligned with the spirit of the regulations and does not affect the underlying processes. The change in business processes include a new position of a Data Privacy Officer (DPO) and may change the responsibility reporting chain of privacy challenges or the strategic initiatives. A more detailed understanding about each company's organizational structure can help users and companies understand the impact of privacy awareness or trust, for instance, when a company recognizes or bring privacy to the strategic level. Last, given the high compliance costs, it is also unclear how these regulations may affect the companies' willingness for further innovation in the context of big data and artificial intelligence or it may change the direction of the companies' innovation strategies when utilizing personal information for new business models or services. This will bring an interesting phenomenon by examining the costs and benefits of these regulations for the companies.

For the AI interview act, as discussed, the current form of this law does not explicitly define AI or provide specific guidance about what the employer's explanation of AI used in connection with video interviews should contain. Therefore, it may create more challenges for firms to evaluate the potential impact of the AI interview act. Second, given that it is a learning process to understand job candidates' behavioral patterns, the results may be potentially biased due to the training dataset. Though the false positive cases may be detected through subsequent interviews, the company may lose false negative cases. In the extreme case, when the bias may be related to cultural or racial issues, the company may need to face more challenges. Accordingly, more investigation will help organizations better evaluate the costs and benefits of using AI for job interviews.

The Data Broker Act provides consumers, regulators and researchers more information about the "hidden players" in this domain. Currently, there are more than 100 data brokers that have registered based on Vermont's new rule. It is a great opportunity for researchers to understand these data brokers and how they provide services to other organizations. Their business models and performance are also valuable for researchers to provide policy implications to regulators. In addition, does the disclosed list of these data brokers change any data acquisition activities or affect the privacy protection behavior? Or how does the disclosed list affect the relationships among these brokers and business partners? More understanding can further form potential future policies for regulators. In the future, if we can have a privacy regulation at the federal level, it would be interesting to see how regulations at different levels interact and affect the compliance practices about data brokers, for instance, or whether it provides a new level of protections by affect companies', brokers' or users' behaviors.

In addition to address the issues from the company's perspective, it is also valuable to investigate the issue from the consumers' viewpoints. For instance, GDPR and CCPA have enforced companies to change their users privacy setting and agreements with users. It becomes important to understand whether these policy changes can have expected outcome. One recently observed change is that some companies have started to allow users to customize privacy options on their websites. It will be interesting to investigate how it may affect users' willingness to subscribe to the services or to purchase the products and how it may help companies build trust.

For the AI Interview Act, from the users' perspective, AI interviews may broaden the opportunities of job candidates though with all these privacy concerns. It remains an open question regarding the reactions of job candidates on this potential change. Experiments can be performed to understand how users reacts to AI interviews. More specifically, how people may perform differently with a human interviewer compared to video interviews. A multi-cultural or multi-regional study can help organizations, users and regulators to further understand the limitations and potential issues along with the benefits brought by AI interviews.

New Explanations of Security Compliance

The current research on information systems security behavioral has produced different models to explain security policy compliance such as the theory of reasoned action (i.e., explain the relationship between attitudes and behaviors of human actions) (e.g., Bulgurcu et al., 2010; Siponen et al., 2014), protection motivation theory (i.e., how people protect themselves based on the threats and preventive behavior) (e.g., Herath & Rao, 2009), or deterrence theory and rational choice theory (i.e., people determine whether to follow the rules depending on the assessments of gains and consequences) (e.g., D'Arcy et al., 2009).

With the hope to integrate the existing theories to explain security policy compliance, Moody et al. (2018) further propose the unified model of information security policy compliance (UMISPC) to explain the variation across different models. Some specific constructs such as response efficacy, threat, and habit are included in their model.

Our review regarding the new five regulations above indicates some novel features. For example, the GDPR and CCPA could be considered as one of the examples to guide privacy issues from the consumer perspectives. Illinois Video Interview Act also represents one of the laws in the state level to regulate any potentially unethical issues resulted from the application of AI during the interview process. Finally, Data Broker Regulations in Vermont is one of the existing laws that regulate this emerging industry. Although prior research has established sufficient knowledge in this subject, we may still have limited understanding about whether existing constructs could apply to the new regulations Therefore, we call for more studies to examine the antecedents of security regulation compliance while considering the novel features of these new regulations. For example, one feature of the GDPR is the extraterritoriality requirement. Namely, while regulating the company's practices for collecting and handling European Union residents' information, it does not limit to a company's physical present in Europe. Thus, while discussing security regulation compliance, it will bring the interesting discussion about the cross-culture issue especially for those big international companies. It also provides the further support on our argument that the existing research model, though useful, may not be enough to cover the novel features of the newly policies. In addition, for CCPA, it is also important to understand how customer chooses to provide information and to opt out for selling personal information. The AI Interview Act in Illinois provides an interesting context to understand the potential bias of using AI in the context of human resources. Last, the Data Broker Regulations is the first attempt to reveal these major data players. The compliance of the regulation and how more detailed information of these players may be connected to business practices will provide further insights to researchers and professionals.

CONCLUSION AND FUTURE READINGS

This book chapter provides an overview of five recent privacy regulations, including General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Illinois Video Interview Act, Data Broker Regulations in Vermont, and Privacy Bill of Rights Act. For more detailed information about GDPR, readers can go to https://gdpr.eu/, https://gdpr-info.eu/, or https://ec.europa.eu/info/law/law-topic/data-protection_en for further readings. For CCPA, readers can go to State of California Department of Justice's website (https://oag.ca.gov/privacy/ccpa) in order to search for activities and the regulations. The information about The Illinois Video Interview Act can be found through Illinois General Assembly (https://www.ilga.gov/legislation/BillStatus.asp?DocNum=2557&GAID=15&DocTypeID=HB&SessionID=108&GA=101). There is also interesting floor discussion about the bill that can provide more perspectives to the researchers. Last, for the Data Broker Regulations in Vermont, the attorney general office has provided some guidance that can be found at https://ago.vermont.gov/blog/2018/12/13/attorney-generals-office-issues-guidance-on-data-broker-regulations/ or more information can be obtained from the Vermont General Assembly (https://legislature.vermont.gov/). With a review of existing literature related to these regulations, we noticed that the unique features of these new regulations have not be discussed in academic literature though they may provide additional insights to theories, professionals and regulators. Based on the review of the regulations and recent literature, we highlight two broad possible future research directions: economic consequences and new explanations to security compliance. The former emphasizes on possible economic consequences for the companies and/or customers while the latter focuses on the potential advance in theories. Some possible research designs are also discussed so scholars can further contribute to this particular research stream.

REFERENCES

Andriotis, A., Rapoport, M., & McMillan, R. (2017). *'We've Been Breached': Inside the Equifax hack*. Retrieved from https://www.wsj.com/articles/weve-been-breached-inside-the-equifax-hack-1505693318

Aridor, G., Che, Y.-K., Nelson, W., & Salz, T. (2020). *The economic consequences of data privacy regulation: Empirical evidence from GDPR*. Working paper.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *Management Information Systems Quarterly*, *34*(3), 523–548. doi:10.2307/25750690

Congress—OLL19313. (2020). *Privacy Bill of Rights Act*. Retrieved from https://www.markey.senate.gov/imo/media/doc/Privacy%20Bill%20of%20Rights%20Act.pdf

Corcoran, K. (2018). *Facebook is overhauling its privacy settings in response to the Cambridge Analytica scandal*. Retrieved from https://www.businessinsider.com/facebook-overhauls-privacy-settings-after-cambridge-analytica-scandal-2018-3

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. doi:10.1287/isre.1070.0160

European Commission. (2019). *Data protection: Rules for the protection of personal data inside and outside the EU*. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection_en

Fox, C. (2019). *Google hit with £44m GDPR fine over ads*. Retrieved from https://www.bbc.com/news/technology-46944696

Fruhlinger, J. (2020). *Marriott data breach FAQ: How did it happen and what was the impact?* Retrieved from https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, *59*(6), 703–705. doi:10.2501/IJMR-2017-050

Goodman, S. (2018). *A game changer in the personal data protection in the EU*. Retrieved from https://www.msuilr.org/msuilr-legalforum-blogs/2018/2/19/a-game-changer-in-the-personal-data-protection-in-the-eu

Halzack, S. (2014). *At Hilton Worldwide, job interviews are going digital*. Retrieved from https://www.washingtonpost.com/business/capitalbusiness/at-hilton-worldwide-job-interviews-are-going-digital/2014/01/31/c3e96308-8775-11e3-916e-e01534b1e132_story.html

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. doi:10.1057/ejis.2009.6

Illinois General Assembly. (2020). *Bill status of HB2557*. Retrieved from https://www.ilga.gov/legislation/BillStatus.asp?DocNum=2557&GAID=15&DocTypeID=HB&SessionID=108&GA=101

Leetaru, K. (2018). *The data brokers so powerful even Facebook bought their data - but they got me wildly wrong*. Retrieved from https://www.forbes.com/sites/kalevleetaru/2018/04/05/the-data-brokers-so-powerful-even-facebook-bought-their-data-but-they-got-me-wildly-wrong/#2c1dd7193107

MacMillan, D., & McMillan, R. (2018). *Google exposed user data, feared repercussions of disclosing to public*. Retrieved from https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194

Marelli, L., Lievevrouw, E., & Van Hoyweghen, I. (2020). Fit for purpose? The GDPR and the governance of European digital health. *Policy Studies*, 1–21. doi:10.1080/01442872.2020.1724929

Marovic, B., & Curcin, V. (2020). Impact of the European General Data Protection Regulation (GDPR) on Health Data Management in a European Union Candidate Country: A Case Study of Serbia. *JMIR Medical Informatics*, *8*(4), e14604. doi:10.2196/14604 PMID:32301736

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *Management Information Systems Quarterly*, *42*(1), 285–311. doi:10.25300/MISQ/2018/13853

Myers, K., Lively, H., & Andrews, C. (2019). New laws bring much tougher data protections. *Journal of Accountancy*, *36*(39), 42–43.

Newcomb, A. (2018). *Facebook data harvesting scandal widens to 87 million people*. Retrieved from https://www.nbcnews.com/tech/tech-news/facebook-data-harvesting-scandal-widens-87-million-people-n862771

Rumbold, J. M. M., & Pierscionek, B. (2017). The effect of the general data protection regulation on medical research. *Journal of Medical Internet Research*, *19*(2), e47. doi:10.2196/jmir.7108 PMID:28235748

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217–224. doi:10.1016/j.im.2013.08.006

Snider, M., & Baig, E. C. (2019). *Facebook fined $5 billion by FTC, must update and adopt new privacy, security measures*. Retrieved from https://www.usatoday.com/story/tech/news/2019/07/24/facebook-pay-record-5-billion-fine-u-s-privacy-violations/1812499001/

Stallings, W. (2020). Handling of Personal Information and Deidentified, Aggregated, and Pseudonymized Information Under the California Consumer Privacy Act. *IEEE Security and Privacy*, *18*(1), 61–64. doi:10.1109/MSEC.2019.2953324

State of California Department of Justice. (2020). *Background on the CCPA & the rulemaking process*. Retrieved from https://oag.ca.gov/privacy/ccpa

Suen, H. Y., Chen, M. Y. C., & Lu, S. H. (2019). Does the use of synchrony and artificial intelligence in video interviews affect interview ratings and applicant attitudes? *Computers in Human Behavior*, *98*, 93–101. doi:10.1016/j.chb.2019.04.012

Thomas, I. (2020). Getting ready for the California Consumer Privacy Act: Building on General Data Protection Regulation preparedness. *Applied Marketing Analytics*, *5*(3), 210–222.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134–153. doi:10.1016/j.clsr.2017.05.015

Tiku, N. (2018). *Google's CEO says tests of censored Chinese search engine turned out great*. Retrieved from https://www.wired.com/story/wired-25-sundar-pichai-china-censored-search-engine/

Vermont Office of the Attorney General. (2018). *Guidance on Vermont's Act 171 of 2018Data Broker Regulation*. Retrieved from https://ago.vermont.gov/wp-content/uploads/2018/12/2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf

Victor, J. M. (2013). The EU general data protection regulation: Toward a property regime for protecting data privacy. *The Yale Law Journal*, *123*(2), 266–519.

Wachter, S. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review*, *34*(3), 436–449. doi:10.1016/j.clsr.2018.02.002

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, *7*(2), 76–99. doi:10.1093/idpl/ipx005

Winder, D. (2019). *Google confirms creepy new privacy problem*. Retrieved from https://www.forbes.com/sites/daveywinder/2019/06/23/google-confirms-creepy-new-privacy-problem/#1b4c96a29d8b

Winegar, A. G., & Sunstein, C. R. (2019). How much is data privacy worth? A preliminary investigation. *Journal of Consumer Policy*, *42*(3), 425–440. doi:10.100710603-019-09419-y

Zarsky, T. Z. (2016). Incompatible: The GDPR in the age of big data. *Seton Hall Law Review*, *47*, 995–1020.

Zhang, Y., Wang, T., & Hsu, C. (2019). The effects of voluntary GDPR adoption and the readability of privacy statements on customers' information disclosure intention and trust. *Journal of Intellectual Capital*.

ENDNOTE

[1] According to the Data Broker Regulation in Vermont, the definition of a data broker is as follows: "(A) "Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship. (B) Examples of a direct relationship with a business include if the consumer is a past or present: (i) customer, client, subscriber, user, or registered user of the business's goods or services; (ii) employee, contractor, or agent of the business; (iii) investor in the business; or (iv) donor to the business. (C) The following activities conducted by a business, and the collection and sale or licensing of brokered personal information incidental to conducting these activities, do not qualify the business as a data broker: (i) developing or maintaining third-party e-commerce or application platforms; (ii) providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier" (Vermont Office of the Attorney General, 2018).