Policy Response Analysis of the Facebook – Cambridge Analytica Scandal: Comparing the GDPR, CCPA, and APPI

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Benjamin Ainley

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kent Wayland, Department of Engineering and Society

Introduction

In today's world data is constantly being collected and stored by companies. This can be for several reasons such as personalizing user experience, improving marketing strategy, or selling customer data. Customers may not even know what kind of data is being collected, or feel they have no say in what kind of data large tech companies are collecting. Advances in data collection technology chains have enabled companies to collect, track, and analyze information, patterns, and habits about a user. This form of data is largely unregulated and can be sold to other companies without user consent. Because of this lack of control, customers may feel that their privacy is being violated and lose trust in companies. This data could also be potentially used for unethical purposes causing further harm to consumers or organizations. One data breach that brought major attention to ethics regarding people's data was the Facebook – Cambridge Analytica scandal, which was made known in 2018.

This scandal had a massive impact worldwide, with governments of numerous countries investigating the data breach. It sparked debate about the idea of data privacy, making it a center of concern in today's world. The Facebook – Cambridge Analytica incident led to the creation of laws regarding data privacy, and heightened the significance of existing ones, possibly influencing some changes. Data privacy laws have been passed around the globe in recent years, and each country is culturally different. This could lead to variations in these laws, affecting how countries do business with one another. By looking at these policy responses, we can gain better insight into the current state of personal information use and collection by companies. Although different countries each have their own laws regarding data privacy, companies will have to abide by the laws of other countries in order to do business internationally. The regulations of one nation can have effects on businesses based in another.

Background

In 2015 Cambridge Analytica was able to gain access to users' personal data by leveraging its alliance with Facebook. The scandal began when Global Science Research (GSR) initiated a research project in cooperation with Cambridge Analytica in order to identify the parameters necessary to develop "OCEAN" psychological profiles. These profiles were developed using a personality quiz and required users to allow access to their Facebook profiles, which gave the company access to the participants' friends' data through the Facebook Open API. The goal of the research was to establish a methodology for psychographic profiling of individuals; therefore, it was not necessary for the company to keep specific user data to conduct their research. However, Cambridge Analytica realized they could combine these user profiles with other data from social media, browsers, online purchases, voting results, and more. With all these data points, users could be micro-targeted with messages or advertisements likely to influence their behavior (Isaak 2018).

This scandal played a large role in the erosion of trust in consumers in companies. The fact that profiles of users could be made, and users could be subconsciously influenced through messages without consent caused public distrust in Facebook. A year before the scandal, 79 percent of users believed that Facebook was committed to protecting the privacy of their personal information. This dropped to 27 percent immediately after, and 28 percent after Zuckerberg's testimony with Congress (Weisbaum 2018).

The Facebook – Cambridge Analytica scandal impacted over 30 countries causing governments around the world to investigate. The magnitude of the incident also heightened public awareness to the topic of data privacy. This concern was heard, and in following years,

Governments looked to create or modify policies to give people better rights to privacy. Two significant pieces of legislation regarding this issue are the California Consumer Privacy Act (CCPA) and the EU's General Data Protection Regulation (GDPR). Both of these may have been significantly impacted by the data breach.

The California Consumer Privacy Act is a state statute intended to enhance privacy rights and consumer protection for residents of California, and is the United States' first comprehensive data privacy law. The statute was originally hastily passed and put on the November 2018 ballot. It is the toughest privacy law in the United States, which slightly concerned lawmakers. They initially felt that this law was too consumer privacy focused instead of striking a balance between consumer protection and preserving innovation. However, the Cambridge Analytica scandal caused the ballot initiative to gain more traction, and the California legislature faced pressure from data privacy advocates in the states of Washington and California. The CCPA then went into effect in January of 2020 after numerous amendments (Lee 2020).

The GDPR was approved by the European Union in 2016 and went into effect in May 2018. Although this is an EU regulation, the territorial scope of it applies broadly. The GDPR applies to any business that processes personal data of subjects in the European Union, making it an influential piece of legislature. Although the passing of the regulation was not directly caused by Cambridge Analytica scandal, the scandal heightened awareness. With regulators worried about the adequacy of security and data protection controls, it is likely that it had an impact on the way GDPR controls will be enforced and implemented. The scandal may have accelerated investigations and enforcement actions from the European Data Protection Authorities that may have otherwise been implemented with some restraint (Simberkoff 2018). Right now, many

countries look to the GDPR as a template when creating their own privacy laws, and this scandal may have contributed to its importance.

Looking at journals and articles can provide insight into how the GDPR is making a global impact by describing how other countries are affected by the legislation. In order to do business with the European Union, companies must follow GDPR protocols. Countries may look to pass data privacy laws in order to comply with GDPR regulations, but each country's laws will vary. Journals and articles will be used to explore how historical, cultural, business, and political traditions in each country may have shaped the laws and regulations in their respective jurisdictions.

The journal, "New Global Developments in Data Protection and Privacy Regulations", by Fiero and Beier (2022) provides an overview of the EU, US, and Russian data privacy regulations, as influenced by the GDPR, and how the culture of the countries may have affected these privacy regulations. The U.S. approach tends to be focused on concepts like personal freedom and non-interference by the state. The more uniform European approach tends to focus on the dignity of individuals and their protection not only against the state but also against private companies and other individuals. The European privacy mentality has also been largely influenced by its historical and political systems, such as European monarchies. the Nazi regime in Germany, and the totalitarian regime in the Soviet Union, under which disclosure of personal information could lead to severe consequences and prosecutions. Recently, U.S. society has focused more closely on data privacy concepts, with recent scrutiny on credit history checks, social media networks, and sharing other attributes of everyday American life, concepts that have long been considered invasive for many Europeans.

From pieces of literature, we also learn that the GDPR has influenced nonwestern cultures, such as Japan, who hold different values. Historically, Japanese society has not been as sensitive to the protection of privacy like westerners have. There was no real word for privacy in their dictionary until they recently imported the word "purabashi" during a legal issue in 1964 (Orito 2005). However, in order to play a role in the international market, Japan has recently enacted the Act on the Protection of Personal Information (APPI) to comply with the GDPR, and aiming to protect the personal information of Japanese Citizens. The EU recognized the Japanese APPI as providing an "equivalent" level of protection as the GDPR (Wang 2020). It is interesting how the EU and Japan were able to achieve this even with different cultural views on data privacy. This Japanese model of cooperative data privacy can serve as a precedent for other countries looking to reform their policies in order to meet GDPR standards.

Information from DataGuidance by One Trust is also useful when analyzing the technicalities of the different privacy policies. One Trust is the largest and most widely used privacy, security and third-party risk technology platform, trusted by more than 4,500 companies to comply with the CCPA, GDPR, ISO27001 and hundreds of the world's privacy and security laws. The article, "Comparing Privacy Laws: GDPR v. APPI", published by DataGuidance (2020) gives a comparison between the GDPR and the Act on the Protection of Personal Information (APPI) privacy laws. This provides key evidence by directly looking at important axes of comparison, such as terms defined by each policy, who it applies to, and what rights are given to individuals by each regulation.

Methods

This paper seeks to compare different data privacy policies around the globe, specifically the United States, European Union, and Japan. Law review articles discussing the GDPR, CCPA, and APPI were examined, as the offer critical commentary on these policies. These articles provide a better understanding of what each policy looks to accomplish, making it easier to compare each policy to highlight what varies between countries. Scholarly articles discussing the recent history of policies in certain countries were also examined. These give insight into the culture of each country and how it may or may not have changed in recent history. It also gives insight into what other factors influenced new legislation to be passed. I will also be looking directly at the GDPR, CCPA, and APPI acts, since they are the focus of this research paper. Through these law reviews, articles, and direct sources, what makes each policy different can be made clear, and what influenced each policy can be explored.

European Union's General Data Protection Regulation

Data privacy and protection has long been a concern in European countries. Beginning in the 1970s, European countries began enacting broad, omnibus national laws regarding data privacy, protection, and practices. Sweden was the first to enact a national statute in 1973. Similar laws soon followed in Germany, France, Spain, the United Kingdom, and the Netherlands. Finally in 1995, the EU passed the Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Data Protection Directive) in order to make one EU-wide data privacy and protection initiative. The Data Protection Directive applied to all EU members, but each member nation was required to implement the directive's requirements into their countries national law. This led to differing

implementations. To fix this and to bring EU law up to date with technological developments, the GDPR went into effect in 2018 (Mulligan 2019).

The GDPR applies to a company or entity which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed. It also applies to a company established outside the EU that is offering goods/services (paid or for free) or is monitoring the behavior of individuals in the EU. Thirdly, it applies if the data is physically processed in the EU (European Commission).

The GDPR also extends the definitions of personal data, which is characterized as any information relating to an identifiable person, whether directly or indirectly. This can include but is not limited to names, ID numbers, location data, or cookies if they can be "singled out" for the purpose of tracking user behavior. Processing includes collection, use, storage, organization, disclosure, or any set of operations performed on personal data. The GDPR also establishes different requirements for controllers and processors of personal data. Controllers determine the means of processing personal data, and a processor is responsible for processing data for the controller (Mulligan 2019).

There are certain conditions that need to be satisfied for the processing of personal data to be lawful: the consent of the data subject; necessary for the performance of a contract with the data subject; necessary for compliance with a legal obligation; necessary to protect the vital interests of the data subject; necessary for the performance of a task carried out in the public interests; or necessary for the purposes of legitimate interests. This last grounds for processing is new, and has been controversial.

The GDPR also encourages the use of "pseudonymization"; pseudonymized data is personal data that can no longer be attributed to a specific data subject without the addition of

other information, and may be processed subject to technical and organizational measures to ensure non-attribution (Bennet 2018). The GDPR refers to pseudonymisation as an example of an appropriate data protection safeguard in many circumstances, but distinguishes this from anonymized data.

What differs pseudonymisation from anonymization is that the latter consists of removing personal identifiers, aggregating data, or processing this data in a way that it can no longer be related to an identified or identifiable individual. Unlike anonymized data, pseudonymized data qualifies as personal data. The GDPR makes it compulsory to delete or anonymize personal data when there is no lawful purpose to keep it in a way that enables identification of an individual. Once anonymized, data is no longer under the scope of the GDPR.

Data subjects have the right to request erasure of personal data under six circumstances. They also have the right to correct inaccurate personal data and complete incomplete personal data. Consumers also have the right to restrict processing under certain circumstances, and a right to object to processing for profiling, direct marketing, and statistical, scientific, or historical research purposes (Friel 2018).

When it comes to a child's data, the default age for consent is 16, although individual member state law may lower the age to no lower than 13. The person with parental responsibility must provide consent for children under the consent age. Children must also receive an age-appropriate privacy notice, and their personal data is subject to heightened security requirements (GDPR Art. 8).

California Consumer Privacy Act (CCPA)

Consumers were originally provided with three main rights under this act. These rights include a "right to know" the information that businesses have collected or sold about them, a "right to opt out" of the sale of consumer information, and a right to request for the deletion of any information collected about the consumer under certain circumstances ("right to delete"). The act was then amended and as of January 1, 2023, consumers now have the "right to correct" inaccurate personal information that a business has about them and the "right to limit" the use and disclosure of sensitive personal information collected about them (Bonta 2023).

The CCPA applies to any company that collects personal information of California residents, is for-profit, and does business in California. However, there is also a basic set of thresholds needed to be met for the CCPA to apply. The company needs to make more than $25 million in annual gross revenues, or engages in the buying, selling, or receipt of the personal information of more than 50,000 Californians, or the company derives over 50% of its annual revenues from the sale of Californians' personal information (Bonta 2023).

This act does not distinguish between the sources of data, but rather regulates all "personal information." By the CCPA's definition, personal information is "information that identifies, relates to, describes, or is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," which basically includes any information a business would collect from a consumer. Browsing history, search history, information regarding a customer's interaction with a website, along with any inferences drawn from this information all fall under personal information (Mulligan 2019).

The CCPA also talks about deidentified data as "data, which cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer." This means the personal identifiers have been removed with the intent that they will not be associated with a specific individual again. If a business uses de-identified information, it must take organizational and operational steps to ensure that data is neither reidentified nor distributed (Blesch 2023).

Regarding children's information businesses can only sell the personal information of a child that they know to be under the age of 16 if they get affirmative authorization ("opt-in") for the sale of the child's personal information. For children under the age of 13, that opt-in must come from the child's parent or guardian (Bonta 2023).

Act on the Protection of Personal Information (APPI)

The APPI was originally enacted in 2003, making it one of the early omnibus privacy and data protection laws to be enacted. Since then, it was amended a number of times to better account for current trends in privacy law and place more restrictions on businesses while giving more rights to consumers. These amendments came into force on 30 May 2017. On 5 June 2020, the Japanese Diet approved a bill to further amend the APPI. The Amended APPI focuses on further regulating cross-border data transfers and came into force on April 1, 2022 (Schaetzel 2022).

The APPI, applies to all business operators that handle the personal data of individuals in Japan, which includes any business that provides a personal information database for commercial use. Under the APPI, a "personal information database" essentially includes any assembly of personal information arranged in a way so specific personal information can be retrieved via a

computer (Schaetzel 2022). Generally, any business that receives personal information to provide services or products to individuals in Japan will be subject to the APPI, even if the business is not located in Japan. However, a broadcasting institution, newspaper publisher or other press organization, professional writer, university, or other academic organization, religious body, or political party are exempted from the obligations under the APPI in connection with such press, professional writing, academic, and political activities respectively (Hounslow 2022).

Subsequently, "personal information" under the APPI includes any information that can identify an individual or contains an "Individual Identification Code." This second category of personal information includes computer-generated numbers, symbols, or code that is used to identify a body feature and to identify an individual person (i.e., fingerprint scanning). Another category included in the amended APPI is personal-related information. This includes information outside the scope of personal information such as pseudonymous information, or anonymous information. This information could still be used to identify an individual if connected to other information. Cookies and IP addresses would likely fall within this category. Personal and personal-related information do not require opt-in consent before a business collects this information. Instead, notice and choice, in the form of a privacy policy that properly accounts for the purposes the personal related information is collected, is sufficient. In addition, some provisions of the APPI specifically apply to "retained personal data," which is defined as "personal data which a PIC has the authority to disclose, correct, add or delete the contents of, cease utilization of, erase, and cease the third-party provision of." (Schaetzel 2022).

The APPI doesn't have significant restrictions on the processing of ordinary personal data, though data subjects do have the right to ask what data you process and your reasons for

doing so. The APPI does not list the legal grounds that Personal Information Controllers (PICs) must adhere to a priori when handling personal data. Consent (unless exceptions apply) is required when (i) the handling goes beyond the utilization purpose already declared to the principal; (ii) personal information is obtained by another operator as a result of a merger or another reason and the data is used for a different purpose from the one specified already to the principal; (iii) the personal information handled is special care-required personal data; (iv) personal information is provided to a third party; and (v) in the context of cross border data transfers (Hounslow 2022).

Comparison

Now we can directly compare the scope of each policy. To do so, we will look into who each policy applies to, what kind of data is regulated, and what rights people have under the policies. Once key differences are identified, we can look into how the history or culture of each country could have affected the regulations.

When looking at who each policy applies to, we can see that the GDPR is broader in scope than both the CCPA and APPI. Under the GDPR, the terms “data controller” and “data processor” are defined. The GDPR defines a “data controller” as a “natural and legal person, public authority, agency or other body which, alone or jointly, with others, determines the purposes and means of the processing of personal data.” “Data processor” is defined as a “natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller” under the GDPR. In contrast, CCPA does not define the terms “data controller” or “data processor” and instead refers to “businesses” and “service providers.” Instead of defining data controllers and processors, the APPI only explicitly refers to PICs as being subject

to its obligations. A PIC is defined as a "person providing a personal information database etc. for use in business."

The GDPR applies to any data controller or data processor that is established in the EU and uses personal data as part of the activities of one of its branches established in the EU. It also applies to businesses not established in the EU that process EU data subjects' personal data in connection with offering goods or services in the EU, or monitoring their behavior. The CCPA is limited solely to California residents and entities doing business in the state of California. While the GDPR applies to any organization that has a presence in the EU, collects data on subjects from the EU, or processes data physically in the EU (a data center for example), the APPI only covers businesses that handle the personal data of people who are residents Japan. It doesn't matter where the business is based, or where the processing happens

All acts also only really apply to public authorities, agencies, or businesses, so the processing of personal data by individuals for purely personal or household purposes is excluded from each of the acts. However, the GDPR applies to all businesses, public bodies, institutions as well as not for profit businesses. The CCPA only applies to a for-profit entity doing business in California that meets a certain criterion mentioned before. The APPI states that central government organizations, local governments, incorporated administrative agencies, and local incorporated administrative agencies are excluded from the definition of Personal Information Controllers (PIC). Broadcasting institutions, newspaper publishers, communication agencies, press organizations, are also out of the scope of the APPI.

All acts also cover some form of pseudonymized or anonymized data. The GDPR and CCPA are similar in their definitions of pseudonymized data, and requires that any additional information that could be used in combination with pseudonymized data to identify a person is

kept separately and secured. The amended APPI mentions personal-related information, which includes pseudonymous information, requiring companies to keep this secure as well. Both the GDPR and CCPA exclude anonymized data from their application, since both do not consider anonymous data as information that relates to an identified or identifiable natural person. However, the GDPR excludes reasonably deidentified data. The GDPR's concept of anonymization is stricter than the CCPA's deidentification requirement since the GDPR demands that an individual's identifiable information be "irreversibly prevented" from being used. Unlike the GDPR and CCPA, The APPI still applies to business operators who handle anonymously processed information. A business operator must process anonymous data in accordance with standards prescribed by the Personal Information Protection Commission.

None of the acts specifically define "child", but the GDPR and CCPA both provide provisions for people under the age of 16. Under the CCPA businesses must have opt-in consent to sell or share the personal information of consumers under the age of 16. For consumers at least 13 years of age and less than 16 years of age, the child's parent or guardian must affirmatively authorize the sale or sharing of the child's personal information. Under the GDPR, where the processing is based on consent, the consent of a parent or guardian is required for a person under the age of 16. While, the CCPA only requires parental consent for personal data sales, the GDPR's parental consent requirement applies to all processing consent requests. The APPI does not provide children with special protection with regard to the processing of their personal data.

The three legislations provide personal rights such as the right to erasure, right to object, and right to access data, but to varying degrees. Both the GDPR and CCPA give individuals the right to request the deletion of their personal data for free, and organizations must comply subject to certain exemptions. The data controller or business must also inform all third parties

involved with the use of that individual's personal information. Under the APPI, the PIC can collect a fee within a range recognized as reasonable. All three acts give users the ability to correct any inaccurate information, with the CCPA providing this right in the recent amendment. The right to object to the processing of their personal data is also provided under each act. The GDPR states that individuals have the right to withdraw consent to the processing of personal data at any time. Similarly, the CCPA gives consumers the right to consumer shall have the right to direct a business not to sell or share the personal information with a third party, and the APPI provides principals with a right to demand PICs to cease utilization of the personal information that can identify them. However, the APPI highlights that the obligation to cease utilization and delete retained personal information does not apply if it requires a large amount of expense, or in circumstances where it is difficult to fulfill. Unlike the GDPR and CCPA, individuals can not object to processing of their data for direct marketing purposes under the APPI Under all three legislations, users have the right to access their data. Although they are similar, the laws differ slightly with respect to the procedures around responding to a consumer's request to access their data. For example, The GDPR provides that the right of access must not adversely affect the rights or freedoms of others, while the CCPA has no such provisions. The GDPR and CCPA also provide users access free of charge, while PICs under the APPI may charge a fee for providing the data (Kateifides 2020).

Although all three acts take different approaches and have different definitions, what kind of information they protect is similar. The laws all focus on information that relates to an identifiable natural person, and gives users rights to delete, object, and access their data. However, some of the differences in the legislations may be related to the cultural values of each country. The EU considers the privacy of communications and the protection of personal data to

be fundamental rights, which are codified in EU law (Fefer 2020). These values are visible in the GDPR where protection of personal information is stricter compared to California's CCPA and Japan's APPI. For example, anonymized personal data is out of scope of the GDPR while deidentified data is the CCPA's equivalent. Anonymized data is stricter than deidentified data as it cannot be used to identify a person, exemplifying the GDPR's more stringent protection of personal data. Historically, Japan has viewed privacy differently than westerners. In general, Japanese society has not been very sensitive to the protection of privacy. This may be due to their collectivist culture, viewing the group as more important than the individual, leading to less strict privacy laws. The APPI does not restrict processing of ordinary personal data like the GDPR does and only requires consent in certain circumstances, like sensitive personal information. In Japan, government organizations are excluded from the APPI further exemplifying a collectivist culture. In recent years, Japan has made a push in developing data privacy laws, possibly because of external pressures in order to comply with the GDPR. This has led to the Japanese privacy framework protecting a narrower range of personal information than the GDPR, covering only what is necessary in order to comply with the EU's GDPR, allowing them to do business. This has led to Japan having slightly stricter and more comprehensive data privacy laws than the United States as a whole. The United States has more of a business focused culture compared to the other countries, and does not view privacy as a human right like Europe. This is very visible in their laws regarding data privacy. While the GDPR applies to all organizations that process personal data, the CCPA applies to businesses that are for profit and meet certain revenue or data processing thresholds. Additionally, the CCPA includes specific provisions related to the selling of personal information, which is not addressed in the GDPR.

Conclusion

With the Facebook – Cambridge Analytica scandal heightening awareness of personal data privacy and protection, countries worldwide have developed and continue to update comprehensive data privacy laws. Each country may approach how personal information is handled differently, possibly because of the cultural values of that country. The EU has treated data privacy as a human right and has the strictest set of laws regarding data protection and privacy. Many countries such as Japan and the US look to comply with these standards, especially when doing business with the EU, as it has set a "global standard." Japan's laws comply with the GDPR in order to business, but have aspects that are different and resemble more of a collectivist culture. The US's laws are more business oriented with less regards to data privacy and protection as a natural right. These differences are important for organizations to understand when developing their privacy compliance programs. In addition, by looking at different models, other countries can better develop their own comprehensive data privacy laws that suit their country's culture.

References

Bennett, C. J., Chun, S. A., Adam, N. R., & Noveck, B. (2018). The European General Data Protection Regulation: An instrument for the globalization of privacy standards? *Information Polity: The International Journal of Government & Democracy in the Information Age*, *23*(2), 239–246. https://doi.org/10.3233/ip-180002

Blesch, W. (2023, February 27). *The GDPR's anonymization versus CCPA/CPRA's de-identification*. TermsFeed. Retrieved from https://www.termsfeed.com/blog/gdpr-anonymization-versus-ccpa-de-identification/

Bonta, R. (2023, February 15). *California Consumer Privacy Act (CCPA)*. State of California - Department of Justice - Office of the Attorney General. Retrieved from https://oag.ca.gov/privacy/ccpa

European Commission. (n.d.). Who does the data protection law apply to?. from https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en#

Fefer, R. F., & Archick, K. (2020, July 17). *EU Data Protection Rules and U.S. Implications.* Congressional Research Service (CRS report IF10896). https://crsreports.congress.gov/product/pdf/IF/IF10896/11

Fiero, A. W., & Beier, E. (2022). *New Global Developments in Data Protection and Privacy Regulations: Comparative Analysis of European Union, United States, and Russian Legislation*. Stanford Journal of International Law, 58(2), 151–192. https://law.stanford.edu/publications/new-global-developments-in-data-protection-and-privacy-regulations-comparative-analysis-of-european-union-united-states-and-russian-legislation/

Friel, A., & Jehl, L. (2018, November 21). *CCPA and GDPR Comparison Chart*. BakerHostetler. Retrieved March 30, 2023, from https://www.bakerlaw.com/articles/alan-friel-laura-jehl-create-chart-comparing-ccpa-and-gdpr

General Data Protection Regulation (GDPR). (2022, September 27). Retrieved from https://gdpr-info.eu/

Hounslow, D., & Nozaki, R. (2022, December 19). *Japan - Data Protection Overview*. DataGuidance. Retrieved from https://www.dataguidance.com/notes/japan-data-protection-overview

Mulligan, S. P. & Linebaugh, C. D. (2019, March 25). Data Protection Law: An Overview (Report No. R45631). Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R45631

Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, *51*(8), 56–59. https://doi.org/10.1109/mc.2018.3191268

Kateifides, A., Potter, A., Highams, H., Strugnell, C., Campbell, C., Marini, A., Young, A., & Ashcroft, V. (2020, September 11). Comparing privacy laws: GDPR v. Appi. DataGuidance. https://www.dataguidance.com/sites/default/files/gdpr_v_appi_april_update.pdf

Lee, C. (2020). The Aftermath of Cambridge Analytica: A Primer on Online Consumer Data Privacy Note. *AIPLA Quarterly Journal*, *48*(3), 529–568. https://heinonline.org/HOL/P?h=hein.journals/aiplaqj48&i=544

Miltgen, C. L., Cases, A.-S., & Russell, C. A. (2019). Consumers' responses to Facebook advertising across pcs and mobile phones. *Journal of Advertising Research*, *59*(4), 414–432. https://doi.org/10.2501/jar-2019-029

Orito, Yohko & Murata, Kiyoshi. (2005). *Privacy Protection in Japan: Cultural Influence on the Universal Value*. Meiji University Center for Business Information Ethics. http://www.isc.meiji.ac.jp/~ethicj/Privacy%20protection%20in%20Japan.pdf

Pal, R., & Crowcroft, J. (2019). Privacy trading in the surveillance capitalism age *viewpoints on 'privacy-preserving' societal value creation*. *ACM SIGCOMM Computer Communication Review*, *49*(3), 26–31. https://doi.org/10.1145/3371927.3371931

Schaetzel, L., & Sulkin, R. (2022, March 15). *Amended Japanese privacy law creates new categories of regulated personal information and cross-border transfer requirements*. JD Supra. Retrieved from https://www.jdsupra.com/legalnews/amended-japanese-privacy-law-creates-7847421/#

Simberkoff, D. (2018, August 30). How Facebook's Cambridge Analytica scandal impacted the intersection of privacy and regulation. *CMSWire.com*. Retrieved from https://www.cmswire.com/information-management/how-facebooks-cambridge-analytica-scandal-impacted-the-intersection-of-privacy-and-regulation/

Wang, F. Y. (2020). *Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement*. Harvard Journal of Law & Technology (Harvard JOLT, 33(2), 661-692). https://jolt.law.harvard.edu/assets/articlePDFs/v33/33HarvJLTech661.pdf

Weisbaum, H. (2018, April 18). *Trust in Facebook has dropped by 66 percent since the Cambridge Analytica scandal*. NBCNews.com. Retrieved from https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011