Spring 5-1-2023

Consumers' Perceptions of Digital Privacy in the United States and Japan

Destiny Randle
destiny.r3201@gmail.com

(Signed by Gary Gold, Advisor,

on Thursday March 16th)

Consumers' Perceptions of Digital Privacy in the United States and Japan

Destiny Randle

Major: International Marketing

Minor: East Asian Languages

Sponsor: Professor Gary Gold

Whittier Scholars Program

Spring 2023

Tables of Contents

Abstract

The purpose of my study is to explore the contours of contemporary consumer privacy protections derived from legislation, regulations and publicly available company policies as a way to get a better understanding of how consumer data is protected. A few examples ranging from company-based consumer protection in the United States to data breaches in Japan will be explored and examined. Finally, this paper includes a comparative survey of consumer perceptions and concerns related to personal data privacy in the U.S. and Japan. As a way to assess the degree to which digital privacy and personal data breaches have adversely influenced consumer perceptions, several data abuse examples will be highlighted and discussed.

Key Words: Digital Marketing, Consumer Protections, Digital Privacy, United States, Japan

Introduction

Modern technological innovations are creating new opportunities across the marketing landscape, especially in the way consumer data is collected and used. Data collection can be a public service, as it allows the collector to have the ability to gather information that can impact economic development, health care, environmental impact, among others. However, in the absence of regulations concerning consumers, sharing consumer information can sometimes lead to harmful or even ongoing devastating consequences and related damages. Law enforcement, researchers, marketers, data brokers, and hackers are just a few examples of entities that varyingly benefit from the collection and sale of consumer data.

The purpose of my study is to provide insight into consumer perceptions of digital privacy. First, I provide an overview of digital and big data marketing. To later understand societal attitudes, I review incidences of what each country perceived as personal data abuse. I then explore cross-cultural attitudes towards the collection and usage of consumer information. Finally, an exploration of the United States and Japan's legislation, regulations, and enforcement agencies is conducted to see if there is a connection between current protections and consumer perceptions of digital privacy. While there are various approaches to data mining and manipulation, I focus on data collection from network/social data as an example of how companies target users specifically for digital marketing and third-party purposes.

Scope and Limitations

This research focuses on the U.S. Federal[1] and Japan National laws, including legislation and regulations. Naturally, when undertaking an international comparative research, there are likely to be issues finding resources that have been translated into the English language. However, sufficient resources were available in order to make this comparison possible. As a result of technological advancements and the rapid spread of social media platforms and other networking applications, the resources explored and used are post-2000.

Digital and Big Data Marketing

The science of marketing is continuously evolving, as demonstrated by the plethora of companies promoting their brands, and building a stronger sense of community with customers, on a variety of media channels and platforms. In this section, past advertising campaigns/methods will be discussed while also highlighting current practices. Current practices being, in particular, social media and its influence on the success of a company and brand. A platform with millions of users assists in the prediction and marketing of a brand, service or

[1] State privacy legislations, the Children's Online Privacy Protection (COPPA), Health Insurance Portability and Accounting Act (HIPAA), and other consumer based legislations are outside of my scope of research. The legislations mentioned here will not appear in the Table of Authorities, as they will not be used in this project.

product. Lastly, big data analytics will be explored to see how this method brings not only consumer happiness but also consumer doubt, mistrust, and harm.

Modern Marketing

To drive growth in the digital age, traditional marketing practices have been modernized in an effort to connect with brand target audiences, raise customer conversion rates[2], and enhance creative advertising campaigns.

Traditional marketing used channels like TV, newspapers, and flyers to promote a company, its mission, and product. Now, in the modern era, thousands of dollars every year are budgeted to go towards advertising efforts.[3] Online marketing assists a business in building and maintaining customer relationships; personalizing products, services, and messages, and allowing marketers to raise the success rate of a marketing campaign efficiently and quickly.[4] This innovative approach utilizes customer insights from ads and the personal information gathered on social media and other various platforms.[5]

Use of Social Media

Social media information contains the content of those who post publicly on social media sites including Facebook, Twitter, TikTok, etc. Using data collected from those social media platforms improve/create a personalized experience for the customers and helps marketers understand their target audiences' wants.[6] Having the ability to collect data in real-time heightens the success of a product or service and the longevity of a brand/company as it provides insight into consumer feelings, typical behaviors, and their interaction patterns with companies.[7]

It also assists in the personalization of a brands' online marketing strategy, as every platform may not share a similar audience. Within the larger umbrella of digital marketing/the usage of data, social data falls under the category of Big data.

---

[2] The customer conversion rate represents the percentage of consumers who take a certain action.
[3] Armstrong, Sarah, Dianne Esber, Jason Heller, and Björn Timelin. "Modern Marketing: What It Is, What It Isn't, and How to Do It." McKinsey & Company. McKinsey & Company, March 2, 2020. https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/modern-marketing-what-it-is-what-it-isnt-and-how-to-do-it.
[4] Ibid
[5] Ibid
[6] Newberry, Christina. 2022. "Social Media Data Collection: Why and How You Should Do It." Social Media Marketing & Management Dashboard. January 24, 2022. https://blog.hootsuite.com/social-media-data-collection/.
[7] Allen, Richard. "Types of Big Data: Understanding & Interacting with Key Types SelectHub. https://www.selecthub.com/big-data-analytics/types-of-big-data-analytics/.

Big Data Marketing

With technology advancing and globalization increasing, more information about ourselves can be found online. For example, the simple click on a link to access online music generates consumer information and preferences that can be collected, stored, and used for a variety of purposes. This large amount of digital information can be known as Big Data, "pav[ing] the way for virtually any kind of insight an enterprise could be looking for."[8]

Subtypes of big data are:[9]

1) *Social Data*: gathered from social media, including data from likes, tweets, comments, etc.
2) *Real-Time Data*: provided by online streaming media, including Youtube, Skype, and Netflix.
3) *Transactional Data*: gathered when you make an online purchase.
4) *Geographic Data*: collected by satellites, which captures the location data of humans, vehicles, buildings, objects.
5) *Natural Language Data*: gathered mostly from voice searches.

This project explores how marketing types, strategies, and practices are integral in assisting companies gain new insight into consumer buying habits, including brands and other personal preferences and interests. Amazon[10] and Netflix[11] represent two prominent examples of online companies that use such information to better serve their customers by adapting a data driven targeting strategy.

This modern marketing technique brings a lot of benefits due to its effectiveness, but also brings a wave of concern. Most consumers, from all around the world, appreciate personalized advertising and its impact on their everyday life, while an always increasing number of people fear the consequences of the collection of personal digital information.[12] Their concerns are often related to privacy as the collection of personal data can lead to data breaches, the selling of information to third parties (without given consent), and identity theft to name a few. The collection and transferring of personal digital data is a worldwide activity and a potential long-lasting damaging issue/problem.[13]

---

[8] Ibid
[9] Ibid
[10] Amazon specializes in e-commerce, online advertising, artificial intelligence, etc.
[11] Netflix is a streaming service that offers users a variety of shows, movies, etc.
[12] Evolution, Marketing. 2020. "Tackling Data Privacy Issues in a Data-Driven Marketing World." www.marketingevolution.com. August 14, 2020. https://www.marketingevolution.com/knowledge-center/data-privacy-issues-in-data-driven-marketing.
[13] Ibid

American and Japanese Applied Examples

This section explores a spectrum of digital privacy concerns, in the United States and Japan, while also highlighting the significance of each example. The examples describe cases which considered opt-out of app tracking concerns, unauthorized data collection activities, lack of transparency in data collection intent and usage, inadequate data security measures, etc.

United States

Apple and Facebook (Dispute over Privacy and Advertising)

American multinational technology company Apple Inc. developed and released a new feature that allows iOS users to opt out of app tracking, causing Facebook parent company Meta Platforms, Inc. to anticipate a 10 billion dollar drop in ad sales for the upcoming year.

Launched in May 2022, the App Tracking Transparency (ATT) feature offered mobile device owners the opportunity to not share their Identifier for Advertisers (IDFA).[14] Similar to third party cookies on browsers, the IDFA allows brands to follow ad activity and downloads to create personalized app experiences for its users.[15] With the iPhone 14.5 update, app publishers now need to include a pop-up window asking permission to track consumer behavior for sales.[16] Early reports since the update indicate that over 95% of iPhone users were opting out of ad tracking.[17]

As a result of Apple's privacy change, Meta is expected to face a dramatic financial decrease of $10 billion dollars in the upcoming year.[18] Essentially, Apple users are disabling Meta's primary means of collecting advertising data, which is the company's business purpose. Being "the ability to target ads at users with precision and prove to marketers that the ads generate sales."[19]

This scenario serves as an example where a company works towards protecting the consumer's personal data. In this case, Apple serves as a gatekeeper of customer data to preserve digital privacy efforts. It does not, however, disregard Apple's past incidences of the unauthorized usage and sale of personal information. As I mentioned before, it serves the purpose of highlighting

---

[14] Leswing, Kif. 2022. "Facebook Says Apple IOS Privacy Change Will Result in $10 Billion Revenue Hit This Year." CNBC. February 3, 2022. https://www.cnbc.com/2022/02/02/facebook-says-apple-ios-privacy-change-will-cost-10-billion-this-year.html.
[15] "What Is IDFA & Marketing without Identifier for Advertisers?" n.d. www.epsilon.com. https://www.epsilon.com/us/insights/trends/idfa#:~:text=The%20Identifier%20for%20Advertisers%20.
[16] Gilbert, Ben. 2022. "Facebook Blames Apple after a Historically Bad Quarter, Saying IPhone Privacy Changes Will Cost It $10 Billion." Business Insider. February 3, 2022. https://www.businessinsider.com/facebook-blames-apple-10-billion-loss-ad-privacy-warning-2022-2#:~:text=Facebook%20blames%20Apple%20after%20a.
[17] Ibid
[18] Ibid
[19] "Inside Facebook's $10 Billion Breakup with Advertisers." *Wall Street Journal*, 18 Feb. 2022, www.wsj.com/articles/facebook-apple-google-advertising-privacy-changes-1164519987.

business-based consumer data privacy protections. It also significantly demonstrates the importance of the collection of personal data for business operations and the effectiveness of creative advertising. As citizens increasingly have opt-out options, it is crucial to understand consumer sentiment towards tracking and data usage and to develop and innovate consumer-sentiment informed digital marketing campaigns.

FTC v VIZIO **(Unauthorized Collection and Sale of User Data)**

In February 2017, the Federal Trade Commission (FTC) and the New Jersey Attorney General filed a complaint against Television Manufacturer VIZIO Inc. due to its unauthorized gathering and selling of consumer personal data to third parties.[20]

Through the default enabling of the "Smart Interactivity" feature and integrated tracking software within the device, the company collected consumer viewing data and demographic information.[21] Third parties then used this acquired data to measure advertising performance and enhance targeted marketing efforts.[22]

Both the New Jersey Attorney General and the FTC deemed the company's data collection methods deceptive and unfair trade practices in violation of the FTC Act.[23] These violations occurred because VIZIO misrepresented the purpose of the TV feature, failed to be transparent with customers, sold collected consumer information without consent, and made the opt out feature difficult to use. The detailed specifics about the actual violations are as follows:

1) Similar to the personalization feature used by many popular streaming services such as Netflix, VIZIO's "Smart Interactivity" feature purpose was ostensible to provide users with a more personalized experience by collecting and analyzing consumer viewing data. This promise was never kept by the manufacturers, instead this information was sold to third parties for marketing purposes.[24]

2) The collection and disclosure of personal information was never made aware to consumers of VIZIO TVs.[25]

---

[20] McMeley, Christin S., et al. "The Real Takeaway from VIZIO's Privacy FTC Settlement | Davis Wright Tremaine." *www.dwt.com*, Oct. 2017, www.dwt.com/blogs/media-law-monitor/2017/10/the-real-takeaway-from-vizios-privacy-ftc-settleme.
[21] Ibid
[22] Cardozo, Larc, et al. *Why VIZIO's Settlement with the FTC Matters Why VIZIO's Settlement with the FTC Matters*. 2017.
[23] Federal Trade Commission Act, Section 5 (FTC Act) (15 USC §45): Unfair or Deceptive Acts
[24] Cardozo, Larc, et al. *Why VIZIO's Settlement with the FTC Matters Why VIZIO's Settlement with the FTC Matters*. 2017.
[25] McMeley, Christin S., et al. "The Real Takeaway from VIZIO's Privacy FTC Settlement | Davis Wright Tremaine." *www.dwt.com*, Oct. 2017, www.dwt.com/blogs/media-law-monitor/2017/10/the-real-takeaway-from-vizios-privacy-ftc-settleme.

3) Notices sent to consumers about the feature and usage were considered to be vague and misleading.[26]

4) VIZIO made opting out of data collection difficult.[27]

Penalties for the violations included paying the FTC $1.5 million and the New Jersey Division of Consumer Affairs $700,000,[28] deleting (or the deletion of) all pre-existing information and only utilizing data gathered with consent.[29] VIZIO also was mandated to accept a 20-year third party monitor to ensure compliance of the FTC ruling.[30]

This case demonstrates the importance of the FTC and government intervention when it comes to protecting consumers and their personal information. The agency's involvement in customer protection sends a signal that unauthorized data collection and sale, among other digital privacy abuses, will not be accepted. Hopefully with the FTC's well publicized enforcement, consumers can trust that their data will not be misused.

***FTC v Chegg* (Data Breaches)**

The Federal Trade Commission (FTC) found that Chegg violated two counts under the FTC Act[31] as the company suffered four data breaches within the span of three years as a result of inadequate digital security measures.

Chegg, Inc. is an educational technology company that targets primarily high school and university students.[32] It offers a significant range of direct-to-student educational products and services such as textbooks, tutors, homework support, etc.[33] Within its business operations, the company collects sensitive information of its customers, including "religious affiliation, heritage, date of birth, disabilities, and parents' income".[34] All of this information plus employee data was stored on a third party cloud storage service, Simple Storage Service (S3), which is offered by

---

[26] Ibid
[27] Ibid
[28] Murphy, Kathleen A. "Recent FTC regulation of the Internet of Things." *Bus. LAw.* 73 (2017): 289.
[29] Ibid
[30] McMeley, Christin S., et al. "The Real Takeaway from VIZIO's Privacy FTC Settlement | Davis Wright Tremaine." *www.dwt.com*, Oct. 2017, www.dwt.com/blogs/media-law-monitor/2017/10/the-real-takeaway-from-vizios-privacy-ftc-settleme.
[31] Federal Trade Commission Act, Section 5 (FTC Act) (15 USC §45): Unfair or Deceptive Acts
[32] Bryan, Kristin L. "Ed Tech Company's Four Data Breaches in Three Years Leads to FTC Enforcement Action." *The National Law Review*, 4 Nov. 2022, www.natlawreview.com/article/ed-tech-company-s-four-data-breaches-three-years-leads-to-ftc-enforcement-action.
[33] Ibid
[34] Fair, Lesley. "Multiple Data Breaches Suggest Ed Tech Company Chegg Didn't Do Its Homework, Alleges FTC." *Federal Trade Commission*, 31 Oct. 2022, www.ftc.gov/business-guidance/blog/2022/10/multiple-data-breaches-suggest-ed-tech-company-chegg-didnt-do-its-homework-alleges-ftc.

Amazon Web Services (AWS).[35] Employees and third-party contractors of Chegg earned full administrative privileges to these S3 databases by using a single access key. Additionally, the company did not require a multi-factor authentication for account access and failed to encrypt the data collected. As a result of the company's inadequate security measures, four separate data breaches occurred within the span of three years (September 2017 - April 2020),[36] exposing the personal information of Chegg's consumers and employees.[37] The following are the data breaches noted:[38]

1) A data thief gained access to Chegg employee direct deposit payroll information after employees were duped by a phishing attack. Information such as social security numbers, addresses, passwords, and more were collected.

2) Sensitive information was posted on a public website after a former third-party contractor utilized the AWS access key and collected material from Chegg's S3 database.

3) In another phishing attack, a senior Chegg executive allowed a data thief to bypass the company's multi-factor email authentication system. Personal information regarding consumers' financial and medical information was stolen.

4) The same employee responsible for the payroll phishing attack, was again duped allowing the intruder to gather W-2 information of approximately 700 current and former Chegg employees.

The FTC prioritizes privacy and violations[39] and took action against Chegg for the insufficient data security practices leading to the exposure of sensitive data of approximately 40 million customers and employees. Within this complaint included two counts of violation of the FTC Act:[40]

---

[35] Ibid
[36] Bryan, Kristin L. "Ed Tech Company's Four Data Breaches in Three Years Leads to FTC Enforcement Action." *The National Law Review*, 4 Nov. 2022, www.natlawreview.com/article/ed-tech-company-s-four-data-breaches-three-years-leads-to-ftc-enforcement-action.
[37] Fair, Lesley. "Multiple Data Breaches Suggest Ed Tech Company Chegg Didn't Do Its Homework, Alleges FTC." *Federal Trade Commission*, 31 Oct. 2022, www.ftc.gov/business-guidance/blog/2022/10/multiple-data-breaches-suggest-ed-tech-company-chegg-didnt-do-its-homework-alleges-ftc.
[38] Ibid
[39] Bryan, Kristin L. "Ed Tech Company's Four Data Breaches in Three Years Leads to FTC Enforcement Action." *The National Law Review*, 4 Nov. 2022, www.natlawreview.com/article/ed-tech-company-s-four-data-breaches-three-years-leads-to-ftc-enforcement-action.
[40] Federal Trade Commission Act, Section 5 (FTC Act) (15 USC §45): Unfair or Deceptive Acts

1) Under the “Unfair Act or Practice” category, Chegg’s data security practice was deemed a failure as it“causes or is likely to cause substantial injury to consumers” and it “cannot be reasonably avoided by consumers.”

2) According to the “Deceptive Acts or Practices" category, Chegg misrepresented their practices. They falsely claimed to utilize reasonable measures to protect personal information against unauthorized access.

The FTC also alleged that Chegg’s failure to take precautionary measures and practice cybersecurity safeguards led to such an exposure.[41] For example, requiring that Chegg employees take a data security training session could have prevented data breaches as employees may have been able to successfully identify a phishing attempt.[42]

In order to settle the case, the company agreed to restructure its data protection practices by:

1) Transparency: The company must be transparent about what personal information it collects, why it collects the data, and when it will be deleted. Customers will have access to the information collected and Chegg must honor data deletion requests.

2) Data Protection Measures: For the protection of Chegg accounts, the company must provide secure measures such as two-factor authentication to customers and employees.

It is crucial for businesses to understand the vulnerabilities of personal information and the importance of data security practices. This applied example of digital privacy abuse highlights the risk with data collection and how essential data security is to maintain the trust and safety of customers.

Japan

Rikunabi **(Unauthorized Collection and Sale of User Data)**

College students and those just beginning in their career migrate to Rikunabi (リクナビ) as it serves as Japan’s largest job searching platform.[43] This media subsidiary is operated by Recruit Career Co., Ltd, which also owns Indeed[44] and Glassdoor[45]. Rikunabi supports users through

[41] Fair, Lesley. “Multiple Data Breaches Suggest Ed Tech Company Chegg Didn’t Do Its Homework, Alleges FTC.” *Federal Trade Commission*, 31 Oct. 2022, www.ftc.gov/business-guidance/blog/2022/10/multiple-data-breaches-suggest-ed-tech-company-chegg-didnt-do-its-homework-alleges-ftc.
[42] Ibid
[43] jopus編集部. n.d. “Rikunabi｜a Perfect Guide to Get Jobs and Work in Japan – Jopus.” A Perfect Guide to Get Jobs and Work in Japan – Jopus. https://jopus.net/en/jobboard/rikunabi.
[44] Indeed is an American employment website that offers job listings worldwide.
[45] American website Glassdoor allows current and former employees to anonymously review companies.

their professional journeys by providing a listing of thousands of jobs, informational events, joint interview practices, etc.[46] A user's orientation is analyzed based on the companies found on their favorite list. This feature enhances student to company success rates as it recommends businesses suitable for the student and their interests.[47] The Rikunabi data privacy scandal revolves around the collaboration of companies and the distribution of the users' personal information.

It was between March 2018 and February 2019 that Recruit Career started using Rikunabi's data, specifically its cookies.[48] Cookies in general serve as a tracking tool that allows companies to collect users' search history, browsing history, and website interactions as an effort to enhance personalization and gain consumer insight. This information gathered by Rikunabi was calculated and sold to third parties to then be used in analysis to predict how likely an individual job applicant would decline or accept an offer.[49] As Japan exercises a dominant lifetime employment system,[50] students worry that those scores would limit their whole professional life.[51] Public outcry ensued after it was announced that thirty-five companies, including Toyota Motor Corporation and other Japanese corporations, purchased the job-declining scores.[52] Recruit Career justified its decisions by stating that the companies who purchased these scores agreed not to use them for the selection of candidates.[53] Despite there being no way for users' to know how their data would be used.[54]

Unauthorized Collection and Sale of User Data[55]

A Rikunabi cookie ID linked an applicant's account together with information, including their real names, email addresses, browsing activity – what companies they searched for and which industries they seemed interested in. Recruit Career subcontracted Recruit Communications, a marketing and advertising company, to create and distribute job-declining scores using the IDs, and only omitting users' real names. Clients such as Toyota Motor Corporation and Mitsubishi Motors purchased the algorithmic scores. The same client companies also collected job applications on their own website, essentially also collecting the applicants' names and contact

[46] jopus編集部. n.d. "Rikunabi｜a Perfect Guide to Get Jobs and Work in Japan – Jopus." A Perfect Guide to Get Jobs and Work in Japan – Jopus. https://jopus.net/en/jobboard/rikunabi.
[47] Ibid
[48] Cyphers, Hinako Sugiyama, Katitza Rodriguez, and Bennett. 2021. "Japan's Rikunabi Scandal Shows the Dangers of Privacy Law Loopholes." Electronic Frontier Foundation. May 12, 2021. https://www.eff.org/deeplinks/2021/05/japans-rikunabi-scandal-shows-dangers-privacy-law-loopholes.
[49] Ibid
[50] In Japan, there is a culture/history of workers staying with the same company for their entire career.
[51] Cyphers, Hinako Sugiyama, Katitza Rodriguez, and Bennett. 2021. "Japan's Rikunabi Scandal Shows the Dangers of Privacy Law Loopholes." Electronic Frontier Foundation. May 12, 2021. https://www.eff.org/deeplinks/2021/05/japans-rikunabi-scandal-shows-dangers-privacy-law-loopholes.
[52] Ibid
[53] Ibid
[54] jopus編集部. n.d. "Rikunabi｜a Perfect Guide to Get Jobs and Work in Japan – Jopus." A Perfect Guide to Get Jobs and Work in Japan – Jopus. https://jopus.net/en/jobboard/rikunabi.
[55] Cyphers, Hinako Sugiyama, Katitza Rodriguez, and Bennett. 2021. "Japan's Rikunabi Scandal Shows the Dangers of Privacy Law Loopholes." Electronic Frontier Foundation. May 12, 2021. https://www.eff.org/deeplinks/2021/05/japans-rikunabi-scandal-shows-dangers-privacy-law-loopholes.

information. A users' data was assigned under their own unique applicant ID. All of this information was linked to a client's Employer cookie ID, later given to Recruit Communications to connect. Using a method called cookie synching, connection of cookies with one another - combining information from one place to another, applicants were identified. The linked database predicted whether or not a user would accept or reject an offer from a certain employer. Since client companies had their own databases, they could associate the scores received with the real names of job applicants.

The concern is that this data operation may have cost applicants a job offer by potentially, inaccurately predicting what companies they are interested in, nonetheless, without their knowledge or consent.

APPI Scope:[56]

The Act on the Protection of Personal Information (APPI)[57] guidelines do not regard cookies or similar machine-generated identifiers (e.g. IDFA) as personal data if a company itself cannot use it to identify a person. The legal workaround can be seen in the Rikunabi data privacy scandal. It allowed a business to freely collect, calculate and share personal information that the recipient of the data could use to re-identify an individual.

Under the APPI, organizations are prohibited from sharing personal information without consent and notice. Since Recruit Communications analyzed and transferred data that had names and other personal identifiers omitted, there was no need to get user consent. The Personal Information Protection Commission (PPC), a Japanese data protection authority, ordered Rikunabi to improve their privacy protection measures. The company was found to have engaged in "very inappropriate services, which circumvented the spirit of the law."

In June 2020, the APPI was amended, making it a requirement that companies confirm whether or not the recipient of the data could re-identify someone. Rikunabi's work would have violated the 2020 amendment as well as the 2022 APPI guidelines. Both amended legislations require companies to gain users' prior consent to the collection, processing, and transferring of personal data.

The Rikunabi data privacy incident demonstrates the workarounds under Japan's data protection law, the APPI. Although since the case, the act has been revised and updated, it has still been argued that its protections are not adequate. To avoid losing public trust, it is crucial for businesses to partake in ethical norms and understand the consumers place/perceptions of personal data operations before the law regulates them.

[56] Ibid
[57] Act on the Protection of Personal Information (Act No. 57 of 2003)

Aflac Insurance and Zurich Insurance (Consumer Data Breaches)

Aflac Life Insurance Japan Ltd. and Zurich Insurance Co., reported a data breach that compromised the data of 2 million Japanese customers in January 2023.[58]

A hack against a U.S. subcontractor exposed the data of 1,323,486 holders of three cancer insurance policies (Aflac) and 757,463 automobile insurance policyholders with Zurich.[59] The hacker gained personal information including, last names, ages, genders and insurance information, email addresses, customer IDS, etc.[60] It was reported by Zurich that stolen information does not include customers' credit card numbers, bank account details and accident records.[61] Both international insurance companies have launched their own investigations into the incident.

Jon Sullivan, Aflac Director of Communications, shared in a press release that "the incident, caused by a vulnerability in a file transfer server, originated with a subcontractor of a third-party vendor that Aflac Japan uses for marketing purposes and affected approximately 1.3 million customers."[62] It was also mentioned that the data stolen was posted on the dark web, personally identifiable information (PII) was not found online.[63]

Zurich Insurance Group's spokesperson also attributed the stolen customer data to a third-party service provider. "There is no indication that any customer data outside of Japan has been compromised, nor indication of any compromise of Zurich internal systems," shared the spokesperson.[64]

This case is another example of the dangers of entrusting personal data to third parties that have inadequate digital security practices. It is considered to be one of the reasons why they remain top targets for hacking and stealing data. To ensure the safety of consumers, companies should work with business partners that use the same, if not better, data protection practices.

---

[58] Olano, Gabriel. 2023. "Aflac and Zurich Japan Businesses Hit by Data Breaches." www.insurancebusinessmag.com. January 12, 2023. https://www.insurancebusinessmag.com/asia/news/cyber/aflac-and-zurich-japan-businesses-hit-by-data-breaches-432564.aspx.
[59] "Two Insurers in Japan Suffer Major Data Breach." 2023. Business Insurance. January 11, 2023. https://www.businessinsurance.com/article/20230111/STORY/912354813/Two-insurers-in-Japan-suffer-major-data-breach.
[60] Olano, Gabriel. 2023. "Aflac and Zurich Japan Businesses Hit by Data Breaches." www.insurancebusinessmag.com. January 12, 2023. https://www.insurancebusinessmag.com/asia/news/cyber/aflac-and-zurich-japan-businesses-hit-by-data-breaches-432564.aspx.
[61] Ibid
[62] Greig, Jonathan. 2023. "Millions of Aflac, Zurich Insurance Customers in Japan Have Data Leaked after Breach." The Record from Recorded Future News. January 12, 2023. https://therecord.media/millions-of-aflac-zurich-insurance-customers-in-japan-have-data-leaked-after-breach/.
[63] Ibid
[64] Ibid

It is clear that the collection of consumer data provides a multitude of benefits and usages, specifically in the Advertising Industry. It is also noted that such collections can put consumers at risk due to a variety of digital privacy concerns. The examples presented in this paper illustrate the importance for governmental and business cooperation and collaboration to earn consumer trust and ultimately, to maintain and ensure consumer safety.

American and Japanese Attitudes

One of the primary goals of this paper is to identify the intersections of digital marketing, intercultural consumer perceptions, and data abuses. Within this section, I will explore some of the similarities and differences in attitudes and perceptions between Japanese and American consumers concerning digital privacy.

Survey Design

To gain a better understanding of current consumer perceptions of digital privacy in the United States and Japan, I conducted an online survey. Participants of this survey were members of the Whittier College community, located in Southern California, and J.F. Oberlin University, located in Tokyo, Japan. Amongst those respondents, outside groups such as friends and family of both countries also supported and participated in this research. Using Formstack, 140 American and 48 Japanese respondents were asked to provide their thoughts on digital privacy concerns and the consumer protections that exist, don't exist, or that should be improved upon.

For questions 1 and 2, participants provided their demographic information including age and nationality. Additionally, for question 3, they were asked "How active are you online daily?", to gauge their involvement with digital environments. Further questions measured their agreement with certain statements to which a two sample t-test was performed to compare and contrast American and Japanese consumers' responses. Questions that measured respondents' agreement to a statement allowed them to answer using the 7-point likert scale, Strongly Disagree-Strongly Agree.

Data collection for this study started in January and ended in February 2023 (survey opened for one month). Subjects were not required to answer every question before submitting their responses to be analyzed. Therefore, the N of respondents for each question varies slightly, and are individually reported below.

Scope and Limitations

As a result of an error in Question 5, only 75 American respondents out of the 140 responses were able to be analyzed and reported on. To ensure fairness and accurate results, the remaining 65 responses have been discarded from analysis.

Question 5 asked participants, ‘Please select all of the digital privacy concerns that bother you.’ In the American survey, respondents were allowed to choose multiple concerns while the Japanese survey only allowed members to pick one digital privacy concern. I edited and redistributed the survey to a new American subject group to correct the error.

Lastly, although there are many digital privacy concerns that exist, I've only chosen a select group for the survey and analysis. These were chosen after my research, detailed in previous sections.

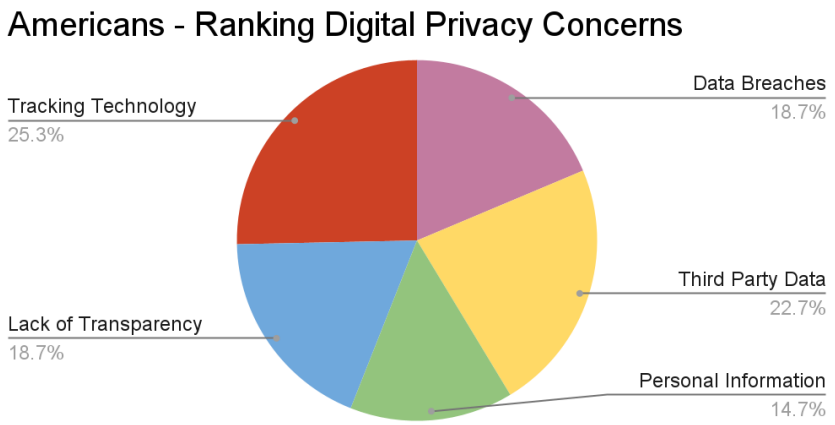
Opinions on Digital Privacy

This section explores consumer opinions of digital privacy in the United States and Japan by measuring the agreement of a definition and revealing the ranking of related concerns.

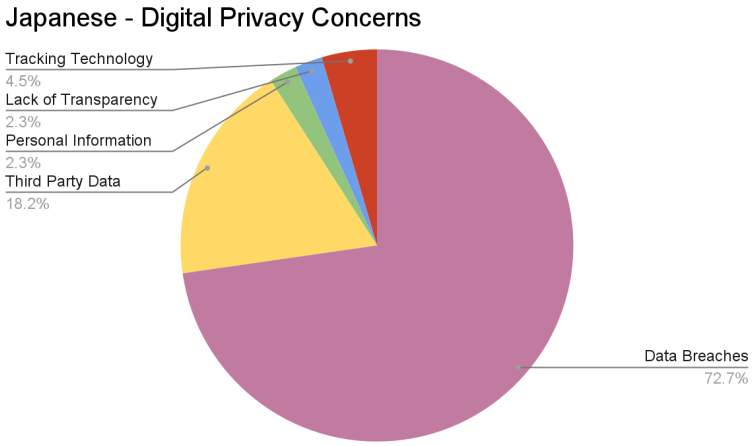
Question 4 measures the agreement of this statement, “Digital Privacy is the protection of one’s personal information which is used and gathered by a device connected to the Internet. Do you agree with this definition of digital privacy?” Responses were collected from N=48 Japanese respondents and N=75 American respondents.

An independent two-sample t-test showcased that there was not a significant difference in the views of this statement between the Americans (M = [5.84], SD = [1.19]) and Japanese participants (M = [5.88], SD = [0.98]); 0.1704(121) = t-value, p = 0.8649. It is clear that both subject groups agreed with this definition of digital privacy.

Question 5: “Please select a digital privacy concern that bothers you.” The two graphs below represent the digital privacy concerns that bother each group the most. Responses were collected from N=44 Japanese respondents and N=75 American respondents.



Within this ranking, tracking technology was determined to be the American consumers' highest concern. Third party data collection found itself in second place while lack of transparency and data breaches were tied for third. Labeled as the least digital privacy concern comes personal information consent/accessibility.



Japanese respondents did not share the same sentiment towards certain privacy concerns. It is clear that the highest concern of the Japanese community is data breaches, understandably so, due to its frequent occurrence, despite an existing consumer data protection law. In 2021, it was reported by Nippon.com that "incidents of leakage or loss of personal information at Japanese listed companies and their subsidiaries in 2021 increased by 34 over the previous year to 137, involving the information on 5,749,773 individuals."[65] Out of 44 respondents, 18% found themselves concerned with third party data collection while 4.5% found tracking technology a problem. Tied at 2.3% are the privacy concerns, lack of transparency and personal information collection consent/accessibility.

It was found that American participants share an equal, diverse perception of data privacy concerns. It was also found that Japanese consumers share a broad unity of data concerns based on previous experiences (covered in the Applied Examples section).

[65] "Over 5 Million Individuals' Information Leaked or Lost in Japan in 2021." 2022. Nippon.com. February 9, 2022. https://www.nippon.com/en/japan-data/h01241/.

Implementations

Question 6 measured agreement with this statement: "I trust that my personal data is secured and protected – whether this is by law or company measures." Responses were collected from N=46 Japanese respondents and N=75 American respondents.

There was not a significant difference in the views of this statement between the Americans (M = [3.73], SD = [1.50]) and Japanese participants (M = [3.80], SD = [1.51]); 0.2518(119) = t-value, p = 0.8016. Their similar responses demonstrate that enough participants on both sides agree, feel neutral, and disagree with this statement and the current data protection measures that exist today.

Similar to Question 6, Question 7 measured agreement with this statement: "I am aware of Japan's/the United States' current data protection laws/legislation." Responses were collected from N=47 Japanese respondents and N=75 American respondents.

Both subject groups, Americans (M = [3.05], SD = [1.67]) and Japanese participants (M = [3.36], SD = [1.66]); 0.9956(120) = t-value, p = .0.3215, expressed a lack of awareness of current data protection laws which resulted in the difference being considered not statistically significant. It was Japanese consumers who had a slightly higher awareness of data protection laws.

Question 8 asked participants their agreement with this statement: "National/Federal consumer data protections can/should be improved upon." Responses were collected from N=46 Japanese respondents and N=75 American respondents.

This time, there was a very significant difference in the views of this statement between the Americans (M = [6.07], SD = [1.09]) and Japanese participants (M = [5.46], SD = [1.28]); 2.7916(119) = t-value, p =0.0061. It was discovered that American consumers find that consumer data protection laws should be improved upon. Although Japanese consumers also hold this sentiment, it was imminent that it wasn't to the same degree as the other target group.

Question 9 measured the agreement with this statement, "Apps and companies do a good job of making their privacy and data collection & usage policies transparent and easily accessible to consumers." Responses were collected from N=46 Japanese respondents and N=74 American respondents.

It was found that Americans (M = [3.49], SD = [1.53]) and Japanese participants (M = [4.35], SD = [1.30]); 3.1713(118) = t-value, p = 0.0019 share different views on this statement. The difference is considered to be very statistically significant. This is because the American subject pool leaned more towards the idea that companies and apps do not do a good job of making their

privacy and data collection & usage policies transparent while the Japanese subject pool felt the opposite.

To summarize, the questions pertaining to defining digital privacy, how secure consumers feel about their personal data being protected, and the knowledge of existing data protection laws was shown to have no significant difference in responses. It was identified that American and Japanese consumers did show differences when discussing the improvement of laws and the company-based protection measures that are practiced today. The existing legal and regulatory framework in these two countries seem to have influenced the views and perceptions of consumers related to digital privacy protections.

American and Japanese Current Laws

In the past decade, there has been an increased use of big data analytics and awareness of privacy concerns among consumers, policy makers, and some legal scholars. This increased awareness, and the rapid growth of personal data collection points to the need for a re-examination of consumer data privacy protections, government regulations and enforcement, company-based initiatives, and the role of consumer advocacy, if any, in protecting personal information. In this section, I explore the legal implications behind modern marketing practices and data usages in the United States and Japan.

United States

Currently, the U.S. does not have a federal consumer privacy protection law, although many individual states have developed their own comprehensive legislation.[66] Existing data protection laws are sector-based, including but not limited to "telecommunication, health services, financial institutions, credit information, and marketing."[67]

The American Data Privacy Protection Act (ADPPA)[68] - an upcoming comprehensive federal data privacy law - is under development. In 2022, the House Energy and Commerce Committee passed the ADPPA on bipartisan support, 53-2 vote.[69] Despite its passing, it hasn't been to the floor of Congress, as some senators worry that the federal privacy law will remove strong protections, such as the ones under the California Consumer Privacy Act (CCPA)[70]. The ADPPA establishes consumer data protections, including "the right to access, correct, and delete personal

[66] Ramirez, Noah. 2019. "What You Need to Know about Data Privacy Laws | Osano." Osano. October 3, 2019. https://www.osano.com/articles/data-privacy-laws.
[67] Ibid
[68] H.R.8152 - American Data Privacy and Protection Act 117th Congress (2021-2022)
[69] Ng, Alfred. 2023. "The Raucous Battle over Americans' Online Privacy Is Landing on States." POLITICO. February 22, 2023. https://www.politico.com/news/2023/02/22/statehouses-privacy-law-cybersecurity-00083775.
[70] CA Civ Code § 1798.192 (2018)

data."[71] It also requires companies to implement security practices to protect consumers, offer an opt out opportunity, prohibits using data to discriminate based on specific characteristics, etc.[72] The enforcement of the ADPPA falls under the Federal Trade Commission (FTC) and state attorney generals. The Federal Trade Commission (FTC) serves as an enforcement agency to protect consumers under the Federal Trade Commission Act (FTC Act).[73] The FTC Act "has broad jurisdiction over commercial entities under its authority to prevent unfair or deceptive trade practices."[74]

Japan

Here, I will identify the legal authority for consumer data protections in Japan. The National Diet, the Japanese Parliament, and the Personal Information Protection Commission (PPC) work together to propose, approve, and enforce laws that protect the privacy of Japanese citizens.[75] The PPC "protects the rights and interests of individuals while taking into consideration proper and effective use of personal information."[76]

This agency serves as the main enforcer of the Act on the Protection of Personal Information (APPI),[77] a detailed ruling that is updated and revised every three years.[78] The aims of the APPI are to strengthen the rights of data subjects, increase the Privacy Information Handling Operator (the "PIH Operator")'s obligations, toughen the penalties for non-compliance and violations of a PPC order and fine, and require a data breach report be sent to the PPC.[79]

Under this legislation, companies have a responsibility to notify consumers the purposes of use of their information, report data breaches to both the PPC & consumers, follow rules regarding data subjects' 'retained personal data', abide by provisions that exist – the collection of sensitive and provision of personal data to third parties, and commit to a following a proper overseas transfer of personal data.

---

[71] Pallone, Frank. 2022. "H.R.8152 - 117th Congress (2021-2022): American Data Privacy and Protection Act." www.congress.gov. July 20, 2022. https://www.congress.gov/bill/117th-congress/house-bill/8152.
[72] Ibid
[73] Act on the Protection of Personal Information (Act No. 57 of 2003)
[74] Ramirez, Noah. 2019. "What You Need to Know about Data Privacy Laws | Osano." Osano. October 3, 2019. https://www.osano.com/articles/data-privacy-laws.
[75] "Roles and Responsibilities |PPC Personal Information Protection Commission,Japan." n.d. www.ppc.go.jp. https://www.ppc.go.jp/en/aboutus/roles/.
[76] Ibid
[77] Act on the Protection of Personal Information (Act No. 57 of 2003)
[78] Tanaka, Hiroyuki, Naoto Obayashi, and Noboru Kitayama. 2020. "Analysis of Cabinet of Japan's Approved Bill to Amend APPI." Iapp.org. International Association of Privacy Professionals. March 18, 2020. https://iapp.org/news/a/analysis-of-japans-approved-bill-to-amend-the-appi.
[79] Ibid

In addition to those legal and enforcement agencies, the Japan Fair Trade Commission (JFTC)[80] also acts against personal data abuses as operations constitute "the abuse of an advantageous position,"[81] a violation under the Anti-Monopoly Law.[82]

It is clear that the United States and Japan both have different legal and enforcement measures in place to protect the data and privacy of consumers. These differences, along with any gaps in consumer privacy protections, play a role in contributing to some of the digital privacy breaches and abuses identified in the examples provided earlier in this paper. Such differences influence the perceptions of consumers, and how businesses and marketers, ultimately, rebuild and maintain, and enhance consumer trust and safety.

Discussion and Potential Future Research Opportunities

The exploration of American and Japanese consumers' concerns about digital privacy and the review of data privacy abuses demonstrate the rapidly expanding use and misuse of technological advances. These innovations are at the center of the intersection between modern marketing practices, digital privacy and data protection, and consumers' constantly changing perceptions.

In conclusion, the degree to which the interest of consumers is protected is dependent on whether the legal and regulatory framework, including enforcement, is weak or robust. It is the responsibility of businesses to be mindful of public sentiment and to always work towards data literacy and security. The survey respondents indicated many similarities and a few differences in their perceptions of digital privacy and the effectiveness of legal enforcement and other interventions on behalf of consumers. Although it was overwhelmingly clear that privacy concerns exist and that appropriate entities should work towards alleviating these issues.

Potential future research includes diving deeper into demographics differentiations (age, sex, gender, occupation, etc.) to see if they play a role in a consumers' perception of digital privacy. For example, professionals from various industries may hold similar or different views on this topic based on their interactions/experiences. While this study touched upon a multitude of digital concerns, subsequent research could focus on one or more specific concerns. Another potential future research topic would be exploring which countries have the best consumer protections laws and why they are considered stronger in the way they protect consumer data and privacy. This might also include whether these countries have experienced some of the data

[80] The Japan Fair Trade Commission (JFTC) is responsible for regulating economic competition and enforcing the Antimonopoly Act.

[81] "Editorial: Rikunabi Scandal Highlights Risks of Exploitation of Personal Data: The Asahi Shimbun: Breaking News, Japan News and Analysis." The Asahi Shimbun. August 13, 2019. https://www.asahi.com/ajw/articles/13061507#:~:text=The%20Rikunabi%20scandal%20has%20raised.

[82] Act on Prohibition of Private Monopolization and Maintenance of Fair Trade (Act No. 54 of 1947)

breaches and abuses discussed here and what factors consumers from these countries consider are essential and necessary. While also discovering that countries previous digital privacy abuse experience and the citizens viewpoints.

Conclusion

With technological advancements and the increasing concerns about how data is being collected, stored and used, the focus of this research was to explore the perceptions of modern marketing and the potential dangers for abuse and misuse of personal information. These issues are relevant to businesses who want to support best practices for ensuring consumer privacy and maintaining consumer trust. It is also important for government regulators to remain aware of consumer concerns and make an effort to modify and expand the legal and regulatory framework for consumer data and digital privacy. Finally, it is important for consumer advocacy groups to remain vigilant in light of consumer complaints and experiences, which can be largely monitored by studies and consumer perception surveys and a compilation of actual consumer personalized experiences.

References

Allen, Richard. “Types of Big Data: Understanding & Interacting with Key Types SelectHub. https://www.selecthub.com/big-data-analytics/types-of-big-data-analytics/.

Armstrong, Sarah, Dianne Esber, Jason Heller, and Bjorn Timelin. “Modern Marketing: What It Is, What It Isn’t, and How to Do It.” McKinsey & Company. McKinsey & Company, March 2, 2020. https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/modern-marketing-what-it-is-what-it-isnt-and-how-to-do-it.

Bryan, Kristin L. “Ed Tech Company’s Four Data Breaches in Three Years Leads to FTC Enforcement Action.” *The National Law Review*, 4 Nov. 2022, www.natlawreview.com/article/ed-tech-company-s-four-data-breaches-three-years-leads-to-ftc-enforcement-action.

Cardozo, Larc, et al. *Why VIZIO’s Settlement with the FTC Matters Why VIZIO’s Settlement with the FTC Matters*. 2017.

Cyphers, Hinako Sugiyama, Katitza Rodriguez, and Bennett. 2021. “Japan’s Rikunabi Scandal Shows the Dangers of Privacy Law Loopholes.” Electronic Frontier Foundation. May 12, 2021. https://www.eff.org/deeplinks/2021/05/japans-rikunabi-scandal-shows-dangers-privacy-law-loopholes.

“Editorial: Rikunabi Scandal Highlights Risks of Exploitation of Personal Data: The Asahi Shimbun: Breaking News, Japan News and Analysis.” The Asahi Shimbun. August 13, 2019. https://www.asahi.com/ajw/articles/13061507#:~:text=The%20Rikunabi%20scandal%20has%20raised.

Evolution, Marketing. 2020. “Tackling Data Privacy Issues in a Data-Driven Marketing World.” www.marketingevolution.com.August 14, 2020. https://www.marketingevolution.com/knowledge-center/data-privacy-issues-in-data-driven-marketing.

Fair, Lesley. “Multiple Data Breaches Suggest Ed Tech Company Chegg Didn’t Do Its Homework, Alleges FTC.” *Federal Trade Commission*, 31 Oct. 2022, www.ftc.gov/business-guidance/blog/2022/10/multiple-data-breaches-suggest-ed-tech-company-chegg-didnt-do-its-homework-alleges-ftc.

Gilbert, Ben. 2022. “Facebook Blames Apple after a Historically Bad Quarter, Saying IPhone Privacy Changes Will Cost It $10 Billion.” Business Insider. February 3, 2022. https://www.businessinsider.com/facebook-blames-apple-10-billion-loss-ad-privacy-warning-2022-2#:~:text=Facebook%20blames%20Apple%20after%20a.

Jopus編集部. n.d. “Rikunabi｜a Perfect Guide to Get Jobs and Work in Japan – Jopus.” A Perfect Guide to Get Jobs and Work in Japan – Jopus. https://jopus.net/en/jobboard/rikunabi.

Leswing, Kif. 2022. “Facebook Says Apple IOS Privacy Change Will Result in $10 Billion Revenue Hit This Year.” CNBC. February 3, 2022. https://www.cnbc.com/2022/02/02/facebook-says-apple-ios-privacy-change-will-cost-10-billion-this-year.html.

Ng, Alfred. 2023. “The Raucous Battle over Americans’ Online Privacy Is Landing on States.” POLITICO. February 22, 2023. https://www.politico.com/news/2023/02/22/statehouses-privacy-law-cybersecurity-00083775.

McMeley, Christin S., et al. “The Real Takeaway from VIZIO’s Privacy FTC Settlement | Davis Wright Tremaine.”www.dwt.com, Oct. 2017, www.dwt.com/blogs/media-law-monitor/2017/10/the-real-takeaway-from-vizios-privacy-ftc-settleme.

Murphy, Kathleen A. "Recent FTC regulation of the Internet of Things." *Bus. LAw.* 73 (2017): 289.

Olano, Gabriel. 2023. “Aflac and Zurich Japan Businesses Hit by Data Breaches.” www.insurancebusinessmag.com. January 12, 2023. https://www.insurancebusinessmag.com/asia/news/cyber/aflac-and-zurich-japan-businesses-hit-by-data-breaches-432564.aspx.

“Over 5 Million Individuals’ Information Leaked or Lost in Japan in 2021.” 2022. Nippon.com. February 9, 2022. https://www.nippon.com/en/japan-data/h01241/.

Pallone, Frank. 2022. “H.R.8152 - 117th Congress (2021-2022): American Data Privacy and Protection Act.” www.congress.gov. July 20, 2022. https://www.congress.gov/bill/117th-congress/house-bill/8152.

Ramirez, Noah. 2019. “What You Need to Know about Data Privacy Laws | Osano.” Osano. October 3, 2019. https://www.osano.com/articles/data-privacy-laws.

“Roles and Responsibilities |PPC Personal Information Protection Commission,Japan.” n.d. www.pc.go.jp. https://www.ppc.go.jp/en/aboutus/roles/.

Tanaka, Hiroyuki, Naoto Obayashi, and Noboru Kitayama. 2020. “Analysis of Cabinet of Japan’s Approved Bill to Amend APPI.” Iapp.org. International Association of Privacy Professionals. March 18, 2020. https://iapp.org/news/a/analysis-of-japans-approved-bill-to-amend-the-appi.

"Two Insurers in Japan Suffer Major Data Breach." 2023. Business Insurance. January 11, 2023. https://www.businessinsurance.com/article/20230111/STORY/912354813/Two-insurers-in-Japan-suffer-major-data-breach.

"What Is IDFA & Marketing without Identifier for Advertisers?" n.d.www.epsilon.com. https://www.epsilon.com/us/insights/trends/idfa#:~:text=The%20Identifier%20for%20Advertisers%20.

Table of Authorities

United States

CA Civ Code § 1798.192 (2018) - California Consumer Privacy Act

Federal Trade Commission Act, Section 5 (FTC Act) (15 USC §45): Unfair or Deceptive Acts

H.R.8152 - American Data Privacy and Protection Act 117th Congress (2021-2022)

Japan

Act on Prohibition of Private Monopolization and Maintenance of Fair Trade (Act No. 54 of 1947)

Act on the Protection of Personal Information (Act No. 57 of 2003)

Bibliography

Edelman, Gilad. 2022. "Congress Might Pass an Actually Good Privacy Bill." Wired. July 21, 2022. https://www.wired.com/story/american-data-privacy-protection-act-adppa/.

LLP, Hunton Andrews Kurth. 2023. "House Energy & Commerce Subcommittee Holds Hearing on U.S. Privacy Law." Privacy & Information Security Law Blog. March 3, 2023. https://www.huntonprivacyblog.com/2023/03/03/house-energy-commerce-subcommittee-holds-hearing-on-u-s-privacy-law/.

Newberry, Christina. 2022. "Social Media Data Collection: Why and How You Should Do It." Social Media Marketing & Management Dashboard. January 24, 2022. https://blog.hootsuite.com/social-media-data-collection/.

Appendices

Appendix A (Connection between my research and the WSP Program)

My self-designed major is International Marketing with a concentration in East Asia, combining political science/law, business marketing, consumer psychology, data science, and history. Through the Whittier Scholars Program, I have also pursued a minor in East Asian languages. Combining this minor and these major disciplines creates a breadth of knowledge applicable to International Marketing. I have identified key concepts and the touchstones that form the foundation for the work of this project. I briefly describe each below as cumulatively, these touchstones provided the basis for furthering my exploration of these modern, cross-cultural marketing practices.

East Asian History: Cognizance of East Asian history, religion, and literature in addition to the review of a country's political/legal background provides better understanding of how and why some East Asian countries are as powerful and influential as they are today. I have been able to enhance my immersion into East Asian cultures from courses taken at Whittier College and my study abroad experience at J.F Oberlin University, Tokyo, Japan. This insight is beneficial for building relationships and creating successful marketing campaigns overseas.

Consumer Psychology: Understanding the wants and needs of a consumer base is key for effective marketing campaigns and maximum profits. Employing a cultural lens can aid in understanding the motivations of consumers.

Business, Marketing: Knowing general marketing practices/strategies provides the theoretical basis for my major.

Data Science: Utilization of data is a common practice for companies to better market themselves. Possessing both the technical and analytical skills required to synthesize consumer data brings awareness to consumer habits. This reveals the effectiveness of an ad campaign, the purchasing patterns and decisions of consumers, and other factors that inform companies how to adapt to its market. As this is a newer practice, data collection brings up ethical concerns.

Communication: Beyond historical knowledge, business strategies, and data analysis, the ability to communicate is a vital component of my major and minor. Studying abroad in Japan provided me with opportunities to immerse in local culture and engage with individuals from my region of study. These micro and macro interactions allowed me to gain better insight into cultural mindsets.

Appendix B (American Survey Questions)

1) Age

2) Nationality
   Japanese
   Other

3) How active are you online daily?
   Less than an hour
   1-4 hours
   5-8 hours
   More than 8 hours

4) Digital Privacy is the protection of one's personal information which is used and gathered by a device connected to the Internet. Do you agree with this definition of digital privacy?

5) Please select all of the digital privacy concerns that bother you.
   Data Breaches
   Third Party Data Collection
   Personal Information Consent/Accessibility
   Lack of Transparency
   Tracking Technology

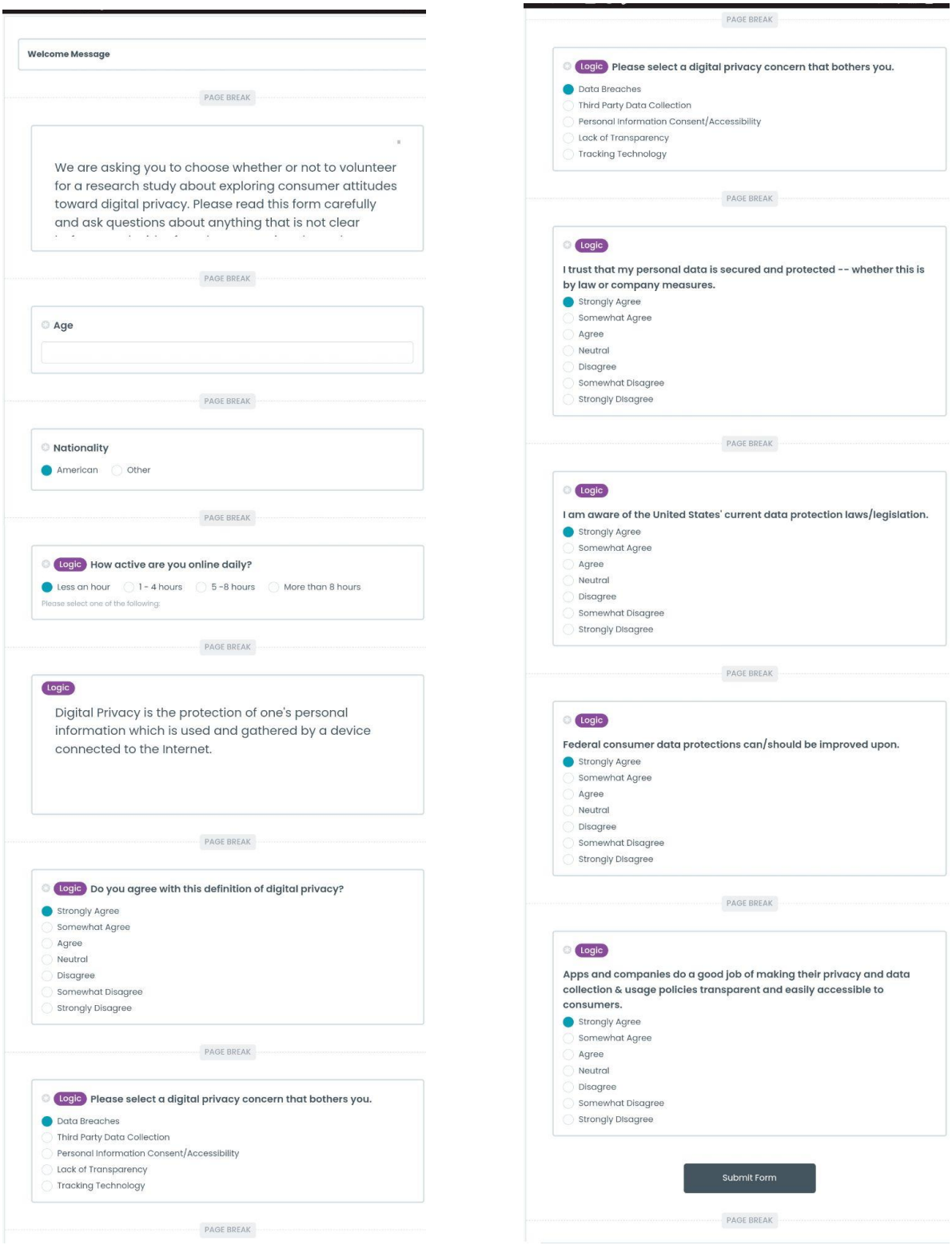
6) I trust that my personal data is secured and protected – whether this is by law or company measures.

7) I am aware of Japan's current data protection laws/legislation.

8) National consumer data protections can/should be improved upon.

9) Apps and companies do a good job of making their privacy and data collection & usage policies transparent and easily accessible to consumers.

Appendix C (Screen Capture of American Survey)



Appendix D (Japanese Survey Questions)

1) 年齢

2) 国籍
日本国籍
その他

3) あなたは毎日どのくらいネットを利用していますか？
1時間未満
1-4時間
5-8時間
8時間以上

4) デジタル・プライバシーとは、インターネットに接続されたデバイスで使用・収集される個人情報の保護です。このデジタル・プライバシーの定義に同意しますか？

5) デジタル・プライバシーに関する懸念事項のうち、あなたを悩ませるものをすべて選択してください。
データ流出
第三者によるデータ収集
個人情報の同意／アクセシビリティ
透明性の欠如
トラッキング技術

6) 私は、自分の個人情報が法律や会社の施策によって安全に保護されていることを信頼しています。

7) 私は、日本の現在のデータ保護法／法律を理解しています。

8) 日本の消費者データ保護は改善される可能性がある／されるべきだと思う。

9) アプリや企業は、自社のプライバシーやデータ収集・利用方針を透明化し、消費者が容易にアクセスできるようにするために、良い仕事をしている。

Appendix E (Screen Capture of Japanese Survey)