Journal of Computer Information Systems

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/ucis20

Online Privacy Policy Disclosure: An Empirical Investigation

Yabing Jiang & Thant Syn

To cite this article: Yabing Jiang & Thant Syn (2022): Online Privacy Policy Disclosure: An Empirical Investigation, Journal of Computer Information Systems, DOI: 10.1080/08874417.2022.2095542

To link to this article: https://doi.org/10.1080/08874417.2022.2095542

Published online: 14 Jul 2022.

JOURNAL OF COMPUTER INFORMATION SYSTEMS
https://doi.org/10.1080/08874417.2022.2095542

Taylor & Francis
Taylor & Francis Group

Online Privacy Policy Disclosure: An Empirical Investigation

Yabing Jiang and Thant Syn

Florida Gulf Coast University, Fort Myers, Florida, USA

ABSTRACT
While companies' privacy policies inform consumers about their privacy practices, their adherence to regulations and Fair Information Practices (FIP) may vary widely. We develop and apply an extended checklist to examine the privacy practices of companies with a higher privacy and data security risk. We find that industry sector has a significant effect on companies' privacy practice. Specifically, companies in the non-regulated communication services sector complied to FIP better than those in the regulated financial sector, indicating that the FTC' self-regulation approach works, at least for the examined sector. While 67% of companies fully complied to the Security principle, they were not doing enough in full specification of Enforcement in their privacy policies, indicating that regulators need to strengthen enforcement provision in regulations and develop and enlist various enforcement mechanisms. Overall, this research informs legislation and the public on the effectiveness of self-regulation and government regulation.

KEYWORDS
Privacy policy; privacy practices; information privacy; fair information practices

Introduction

In 2019, more than 56% of the world's population and about 89% of the U.S. population were Internet users.[1] People use the Internet for various activities, such as searching, shopping, banking, communicating, entertaining, or learning. During the course of these activities, various organizations collect and use our personal information (PI) to facilitate the services we consume. Sometimes, we are cognizant of what PI is collected and how it is used. Some other times, our PI is collected, used, or shared without our knowledge or consent.[2] Facebook shared personally identifiable information of more than 87 million users to the political consulting firm Cambridge Analytica without users' consent.[3] High-profile incidents like these appear to have heightened consumers' privacy concerns.

The exponential growth of social media and networking platforms is one of the major drivers of privacy concerns. The growing importance of this segment of industries is unmistakable. In September 2018, the Global Industry Classification Standard (GICS) created the Communication Services (CS) sector to replace the former Telecommunication Services sector. GICS, jointly developed by MSCI Inc. and S&P Global, is a widely accepted classification of companies and industries. This change was designed to "reflect the evolving nature of the U.S. economy over the last two decades."[4] As a result, a few thousands of stocks were being reclassified. For example, three of the FANG stocks, Facebook, Inc., Alphabet, Inc., and Netflix, Inc., were reclassified into this new sector. GICS further classified the first two FANG stocks into a new sub-industry, Interactive Media & Services (IMS). Companies in this newly defined sub-industry, including search engines, social media and networking platforms, and online review companies, mostly generate revenue from digital products and services. This is a new and fast-growing industry, which primarily deals with users' personal data for digital advertising. Due to the business nature of this industry and its prevalence in the society, the privacy practices of companies in this group have profound impacts on users' daily lives and yet they are less studied in the Information System (IS) literature.

Consumers' concern over the collection and use of their information by various companies can be highly undesirable to the companies. Privacy concerns are found to have negative impacts on their engagement with companies.[5] Privacy concerns can also hinder one's willingness to adopt or use a technology even when the benefits of use clearly outweigh the costs. One such scenario played out in public health during the recent COVID-19 pandemic. The general public's concerns over the collection and use of sensitive data by contact tracing apps were a major barrier for many people to download and use potentially life-saving apps in France, Australia, and the U.S.[6]

CONTACT Yabing Jiang ✉ yjiang@fgcu.edu Department of Information Systems & Operations Management, Florida Gulf Coast University, Fort Myers, Florida, USA

To mitigate consumers' privacy concerns and improve their trust, organizations often delineate their privacy practices in online privacy policies. Such policy documents are an important source for consumers to learn what are in companies' privacy policies, what are their rights, and what actions are taken by companies to protect data collected from them. Governments and regulators around the world have also taken steps to protect the privacy of consumers. Some privacy regulations, such as European Union's (EU) General Data Protection Regulation (GDPR)[7] and California Consumer Privacy Act (CCPA)[8] include provisions that require companies to disclose their privacy practices. All privacy regulations in general require the disclosure of privacy or information-sharing practices to customers, following the Federal Trade Commission's (FTC) Fair Information Practices (FIP) principles. FIP principles delineate a company's privacy practices in five categories: notice/awareness, choice/consent, access/participation, security/integrity, and enforcement/redress.[9–12] Although most companies, regulated or not, have posted privacy policies online, their adherence to FIP principles may vary widely.[13–15]

In this paper, we take the first step to examine the online disclosure of privacy policies by companies in the newly defined IMS sub-industry. Additionally, we compare the privacy policies and practices of these companies with those in the highly regulated Financials (FIN) and Health Care (HC) sectors. Companies such as MSCI Inc. and Sustainalytics have developed ESG Rating models to assess companies based on their exposure and resilience to environmental, social, and governance (ESG) risk, and Privacy and Data Security (PDS) is one of the key issues assessed in the ESG framework. Companies selected for this study are from sub-industries that have a higher PDS risk as identified by the MSCI ESG rating model. However, since the selected companies in FIN and HC sectors are also governed by regulations, it is important to learn whether the privacy practices of companies in the IMS sub-industry measure up to those that are regulated.

In this study, we are interested in learning whether self-regulation works. The research questions we want to address are the followings. To what extent companies comply with the FIP and whether companies' privacy practices differ across industry sectors. Do companies in the non-regulated sectors comply with FIP equally compared to those in the government regulated sectors? The objectives of this research are manifold. First, we develop an integrated framework for assessing firms' privacy policy compliance with FIP principles. We incorporate in the framework additional web content and design features, assessing firms' privacy practice that goes beyond the basic FIP compliance. Second, we apply the framework to examine the privacy practices of firms in the government regulated FIN and HC sectors as well as firms in the newly classified, unregulated IMS sub-industry, which includes many new businesses, such as search engines and social media platforms. Third, we compare these firms' privacy policies and their online disclosure to understand the current state of privacy practice in these sectors and discover differences across sectors. Forth, we compare findings from this research with prior studies to identify trends and changes over the years. By examining additional content and design factors as part of the assessments of firms' privacy practices, we discover additional areas of privacy practice for improvement. Overall, this research informs legislation and the public on the effectiveness of self-regulation and government regulation.

The remainder of the paper is organized as follows: First, we review the relevant literature on information privacy, FIP and regulations, and prior studies on privacy policy disclosure. Next, we explain the research framework, including our checklist for privacy policy compliance. We then describe the data collection and hypotheses in the research method section. We discuss the results of the analysis in the following two sections. The paper concludes with the discussion on the implications of the findings on policymakers and on future information privacy research.

Literature review

Information privacy and consumer privacy concerns

Privacy is a multifaceted concept. It intersects multiple dominions and disciplines, most notably, philosophy, psychology, sociology, economics, legal, marketing, and IS. Information privacy is concerned with individuals' PI. It is often considered a subdomain of the general privacy in contrast to the physical privacy, which is concerned with individuals' physical private space or surroundings.[16] The general privacy is variably defined as either value- or cognate-based. The former defines privacy as individuals' right or commodity whereas the latter conceptualizes privacy as a construct related to mind, perceptions, and cognition of individuals. Some disciplines naturally prefer one definition over the other; for instance, the legal domain predominantly considers privacy as individuals' right in a society. Some other disciplines like IS study privacy through various lens encompassing both value- and cognate-based definitions. In the IS literature, the information privacy which is also often referred to as personal information privacy (PIP) denotes individuals' desire to have some control over their PI.[17,18]

Privacy concerns and to a larger extent the concept of information privacy coevolve with IT/IS over time.[16] The prevailing macro-research model on information privacy called Antecedents–Privacy Concerns–Outcomes (APCO)[16] and later extensions[19] suggests that individuals' privacy concern impacts their privacy-related behaviors. However, research has shown that there is a significant gap between users' privacy concern and their behavior in allowing companies to collect their personal data. On the one hand, the majority of users are concerned with how companies are making use of their data. On the other hand, more and more users are willingly allowing companies to collect increasing amount of personal data to use popular online services that seems to suggest that users are downplaying their privacy concerns. The dichotomy between users' attitude and behavior toward privacy of their data is known as privacy paradox.[20,21]

FIP and related regulations

FIP are a set of principles that are intended to protect the privacy of personal data collected by organizations. It is one of the earliest meaningful efforts to protect the privacy of consumers by the FTC in the U.S. It also serves as the foundation for subsequent privacy protection measures, such as the US Privacy Act of 1974[22] and Guidelines for the Protection of Privacy and Transborder Flows of Personal Data by the Organization for Economic Cooperation and Development (OECD).[12] The five main tenets of FIP include Notice, Choice, Access, Security, and Enforcement.[9,10,12,23,24] In short, FIP urge data collectors to a) disclose their information practices, b) obtain consent from people, c) give people access to their data, d) have reasonable safeguards in place to protect the collected data from unauthorized use and access, and e) implement enforcement mechanisms to uphold the policy.

Although FIP are considered as the recommended privacy guidelines, they permeate into privacy regulations and legislations across the world. Prominent examples include GDPR that enforces data privacy for EU citizens and CCPA that protects the privacy of the residents of the state of California. In the U.S., there are FIP-inspired regulations and legislations for specific industries such as the Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA).

HIPAA's Privacy Rule introduced in 1999 and finalized in 2002 specifically dictates individuals' right to know and control how their protected health information (PHI) is used by covered entities, including health-care providers, health plans, health-care clearinghouses, and their business associates. Safeguarding PHI is also mandated in the Security Rule of HIPAA. The purpose of HIPAA is to balance the privacy and security of individuals' information against the quality of health care enabled by sharing of information among covered entities. The increasing use of Electronic Health Records (EHR) and Electronic Medical Records (EMR) in health care, notably promoted by the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009, necessitates the regulation and assurance provided by HIPAA. Since April 2003, the compliance with the Privacy Rule has been required at all covered entities.[25]

The specific provision of GLBA that is concerned with privacy is the Privacy of Consumer Financial Information or Privacy Rule. It lays out the use and disclosure of nonpublic personal information (NPI) of consumers by financial institutions that engages in a wide range of financial activities. The Safeguards Rule requires financial institutions to develop, implement, and maintain suitable information security programs to protect consumer's financial information.

The CCPA regulations apply to "for-profit businesses that do business in California and meet any of the following: Have a gross annual revenue of over $25 million; Buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices; or Derive 50% or more of their annual revenue from selling California residents' personal information."[8] The CCPA went into effect on August 14, 2020. The regulations require companies to give consumers certain notices explaining their privacy practices, such as consumers' privacy rights and how to exercise them. The CCPA gives California consumers more control over the PI that businesses collect about them, including consumers' Right to Know, Right to Delete, Right to Opt-Out of Sale, and Right to Nondiscrimination.[8]

Table 1 summarizes the implementation of FIP principles in various regulations and legislations. All privacy regulations, to varying extents, cover four major FIP principles – Notice, Choice, Access, and Security. Most regulations do not, however, provide specific information on enforcement mechanisms that companies should implement. GDPR can be considered as the most significant privacy regulation that is enforced by national governments. It comprehensively covers

Table 1. FIP principles in privacy regulations.

FIP Principles	GDPR	CCPA	HIPAA	GLBA
Notice Businesses should provide notice of what information they collect from consumers and how they use it.	Organizations are required to inform users what information about them is collected, what it is used for, how long it will be retained, and whom it will be shared with and when.	California residents have the right to know what type or specific personal information collected, used, shared/sold. Business must provide notice to residents at or before data collection. Businesses must disclose financial incentives from selling personal information.	Covered entities must provide notice of privacy practices to individuals.	Financial institutions must provide customers notice of privacy policies and practices. Institutions must also detail the conditions to disclose NPI.
Choice Consumers should be given choice about how information collected from them may be used.	Users or individuals have the right to deny consent for processing their data by organizations. They can also object specific use of their data by organizations and request their data be deleted. However, the right to deny consent and erasure is not absolute.	California residents have the right to opt-out of sales of their information. Businesses must obtain opt-in consent from residents under the age of 16 or from consenting adult for children under 13.	Covered entities can use or disclose PHI without individuals' authorization for treatment, payment, health care operations, and public interest use. Individuals can request covered entities to restrict use or disclosure of PHI.	Customers can opt out of disclosure of NPI to nonaffiliated third parties.
Access Consumers should have access to data collected about them.	Organizations are mandated to provide a means to users or individuals to request access to a copy of their data. In addition, organizations must allow users to amend incorrect data and download their data for use elsewhere.	California residents are granted greater access to their personal information. Businesses are mandated to respond to residents' requests to delete their information in a certain timeframe.	Individuals can request to amend inaccurate or incomplete PHI. Covered entities can deny the request under certain circumstances.	Financial institutions are not required to give customers access to collected data.
Security Businesses should take reasonable steps to ensure the security of the information they collect from consumers.	The principle of security dictates that organizations must ensure that data is secured, covering physical and organizational security as well as cybersecurity.	Businesses have the responsibility to protect personal data collected from residents. Principles similar to GDPR's principle of security apply to businesses.	Security Rule requires covered entities to put in place physical, administrative, and technical safeguards to protect PHI.	Safeguards Rule requires financial institutions to develop, implement, and maintain information security programs.
Enforcement Businesses should have an enforcement mechanism to uphold the policy.	No specific provisions on how organizations should enforce or self-regulate privacy violations.	No specific provisions on how businesses should enforce or self-regulate privacy violations. Residents have the right to sue businesses for data breach.	No specific provisions on how covered entities should enforce or self-regulate privacy violations.	No specific provisions on how financial institutions should enforce or self-regulate privacy violations.

information privacy concerns in a significant bloc of countries in Europe. The privacy regulations in the U.S. are more fragmented. HIPAA regulates only healthcare providers and business associates, whereas GLBA regulates financial institutions. CCPA represents the most comprehensive regulation even though it benefits the residents of California only. Companies in FIN and HC sectors are required to be fully complied with GLBA and HIPPA, respectively. Companies that do business in CA and meet the specified criteria are required to fully comply with CCPA. Hence, regulated companies are expected to fully comply with at least the first four FIP, given that there is a lack of specific enforcement provision in each regulation. Table 2 summarizes the abbreviations used in the paper.

FIP and privacy policy disclosure

The FTC and other organizations have conducted several surveys of random samples of general websites and popular U.S. websites to assess their privacy policy disclosures and compliance with FIP from 1998 to 2001.[26] Following the FTC studies, one stream of IS privacy research started to examine organizations' privacy policies for their compliance with the principles and regulations, such as the FTC's FIP, OECD privacy principles, and EU's GDPR.

Privacy policies of the Fortune 500 companies were examined extensively for their compliance with the first four FIP principles.[15,27] Schwaig et al.[15] found that 383 out of the Fortune 500 companies collected PI and posted a privacy policy on their websites, but less than 4% of

Table 2. List of abbreviations.

Abbreviation	Description
APCO	Antecedents–Privacy Concerns–Outcomes
CCPA	California Consumer Privacy Act
CCPN	California Consumer Privacy Notice
CS	Communication Services Sector
EHR	Electronic Health Records
EMR	Electronic Medical Records
ESG	Environmental, Social, and Governance Risks
FANG	Facebook, Amazon, Netflix, and Google
FIN	Financials Sector
FIP	Fair Information Practices
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
GICS	Global Industry Classification Standard
GLBA	Gramm-Leach-Bliley Act
HC	Health Care Sector
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
IMS	Interactive Media & Services Sub-industry
NPI	Nonpublic Personal Information
OECD	Organization for Economic Cooperation and Development
OTC	Over-The-Counter
PDS	Privacy and Data Security
PHI	Protected Health Information
PI	Personal Information
PIP	Personal Information Privacy

them had all of the checked elements regarding the four FIP principles. They also found that companies in different industry sectors exhibited different levels of compliances with FIP, with the hardware, software, and financials sectors outperforming the averages of the Fortune 500 companies on the checked FIP elements. Additionally, information-intensity group complied with FIP better than the non-information intensive group.

Peslak[28] examined the privacy policies of top 50 Fortune companies to check their conformity to five FIP principles. He expanded the ten-item checklist used by the FTC 2000 report to include Enforcement, the fifth FIP principle outlined by FTC. He found that only 16% of the Fortune 50 websites had all 5 FIP principles and 32% provided some type of procedure for privacy policy enforcement. In another study, Peslak[29] examined the compliance with FIP by Forbes international 100 companies. He found that overall, the Forbes international 100 companies did not closely follow the FIP, only 5 companies conformed to all 5 FIP, and only 6 companies enlisted a third-party seal.

Zhang et al.[30] conducted a content analysis on the privacy notices of 125 international companies to identify the cross-culture differences. They also used the FIP as the privacy evaluation criteria and found that Australia companies outperformed peers in China, Japan, U.K, and U.S. on compliance with most of the FIP categories. While there were differences on some privacy policy elements between individualistic and collectivistic cultures, all countries were lacking in the FIP enforcement dimension.

A few recent papers further explored organizations' FIP compliance. Li et al.[14] developed a fourteen-item checklist on all five FIP to evaluate the compliance levels of the Dow Jones 30 companies. They found that while most of the Dow Jones 30 companies complied well with Notice, only three companies conformed to all five principles. Al-Jamal and Abu-Shanab[31] examined the privacy policies of 40 e-government websites. They used a similar fourteen-item checklist and found that nine out of the 14 items were not included in the privacy policies by more than 50% of the countries examined. E-government privacy policies were particularly lacking in the Access and Enforcement dimensions of FIP. New studies have used natural language processing, data mining tool, and crowd sourcing to examine firms' privacy policies[32–36] and to identify improvements that need to be made to meet the requirements of the GDPR.[37,38]

In terms of how to evaluate companies' privacy policies, Al-Jamal and Abu-Shanab[31] found that most studies used the FTC's FIP principles to evaluate companies' privacy practices, and seven out of the eight OECD principles can be matched to the five FIP. Compared to Peslak,[28,29] Schwaig et al.[15] used a fuller checklist that included two to three items for each of the first four FIP principles, and they measured both full and partial compliances to each of the FIP. They did not check for compliance with the Enforcement dimension of FIP, though they used online privacy seal as a measure for advanced disclosure. Li et al.[14] and Al-Jamal and Abu-Shanab[31] each used a fourteen-item checklist on all five FIP principles, and most of the items on the first four FIP were similar to that used in Schwaig et al.[15] Linden et al.[37] and Zaeem and Barber[38] checked privacy policy compliance with only some aspects of GDPR principles and with only one or two specific questions for a principle.

Privacy policies or statements are one mechanism companies employ to alleviate users' privacy concern.[27] It is an important source for consumers to learn companies' privacy practices, what data is collected, how data is used or shared, and how data is protected. Policies that offer greater protection may help increase consumer confidence and online participation. Some studies have found positive effects of privacy policies on users' willingness to share their personal data while other studies have discovered tentative effects on behavior.[39] Since the FTC's initial studies, privacy policy research has found more websites disclose privacy policies and implement core elements of FIP over time. However, only a small percentage of surveyed firms complied to all 4 or 5 FIP elements, which is concerning for both the consumers and regulators. Continued research on privacy policy disclosure is warranted. Assessing contents and effectiveness of firms' privacy policies helps us understand the status of firms' privacy practices, and it informs us whether regulation or the approach of enforcing FIP through self-regulation works and helps us identify areas for improvement.

Research framework

This study extended prior research on privacy policy in multiple ways. First, we updated prior studies by examining the current state of companies' FIP compliance. It has been over 20 years since the FTC 1998 and 2000 studies. During this time, the rapid expansion of Internet has fundamentally changed the landscape of every industry and prompted the creation of new data-driven businesses, such as search engines and social media. Consumers' data are being collected and used in unprecedented ways. It is important and timely to examine the current state of companies' privacy practices so as to inform legislators and the public whether government regulation and industry wide self-regulation are working in protecting consumers' data and privacy.

Second, we developed a 29-item privacy policy checklist, expanding the lists used in prior studies and including items associated with consumers' privacy rights specified in the recent CCPA. Specifically, 20 items in the list are used to check for FIP compliance, and eight of them are associated with CCPA. The remaining nine are content and design features that go beyond the requirements of FIP. Using this extensive checklist, this study provides a fuller picture on companies' privacy practice.

Third, we focused on companies from industries that are exposed to high PDS risk. Prior studies either randomly selected companies[26,37,38] or used the Dow Jones, Forbes, or Fortune company lists.[14,15,28,29] Both approaches included companies that do not collect or handle consumer data due to their business nature or practices. Even for the included companies that do engage in consumer data collection and sharing, some are more information intensive than others. Thus, those studies included companies with different needs in complying with FIP or GDPR and did not provide an accurate picture of FIP compliance for companies with high PDS risk. In this study, we specifically zoomed in on companies in HC, FIN, and CS industries, all of which have business operations that deeply engage in handling consumers' sensitive PI. For the first time, the privacy policies of the newly defined IMS sub-industry are being studied. Consumers are more concerned of their privacy when dealing with these companies, and hence it is important to examine these companies' privacy policy and privacy practice.

Privacy policy compliance checklist

To evaluate companies' privacy practices and the extent to which their privacy policies comply with FIP, we developed a 29-element checklist. Table 3 presents the full checklist, the associated FIP categories, and element coding. The features included in the list are based on prior studies discussed in the literature review section and are expanded to include additional elements. Twenty elements of the list are for FIP compliance, with several items for each FIP principle. Specifically, seven elements are used to access a policy's compliance with the Notice principle, three for Choice, four for Access, two for Security, and four for Enforcement. Eight out of these twenty elements coincide with the CCPA consumer rights, coded in Table 3 CCPA column.

The list also includes nine content and design features of the policy pages as additional features (AFs) that go beyond the FIP compliance. These features provide easy access to the privacy document or various privacy setting (AF1 to AF4), make additional disclosure of relevant information (AF4 to AF7), and help consumers better understand the policy document (AF8 to AF9). We use these AFs as a measure of dedication of firms' privacy practice that goes beyond FIP compliance.

This list checks not only if a company's privacy policy states a practice matching to one of the FIP principles, but also how explicit the policy is in describing the matched practice. That is, using the checklist, we examine both the coverage and degree of specificity of a company's privacy policy to evaluate its compliance with FIP. The AFs in the list further assesses extra efforts that a company exerts in further informing consumers and aiding them to access and understand the disclosed policy.

Research method

MSCI uses industry-specific weights on key ESG issues to derive its widely used ESG ratings on companies, whereas the weights measure the contributions of the corresponding key ESG issues to a company's overall ESG rating. PDS is one of the key issues assessed in the ESG ratings. For this study, we are interested in examining and comparing the privacy policies and the online disclosure of the policies by companies with high PDS risk, specifically in CS, FIN, and HC sectors.

GICS has 11 sectors, and the CS sector has the highest risk weight of 24% on PDS, followed by the FIN sector of 10.3%. For the CS sector, we focus on

Table 3. Privacy policy checklist.

	FIP	CCPA	
FIP Category	Code	Code	Definition
Notice	N1	CA_RtK	The privacy policy states what specific user data will be collected.
	N2	CA_RtK	The privacy policy states the categories of sources from which the user data will be collected.
	N3	CA_RtK	The privacy policy explains why user data will be collected.
	N4	CA_RtK	The privacy policy explains how the collected user data will be used internally.
	N5	CA_RtK	The privacy policy explains whether and how the collected user data will be shared outside the company.
	N6		The privacy policy states how the company will communicate changes to the policy with users.
	N7		The privacy policy states what user data will be retained and for how long.
Choice	C1		The privacy policy states whether users have choices on what data the company can collect and use internally.
	C2	CA_RtOO	The privacy policy states whether users have choices on what collected data the company can disclose to a third party.
	C3	CA_RtNR	The privacy policy states users' right to nondiscrimination for exercising opt-out or other rights.
Access	A1		The privacy policy states whether users are allowed to review the collected data about them.
	A2		The privacy policy states whether users are allowed to export the collected data about them.
	A3		The privacy policy states whether users are allowed to modify the collected data about them to make corrections.
	A4	CA_RtDI	The privacy policy states whether users are allowed to delete all or some of the collected data about them.
Security	S1		The privacy policy states the steps and/or technologies adopted by the company to secure the collected user data.
	S2		The privacy policy states whether the company will prevent unauthorized access to the collected user data.
Enforcement	E1		The privacy policy states whether the company complies with relevant regulations such as California Consumer Privacy Act (CCPA) or others.
	E2		The privacy policy states whether the company will take actions against those who violate its privacy policy.
	E3		The company conducts self-regulation for assurance of privacy standards using one or more third-party providers such as TRUSTe, WebTrust, EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, or BBBOnline.
	E4		The privacy policy page provides contact information for users to file complaints or voice their concerns regarding the policy.
Additional Feature	AF1		One-click from the homepage to the policy page.
	AF2		The privacy policy page provides a link or button to download/print the policy in PDF format.
	AF3		The privacy policy page provides an interactive table of content or highlight/summary of the policy.
	AF4		The privacy policy page provides links to various user privacy settings.
	AF5		The privacy policy page states the effective date of the policy.
	AF6		The privacy policy page provides links to the company's cookies policy page or specifies that it has a cookies policy.
	AF7		The privacy policy page provides a link to the company's California Consumer Privacy Notice page or specifies that it has a California Consumer Privacy Notice policy.
	AF8		The privacy policy page provides explanation of key terms used either as callouts or in a separate section.
	AF9		The privacy policy page provides multiple examples to demonstrate or explain the terms of the policy.

its IMS sub-industry, which has the highest PDS risk weight among all the sub-industries across all sectors. Because the GLBA aims to protect consumer financial privacy, the covered entities are defined as financial institutions that collect NPI from customers.[40] Based on the GICS industry and sub-industry classification, six sub-industries qualify as financial institutions and are studied here. While the PDS risk for the HC sector in general is low (3.4%), the three sub-industries governed by HIPPA all have a much higher risk weight, 25% for Managed Health Care, 19.7% for Health-Care Facilities, and 14.9% for Health-Care Services.[a] Accordingly, these three sub-industries are included in the study. Table 4 lists the studied GICS sub-industries, which are defined in the most recent GICS Methodology.[41]

Data collection

For data collection, we started by selecting a list of companies from each of these three sectors. To obtain a sizable but manageable list, we began with the S&P 500 index, which includes leading companies from major industries of the U.S. equity market. CS, FIN, and HC sectors are included in the index. GICS classifies companies within a sector into industry groups, industries, and then sub-industries. For the FIN sector of the S&P 500 index, there are 65 companies belonging to 13 sub-industries. Only companies in the sub-industries shown in Table 4 were included in this study, resulting 34 companies representing the FIN sector.

For the HC sector of the S&P 500 index, there are 63 companies belonging to 10 sub-industries, but only 3 qualify as the covered entities as shown in Table 4. Since the index only have 11 companies in the selected sub-industries, we expanded the list to include additional companies. We retrieved the list of companies in each of these three sub-industries from the Standard & Poor NetAdvantage (on April 23, 2021), ordered by the measure of market capitalization. All the 11 companies in the S&P 500 index are large cap (with values above $10 billion) and included in the retrieved list. Next, we narrowed down the list to companies that are traded in U.S. equity markets and are either large cap or mid cap (with values between $2 and $10 billion). This resulted in a list of 42 companies. Since the market cap changes with stock price and some of the

[a] Source: MSCI ESG Research LLC. Average Key Issue weights calculated as of Nov 9, 2020.

Table 4. GICS sectors and sub-industries included for this study.

GICS Sector	GICS Sub-Industry
Health Care	35102015 Health Care Services 35102020 Health Care Facilities 35102030 Managed Health Care
Financials	40101010 Diversified Banks 40101015 Regional Banks 40102010 Thrifts & Mortgage Finance 40202010 Consumer Finance 40203010 Asset Management & Custody Banks 40203020 Investment Banking & Brokerage
Communication Services	50203010 Interactive Media & Services

companies had a market cap close to the $2-billion threshold, we further refined the list to select companies with a market-cap of $3 billion and above. This led to 34 companies, representing the HC sector.

For the CS sector of the S&P 500 index, there are 22 companies belonging to 10 sub-industries, but only three companies are in the IMS sub-industry. To expand the list, we retrieved all companies in the sub-industry, traded in the U.S. equity market, from Standard & Poor NetAdvantage. From this list, we removed companies that do not have a wide market presence in U.S. or mostly provide services in non-English languages, and companies that trade over-the-counter (OTC) and do not have a market capitalization value. This resulted in a list of 38 companies, but 5 of them do not have a privacy policy page and were removed as well. Hence, the final list for the CS sector included 33 companies.

The snapshots of the privacy policy pages of the 101 selected companies were collected in the period of April and May of 2021. A company's U.S. website was used to gather the snapshot, that is, only the America version of its privacy policy was studied here. To gather privacy policy data, first, two research assistants participated in a training session, learning what are included in the checklist and how to inspect firms' privacy policy pages to complete the check list. Next, the research assistants individually visited the companies' websites and their privacy policy snapshots to collect the data on the checklist in the period of May and June of 2021. The presence (coded as 1) or absence (coded as 0) of each item in the checklist was recorded. They also checked the number of (mouse) clicks it took to access a company's privacy policy page. Altogether, a total of 2929 items were collected. The research assistants agreed on 83% of the items collected, and they reconciled the differences by jointly re-visiting the policy pages in questions. Table 5 presents the data collection results, showing the descriptive statistics, such as counts (N) and percentages for each item in the checklist by industry sectors and the total.

When collecting privacy policy data from companies' websites, we noticed that some companies have a dedicated California Consumer Privacy Notice (CCPN) page. For this study, we only collected data from a company's privacy policy page, even if it may have a separate CCPN page that applies to California residences. The rationale is that even though the consumer rights specified in CCPA only apply to California residences, incorporating these rights in a company's privacy policy is a good privacy practice that is in alignment with FIP. Thus, the CCPA-index in this study represents how well a company's privacy policy measures up in giving consumers controls over their PI as specified in CCPA, regardless of whether the company is subjected to CCPA or not.

Hypotheses

In this study, we want to understand to what extent companies in different industries comply with the FIP and whether companies' privacy practices differ across industry sectors. While the selected companies are all heavily involved in collecting and using consumers' PI, the nature of the data collected and the purpose of using and sharing the collected data differ fundamentally across these sectors.

Consumers are highly sensitive and concerned of their financial and health information because such PI concerning their financial and physical health. However, in terms of scope and volume, companies in the selected CS sector often collect a much wider range of consumers' PI daily. Other than sharing consumer data internally for normal business operations, companies in all three sectors may also share consumer data with third parties for profits. For companies in the FIN and HC sectors, their primary revenue streams are from the financial or health-care services provided to consumers. However, for companies in the CS sector such as search engines, social media and networking platforms, and online review companies, their business models are mostly about generating revenues from collecting, processing, and sharing consumer data.

Additionally, the FIN and HC sectors are regulated by the GLBA and HIPAA, respectively. Companies covered by such federal regulations are required to follow the rules set for the use, disclosure, and protection of consumers' NPI or PHI. However, for the CS sector, there are no equivalent government regulations.

Table 5. Descriptive statics of the checklist by sector and total.

			CS		HC		FIN		Total	
FIP Category	FIP Code	CCPA Code	N	%	N	%	N	%	N	%
Notice	N1	CA_RtK	33	100%	30	88%	34	100%	97	96%
	N2	CA_RtK	27	82%	24	71%	32	94%	83	82%
	N3	CA_RtK	29	88%	29	85%	12	35%	70	69%
	N4	CA_RtK	30	91%	33	97%	33	97%	96	95%
	N5	CA_RtK	32	97%	33	97%	33	97%	98	97%
	N6		29	88%	33	97%	30	88%	92	91%
	N7		25	76%	10	29%	17	50%	52	51%
Choice	C1		22	67%	18	53%	9	26%	49	49%
	C2	CA_RtOO	31	94%	26	76%	19	56%	76	75%
	C3	CA_RtNR	17	52%	20	59%	24	71%	61	60%
Access	A1		32	97%	28	82%	25	74%	85	84%
	A2		11	33%	23	68%	5	15%	39	39%
	A3		27	82%	28	82%	14	41%	69	68%
	A4	CA_RtDI	30	91%	26	76%	28	82%	84	83%
Security	S1		24	73%	24	71%	27	79%	75	74%
	S2		21	64%	31	91%	30	88%	82	81%
Enforcement	E1		28	85%	24	71%	31	91%	83	82%
	E2		9	27%	4	12%	2	6%	15	15%
	E3		4	12%	2	6%	1	3%	7	7%
	E4		32	97%	33	97%	33	97%	98	97%
Additional Feature	AF1		33	100%	31	91%	16	47%	80	79%
	AF2		4	12%	13	38%	18	53%	35	35%
	AF3		16	48%	27	79%	16	47%	59	58%
	AF4		30	91%	19	56%	26	76%	75	74%
	AF5		30	91%	34	100%	33	97%	97	96%
	AF6		27	82%	20	59%	26	76%	73	72%
	AF7		22	67%	21	62%	30	88%	73	72%
	AF8		4	12%	4	12%	14	41%	22	22%
	AF9		27	82%	25	74%	22	65%	74	73%

Thus, we hypothesize that due to the differences in business nature and levels of regulations, companies in these three sectors may follow different privacy practices, and such differences will be reflected in how well their privacy policies comply with FIP and how they make extra efforts in providing privacy policy content and design features that go beyond FIP.

H1: Companies in different sectors follow different privacy practices: having different levels of compliance with FIP in their privacy policies and acting differently in providing policy content and design features that go beyond FIP.

In this study, the CCPA-index represents a better privacy practice of voluntarily providing consumers' rights and control terms specified in CCPA in a company's privacy policy. That is, giving all consumers more controls over their PI, not just the CA residents. Similarly, given the different business nature and different levels of regulations, we hypothesize that companies in different sectors may comply with the CCPA-terms and non-CCPA-terms in the FIP checklist differently.

H2: In terms of FIP compliance practice, companies in different sectors provide different levels of CCPA- and non-CCPA-related terms in their privacy policies.

Because the CCPA-index represents a better privacy practice, we hypothesize that companies that offer more CCPA-items in their privacy policies are likely to comply more with non-CCPA items in their policies. Similarly, companies that voluntarily comply more with FIP are likely to take steps forward to provide more AF when disclosing their privacy policies.

H3: The practice of offering CCPA-terms in the privacy policy positively affects a company's compliance with non-CCPA-terms.

H4: The practice of complying with FIP in the privacy policy positively affects a company's offering of AF when disclosing its privacy policy.

Analysis and results

Overall privacy policy disclosure

For the Notice principle, the assessed companies as a whole did well in informing consumers what specific user data will be collected (96%), how the collected user data will be used internally (95%), whether and how the collected user data will be shared outside the company (97%), and how the company will communicate changes to the policy with users (91%). However, they were

Table 6. Summary statistics of the checklist.

	CCPA-index			N-CCPA-index			FIP-index			AF-index			Total index		
	CS	HC	FIN	CS	HC	FIN	CS	HC	FIN	CS	HC	FIN	CS	HC	FIN
Max	8	8	8	12	11	9	20	19	17	9	8	8	29	25	23
Min	4	3	4	3	4	2	8	7	6	3	2	2	12	11	10
Mean	6.94	6.50	6.32	8.09	7.59	6.59	15.03	14.09	12.91	5.85	5.71	5.91	20.88	19.79	18.82
Std Dev	1.03	1.67	1.20	2.07	1.79	1.60	2.74	2.99	2.22	1.35	1.55	1.40	3.63	3.98	2.88
Count	33	34	34	33	34	34	33	34	34	33	34	34	33	34	34

lacking in explaining why user data will be collected (69%) and what user data will be retained and for how long (51%). Companies in the CS sector overall conformed to the Notice principle better than those in the other two sectors. However, the assessed companies did not do well in complying with the Choice principle, with only 49% stated whether users have choices on what data the company can collect and use internally, 75% stated whether users have choices on what collected data the company can disclose to a third party, and 60% stated users' right to nondiscrimination for exercising opt-out or other rights. While companies in the CS sector complied better to the first two items, they did not do well on the third one.

For the Access principle, only 39% of the assessed companies stated whether users are allowed to export the collected data about them, and 68% stated whether users are allowed to modify the collected data about them to make corrections. Companies in the FIN sector especially lagged on these two items whereas companies in the HC sector complied better (68%) on the first item. Companies in the CS sector complied better, 97% and 91%, respectively, in allowing users to review and delete the collected data about them.

For the Security principle, 74% and 81% of the assessed companies provided the specified security terms in their privacy policies. For the Enforcement principle, only 15% of the assessed companies stated whether the company will take actions against those who violate its privacy policy, and only 7% mentioned the adoption of a third-party privacy assurance standard.

For the additional features, the assessed companies only did well (96%) in informing consumers the effective date of the privacy policy (AF5). They especially did not do well in providing print/save option of the privacy document (AF2) and explaining key terms to help users better understand the policy document (AF8), with only 35% and 22% provided these features, respectively. Compared to the other two sectors, companies in the FIN sector complied better on these two items, with 58% and 41%, respectively.

We constructed five indexes from Table 5 by adding up the variables included for the FIP compliance (FIP-index), addition features (AF-index), and the full checklist (Total-index), and by separating the FIP compliance items further into CCPA-related (CCPA-index) and non-CCPA-related (N-CCPA-index). Table 6 presents the summary statics for these indexes. Out of the 101 assessed companies, 32 had all of the eight CCPA-related consumers' rights elements in their privacy policies, but only two complied to all of the 12 non-CCPA-related elements in the FIP list. For the nine additional contents and designs features assessed, only one company provided all of these elements. The CS sector has a higher mean FIP-index, and all three sectors have similar mean AF-index. Overall, only one company, Alphabet Inc, provided all elements in the checklist in its privacy policy page. For the five indexes, the spreads are very wide for all three sectors. For instance, it is shocking to see that each sector has some companies that only provided less than half of the items in the FIP checklist in their privacy policies. Similarly, each sector has some companies that only provided less than half of the items in the AF or non-CCPA-related checklist.

Hypothesis testing

To examine the privacy practice differences across sectors, we conducted a multivariate analysis of variance (MANOVA) with the FIP-index and AF-index as dependent variables and sector as the independent variable. The MANOVA results show that the two dependent privacy practice measures, when viewed collectively (multivariate Wilk's λ test: $p < .01$, $\eta^2 = 0.834$) and individually (Table 7), do vary across sectors in a statistically significant manner. Thus, the MANOVA test supports H1 that industry sector has a statistically significant effect on companies' privacy practice in terms of FIP compliance and providing policy content and design features that go beyond FIP. The post hoc Bonferroni tests (Table 8) further show that companies in the CS sector complied to FIP significantly more than those in the FIN sector. While the CS sector complied to FIP more than the HC sector, which also complied to FIP more than the FIN sector, these differences are not statistically significant. However, the pairwise comparisons on AF-index show no significant difference between groups.

Table 7. Tests of between-subjects effects (AF-index and FIP-index).

Source	Dependent Variable	df	Mean Square	F	Sig.	Partial Eta Squared
Sector	AF-index	3	1141.321	553.610	0.000*	0.944
	FIP-index	3	6623.853	929.410	0.000*	0.966

Table 8. Multiple comparisons–Bonferroni test (AF-index and FIP-index).

Dependent Variable	(I) Sector	(J) Sector	Mean Difference (I-J)	Std. Error	Sig.
AF-index	1 (CS)	2 (HC)	0.14	0.351	1.000
		3 (FIN)	−0.06	0.351	1.000
	2 (HC)	1 (CS)	−0.14	0.351	1.000
		3 (FIN)	−0.21	0.348	1.000
	3 (FIN)	1 (CS)	0.06	0.351	1.000
		2 (HC)	0.21	0.348	1.000
FIP-index	1 (CS)	2 (HC)	0.94	0.652	0.456
		3 (FIN)	2.12*	0.652	0.005
	2 (HC)	1 (CS)	−0.94	0.652	0.456
		3 (FIN)	1.18	0.647	0.217
	3 (FIN)	1 (CS)	−2.12*	0.652	0.005
		2 (HC)	−1.18	0.647	0.217

* The mean difference is significant at the .01 level.

In regard to specific AF items, chi-square analyses show that six out of the nine AF features have significant differences across sectors. For AF1, χ^2 = 32.96, p < .01, all companies in the CS sector only required users to click once to access their privacy policy page whereas over half of companies in the FIN sector required two to three clicks. For AF2, χ^2 = 12.61, p < .01, more companies in the FIN sector provided the option for users to download/print the policy in PDF format whereas most companies in the CS sector did not provide this option. For AF3, χ^2 = 9.32, p < .01, more companies in the HC sector implemented the concept of layered privacy notice, by providing interactive table of content or highlights/summary of the policy, to give users a high-level overview of the privacy practices in addition to an in-depth description of these practices. For AF4, χ^2 = 10.88, p < .01, most companies in the CS sector provided links to various privacy settings in their policy page whereas companies in the HC sector were the least likely to offer this feature. For AF7, χ^2 = 6.72, p = .035, most companies in the FIN sector specified that they have a CCPN or provided a link to it in their policy pages. For AF8, χ^2 = 11.32, p < .01, more companies in the FIN sector provided explanation of key terms used in the policy either via callouts or in a designated section in the policy page, whereas this feature was significantly absent from the other two sectors. Even though, there were significant differences across sectors in six out of the nine AF features, because each of the three sectors was doing well providing different AF features, the post hoc Bonferroni tests show no significant pair-wise differences between sectors in terms of the AF-index.

In checking for compliance with FIP principles, we did not classify a company as complied to a FIP principle just because its privacy policy mentions terms that can be somewhat matched to that principle. Instead, we examined how explicit the policy is in describing the matched privacy practice. For example, the FIP notice specifies that consumers have a right to know if PI is being collected and how it will be used. We checked seven specific elements to measure a company's compliance with notice. To examine the differences in a specific FIP compliance, for each FIP principle, we further classified a company into one of the following categories: *F* (full compliance having all of the checked items), *M* (medium level of compliance having at least half of the checked items), *L* (low level of compliance), or *N* (no compliance having none of the checked items). Figure 1 shows the bar-charts of frequency count of compliance for each FIP principle. We then conducted the Pearson's chi-square tests for any significant association between sector and compliance with each of the FIP principles. The test results show that the three sectors have significant differences in their compliance with three FIP principles, Notice ($\chi^2(df = 4)$ = 11.35, p= .023), Choice ($\chi^2(df = 6)$ = 12.54, p = .051), and Access (χ^2 $(df = 6)$ = 24.60, p < .01). Specifically, more companies in the CS sector fully complied to Notice whereas most companies in the FIN and HC sectors only complied at the medium level. For Access, more companies in the HC sector complied fully, whereas most companies in the other two sectors had a medium-level compliance. However, both FIN and HC sectors had companies that did not comply with the Access principle, i.e., their policies did not specify whether users can review, export, modify, or delete data collected about them. For Choice, more companies in the CS sector fully complied, but all sectors had 30% or higher had low or no compliance. The differences in their compliances to the Security and Enforcement principles were not significant.

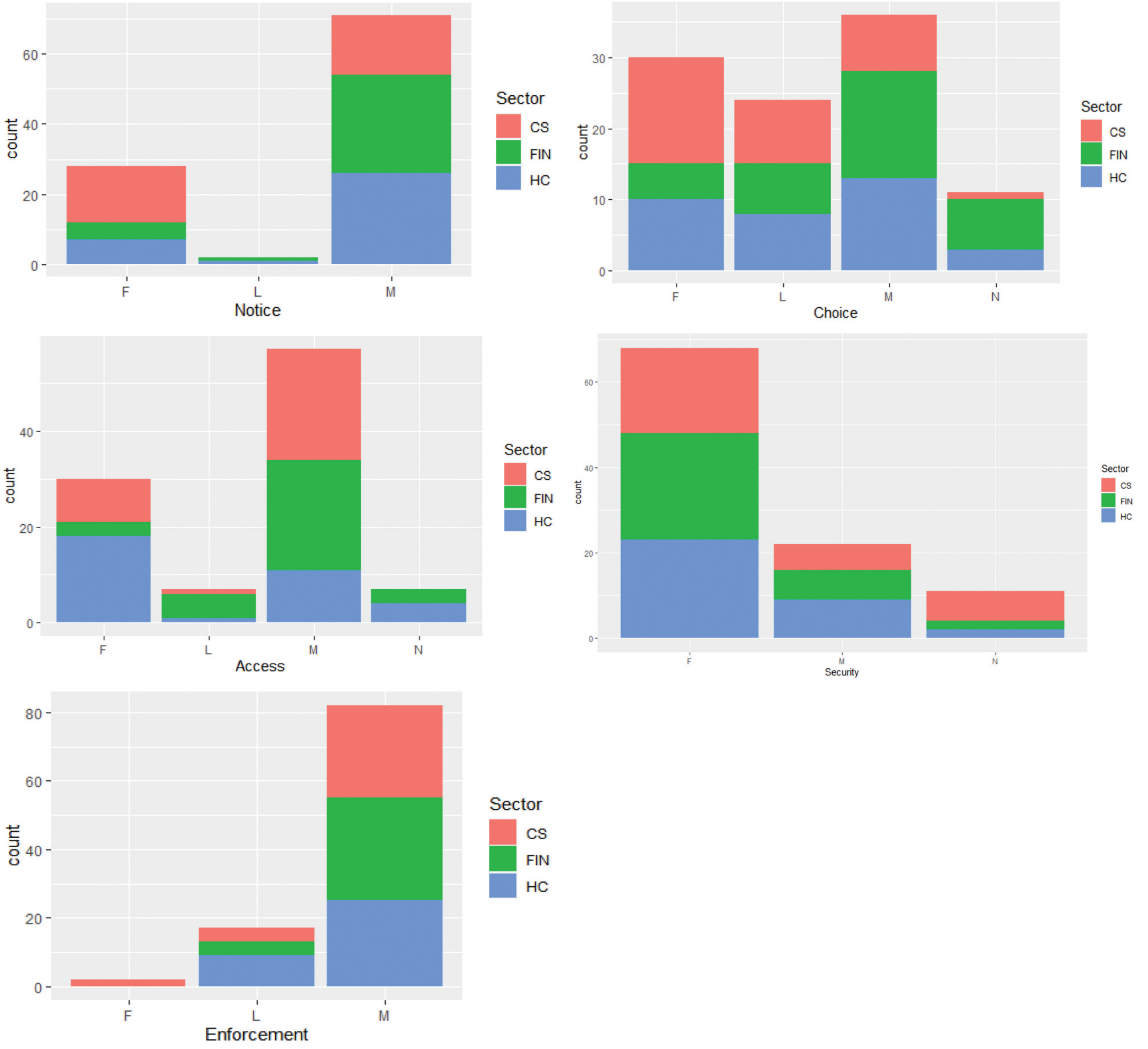

Figure 1. Bar chart of sector compliance with each FIP principle.

In our study, the CCPA-index represents how well a company's privacy policy measures up in giving consumers controls over their PI as specified in CCPA. Since all of the companies in this study are big in the corresponding sub-industries in terms of market capitalizations, we suspect that most of them are subjected to CCPA. While we did not specifically verify that, we did notice that some companies, for example, Fifth Third Bancorp and Zions Bancorp as regional banks, do not have branches in California. We found that Zions only has four out of the eight items in the CCPA checklist whereas the Fifth Third bank has seven and that is three more than American Express, which has operations in California. That is, companies that are not directly subjected to CCPA regulations may voluntarily adhere to a better privacy practice whereas companies that are subjected to CCPA may not extend the CCPA terms to non-Californian consumers. Next, we examine whether companies in different sectors comply with the CCPA- and non-CCPA-terms in the checklist differently.

To test for H2, we conducted a MANOVA with the CCPA-index and N-CCPA-index as dependent variables and sector as the independent variable. The MANOVA results show that the two dependent privacy practice measures, when viewed collectively (multivariate Wilk's λ test: $p < .01$, $\eta^2 = 0.825$) and individually (Table 9), did vary across sectors in a statistically significant manner. Thus, the MANOVA test supports H2 that industry sector has a statistically significant effect on companies' FIP compliance practice, that is, they

Table 9. Tests of between-subjects effects (CCPA-index and N-CCPA-index).

Source	Dependent Variable	df	Mean Square	F	Sig.	Partial Eta Squared
Sector	N-CCPA-Index	3	1864.601	558.472	0.000*	0.945
	CCPA-Index	3	1461.727	824.124	0.000*	0.962

Table 10. Multiple comparisons–Bonferroni test (CCPA-index and N-CCPA-index).

Dependent Variable	(I) Sector	(J) Sector	Mean Difference (I-J)	Std. Error	Sig.
N-CCPA-index2	1 (CS)	2 (HC)	0.50	0.447	0.789
		3 (FIN)	**1.50***	**0.447**	**0.003**
	2 (HC)	1 (CS)	−0.50	0.447	0.789
		3 (FIN)	**1.00****	**0.443**	**0.079**
	3 (FIN)	1 (CS)	−1.50*	0.447	0.003
		2 (HC)	−1.00**	0.443	0.079
CCPA-index2	1 (CS)	2 (HC)	0.44	0.325	0.540
		3 (FIN)	0.62	0.325	0.184
	2 (HC)	1 (CS)	−0.44	0.325	0.540
		3 (FIN)	0.18	0.323	1.000
	3 (FIN)	1 (CS)	−0.62	0.325	0.184
		2 (HC)	−0.18	0.323	1.000

* The mean difference is significant at the .01 level.
** The mean difference is significant at the .1 level.

provide different levels of CCPA-related and non-CCPA related terms. The post hoc Bonferroni tests (Table 10) further show that companies in the CS sector complied to the non-CCPA-related terms significantly ($p < .01$) more than those in the FIN sector. Companies in the HC sector also complied to the non-CCPA-related terms more than those in the FIN sector, but only with a weak statistical support at the 0.1 level. The pairwise comparisons on CCPA-index show no significant between-group differences.

Items in the CCPA-index focus on consumers' rights and controls. We next check whether the practice of offering CCPA-terms in the privacy policy positively affects a company's compliance with non-CCPA-terms. We run a linear regression model with non-CCPA-index as the dependent variable and sector and CCPA-index as independent variables. The result shows that providing CCPA-terms in the privacy policy did significantly and positively influence the provision of non-CCPA-terms in the policy [R^2 = 0.260, Adj. R^2 = 0.237, F = 11.376 (p < .001); $\beta_{(\text{CCPA-index})}$ = 0.568, $t_{(\text{CCPA-index})}$ = 4.478 (p = .000)]. That is, companies that voluntarily adhere to a better privacy practice, giving consumer controls over their PI as specified in CCPA in their general privacy policies, tend to comply more to additional FIP items. Hence, H3 is supported.

Similarly, we run a linear regression model with AF-index as the dependent variable and sector and FIP-index as independent variables. The result shows that complying with FIP in the privacy policy did significantly and positively influence the provision of AF in a company's policy disclosure [R^2 = 0.182, Adj. R^2 = 0.156, F = 7.179 (p < .001); $\beta_{(\text{FIP-index})}$ = 0.227, $t_{(\text{FIP-index})}$ = 4.593 (p = .000)]. That is, companies that comply more to FIP tend to go beyond the minimal requirements by providing additional content and design features to effectively disclose the policies. Hence, H4 is supported. The outcomes of the hypothesis testing are summarized in Table 11.

Table 11. Summary of hypothesis testing.

Hypotheses Tested	F statistic	Sig	β	t statistic	p value	Result
H1: Companies in different sectors have different levels of compliance with FIP and provide different AF that go beyond FIP	FIP-index: 929.410 AF-index: 553.610	<0.001 <0.001				Supported
H2: Companies in different sectors provide different levels of CCPA-related and non-CCPA-related terms	CCPA-Index: 824.124 N-CCPA-Index: 558.472	<0.001 <0.001				Supported
H3: Offering CCPA-terms in the privacy policy positively affects a company's compliance with non-CCPA-terms			0.568	4.478	p < .001	Supported
H4: Complying with FIP in the privacy policy positively affects a company's offering of AF when disclosing its privacy policy			0.227	4.593	p < .001	Supported

Discussion

Content analysis research on privacy policy mostly focus on the largest companies[13,26] or the best or most popular websites in a domain.[42–44] Since they do not always use the same company lists, findings from these studies are usually not directly comparable. Nevertheless, results from these studies still can provide some insights into where the leading companies are heading in terms of privacy policy FIP compliance over the years. Prior studies have found an improving trend that more companies are disclosing their privacy policies online and are adhering to FIP principles.[13,45] Another consistent finding is that privacy policies that are full-FIP complied are less common.[13,34,43–46]

This study updates prior work by focusing on companies with high PDS risk and especially by examining for the first time the privacy practice of companies in the CS sector. Prior studies have found that privacy policies that fully conform to FIP may send a positive signal to consumers and help foster positive consumer trust beliefs and increased willingness to provide PI.[47,48] Findings from this study shows that over 20 years after the FTC's initial privacy policy surveys, an industry-wide full-FIP compliance is still very rare. Only around 30% of companies in this study complied fully to the Notice, Access, or Choice principles, and only 2% complied fully to the Enforcement principle. Most companies provided contact information for consumers to report issues or file complaints, and that might be the first step as self-enforcement. However, a large percentage of companies did not specify what actions will be taken for violation of the stated policy. Even with information provided in the privacy policies, consumers have no way of knowing whether the policies are implemented and followed. Seal programs, such as TRUSTe, EU-U.S., and Swiss-U.S. Privacy Shield Frameworks, provide third-party compliance monitoring to ensure that firms abide by their posted privacy policies, and they were included as one of the self-enforcement elements in our checklist. Our study showed that the adoption of third-party monitoring programs is very low among the assessed companies.

Wu et al.[48] found that Security is the most important FIP dimension for consumers and suggested that companies to focus more on providing security information in their policies to improve consumer trust. Chang et al.[49] found that Enforcement has the strongest effect on consumers' perceived effectiveness of privacy policy. In this study, we did find that 67% of companies fully complied to the Security principle, indicating that companies were paying more attention to the Security dimension of FIP. However, they were not doing enough in full specification of Enforcement in their privacy policies, and this may be related to the lack of specific enforcement provision in regulations and FIP.

By comparing the privacy policy FIP-compliance across sectors, we did find evidence that supports the FTC's approach of relying on self-regulation to ensure fair information practices. While conformity with third-party standards, such as privacy seal programs, might be the primary self-regulatory enforcement mechanism, market competition also plays an important role in shaping firms' privacy practices. Companies in the CS sector are in the business of profiting from collecting, processing, and sharing user data. The types of data collected by the CS sector can be very personal and sensitive, and the scope and volume of data collected by the sector has no match in any other industries. Hence, consumers have a high privacy concern when interacting with CS companies. Having a privacy policy that is in a better alignment with FIP helps mitigate users' privacy concerns and encourage data sharing. In our study, companies in the CS sector, which is not regulated, complied to FIP better than those in the FIN sector, which is regulated by GLBA. More companies in the CS sector complied fully on Notice and Choice, and they measured up to those in the regulated sectors in compliance with both CCPA- and non-CCPA-related items in our FIP checklist. This indicates that self-regulation via the market-based mechanism works for the CS sector. Similar evidence has been found in the Adult sector, offering better notice and sharing practices, and the Cloud Computing sector, offering a greater extent of data security, as the business models and market competition induce firms to incorporate users' preferences into their privacy practices.[50]

The assessed companies had a high compliance for four of the five FIP principles at the full or medium level, with 98% for Notice, 86% for Access, 89% for Security, and 83% for Enforcement. For Choice, 65% of the assessed companies complied at the full or medium level. The CS sector measured up on all FIP dimensions except on Security with only 79% complied at full or medium level whereas the other two regulated sectors had 94% compliance. It is not surprise that the assessed companies in the FIN and HC sectors were doing better in specifying security procedures in their privacy policies since both are specifically regulated to have security programs in place to protect users' information.

Milne and Culnan[45] find that perceived comprehensibility of online privacy policies is positively associated with users' tendency to read the policies and their trust of the policies. Effective policy document representations, such as using text, audio, and pictorial presentation cues or organizing policy by categories, make the policy document apt to read and can help improve user comprehension of the presented policy.[47,51] The AFs identified in this study, such as an interactive design, providing links to the corresponding category sections within the document page or providing policy summary highlights on top of the full policy, and providing explanations of terms used in the privacy policies, help improve users' perceived comprehensibility of the privacy policies. We find that only 58% and 22% of companies included in this study are exploring these opportunities to help improve users' comprehension of the policies and their likelihood of trusting the policies. However, only one company has also provided multiple videos further explaining the policy terms and demonstrating how to change privacy settings.

Schwaig et al.[15] proposed a privacy policy assessment matrix and used it to judge the policy quality and maturity of the Fortune 500 companies. The matrix has two dimensions, compliance with the FIP measuring privacy policy quality, and advanced disclosure measuring factors beyond the minimal requirements. We updated both the FIP compliance and advanced disclosure measures to include additional policy contents and disclosure features in this study. The scatterplot of FIP-index vs AF-index shows that the examined companies can indeed be mapped into four privacy policy categories (labeled as cluster in Figure 2). The insufficient protection polices (cluster 3), with low FIP and low AF, representing companies that provided low FIP compliance in their privacy policies and did not exert much efforts in disclosing policies. The k-means cluster analysis with four clusters showed that 16 companies fall in this category and the three sectors were equally represented, with 5 (CS), 5 (FIN), and 6 (HC). The public relations policies (cluster 2), with high FIP and low AF, representing companies that provided above average FIP compliance in their privacy policies but did not exert efforts in effectively disclosing policies. The cluster analysis shows that 22 companies fall in this category, leading by the CS sector with 11 (CS), 7 (HC), and 4 (FIN). The focused/limited policies (cluster 1), with low FIP and relatively high AF, representing companies that provided below average FIP compliance in their privacy policies but did exert some efforts in effectively disclosing policies. The cluster analysis shows that 39 companies fall in this category, leading by the FIN sector with 21 (FIN), 11 (HC), and 7 (CS). The mature policies (cluster 4), with high FIP and high AF, representing companies that provided high FIP compliance in their privacy policies and also exerted additional efforts beyond the minimal requirements in effectively disclosing policies. The cluster analysis shows that 24 companies fall in this category, dominated by companies in the CS and HC sectors, with 10 (CS), 10 (HC) and 4 (FIN). These companies set the privacy practice standards in both FIP compliance and effective policy disclosure. In this mature category, the CS sector, while not regulated, measures up to the HC sector, which is regulated by HIPPA. On the other hand, all three sectors had companies that lagged behind in both measures, indicating that these companies were unconcerned with users' privacy even though they were heavily involved in data collection, use, and sharing.

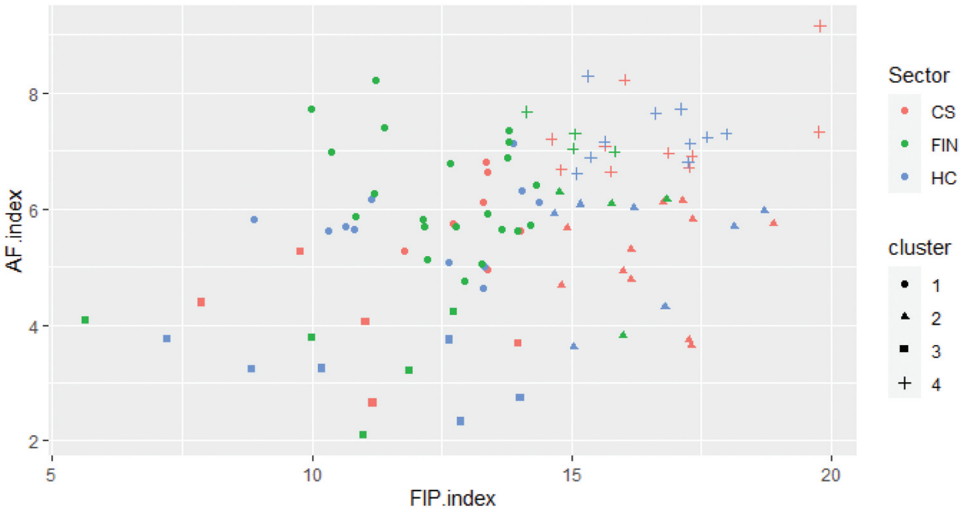

Figure 2. FIP and AF scatterplot.

Conclusion and future research

Developing and disclosing privacy policy that adheres to FIP is an important first step to ease consumers' privacy concerns. A policy that is full-FIP complied shows that the company understands and cares about consumers' privacy issues and is to be trusted with their personal data. This study helps us understand how the FIP and government regulations have influenced companies' privacy practices and if self-regulation via market-based mechanism works. We find that companies in the three studied sectors have different levels of compliance with FIP in their privacy policies, and they also acted differently in providing policy content and design features that go beyond the FIP. The privacy practices of the studied companies in the CS sector showed that the FTC's approach of enforcing FIP through self-regulation works. We found that driven by market forces, companies in this unregulated sector complied more to FIP in their privacy policies than those in the regulated FIN sector, and their FIP compliance also measured up to those in the regulated HC sector.

We further looked into compliance with each of the FIP principles and found direct correlations between regulations and compliance practice. For example, GLBA does not require the regulated financial institutions to give customers access to collected data, and we found that only 15% of assessed companies in the FIN sector stated that users are allowed to export the collected data about them. Companies in the two regulated sectors had more full compliance with the Security principle since the HIPPA and GLBA each has specific security rules. We found a moderate level of full compliance with the Notice, Access, and Choice principles, but a very low level of full compliance with the Enforcement principle due to the lack of specific provision in FIP and regulations. Without a proper enforcement and redress mechanism, the privacy policy may be viewed as less effective by consumers because after all, consumers have no way of knowing whether a company actually adheres to its policy. Hence, regulators need to strengthen enforcement provision in regulations and develop and enlist various enforcement mechanisms. In a recent study, Pilton et al.[52] developed a privacy-paradox browser (Chrome) extension, which can automatically assess and analyze a company's privacy policy to detect/report privacy policy violations and intercept and report various types of trackers with the display of a privacy summary popup. They showed that implementing such kind of browser extension can help provide privacy transparency to users and improve their privacy awareness. Such technology tools can be incorporated into self-regulation regimes and government enforcement to improve the effectiveness of the FTC's notice-choice model and harm-based approach.[53]

While we took the steps to examine the privacy practice of data intensive industries and compared the privacy practices across sectors, the results of this study do not directly apply to other policies outside the set of studied sectors. Future research can extend this study to investigate the privacy practice of other sectors. We focused on examining policy compliance with the five FIP principles and additional features provided in disclosing the policies. We did not, however, assess whether a firm's actual business practices comply with its own privacy policy. Additionally, we did not include surveys of consumers' perceptions or expectations of companies' privacy practices. Wu et al.[48] found partial support that content of online privacy policy has a negative impact on privacy concern and positive impact on trust. Examining the actual policy enforcement, how consumers view the industry-wide privacy practice, and the impact of privacy practice on consumers' trust and disclosure behaviors are important directions for future research. Other extensions are to study whether differences in privacy policy FIP compliance are associated with other firm characteristics, such as firm age, size, and financial strength and to examine the causal relationship between FIP compliance and consumer trust and firm performance.

Overall, this research provides a few important academic and practical implications. First, examining firms' privacy practice and its impact is one stream of IS privacy research that warrants more research attentions. Such studies can inform both the public and regulators on the quality of industries' privacy policies and their disclosures and provide recommendations for practitioners on how to effectively present policy document to better inform consumers. Research studying the impact of privacy policy disclosure may provide further supports for the practice of implementing policy that offers greater privacy protection and hence help promote such practice. Second, privacy policy research such as this one provides evidence on the effectiveness of government regulation and industry self-regulation. Such studies can inform regulators on the needs of provision and the areas of revision of regulations.

Acknowledgement

We thank undergraduate students Kiley Gosselin and Madison Granados for their contributions to data collection. This research was supported through a Professional Development Fund Grant awarded by the Florida Gulf Coast University.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

1. World Bank. Individuals using the Internet (% of population) [Internet]. [accessed 2022 Feb 17]. https://data.worldbank.org/indicator/IT.NET.USER.ZS
2. Chen K, Rea AI. Protecting personal information online: a survey of user privacy concerns and control techniques. J Comput Inf Syst. 2004;44(4):85–92. doi:10.1080/08874417.2004.11647599.
3. Isaak J, Hanna MJ. User data privacy: Facebook, Cambridge analytica, and privacy protection. Computer. 2018;51(8):56–59. doi:10.1109/MC.2018.3191268.
4. Baron Insight. An overview of the new communication services GICS sector [Internet]. 2018. [accessed 2022 Apr 8]. https://www.baronfunds.com/insights/baron-insight-overview-new-communication-services-gics-sector
5. Jozani M, Ayaburi E, Ko M, Choo -K-KR. Privacy concerns and benefits of engagement with social media-enabled apps: a privacy calculus perspective. Comput Hum Behav. 2020;107:106260. doi:10.1016/j.chb.2020.106260.
6. Chan EY, Saqib NU. Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. Comput Hum Behav. 2021;119:106718. doi:10.1016/j.chb.2021.106718.
7. Information Commissioner's Office. Guide to the general data protection regulation. GOVUK [Internet]; 2018 [accessed 2022 Mar 16]. https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation
8. State of California. California Consumer Privacy Act. State Calif - Dep Justice - Off Atty Gen [Internet]. 2018 [accessed 2020 Sep 28]. https://oag.ca.gov/privacy/ccpa
9. Bonner W, Chiasson M. If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy. Inf Organ. 2005;15(4):267–93. doi:10.1016/j.infoandorg.2005.03.001.
10. Federal Trade Commission. Fair information practice principles [Internet]. 2007. https://web.archive.org/web/20070911005723/http://www.ftc.gov:80/reports/privacy3/fairinfo.shtm
11. Gellman R. Fair information practices: a basic history - Version 2.21 [Internet]. Rochester (NY): Social Science Research Network; 2021. doi:10.2139/ssrn.2415020.
12. Organisation for Economic Co-Operation and Development. OECD guidelines on the protection of privacy and transborder flows of personal data [Internet]. 2013 [accessed 2022 Mar 16]. https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
13. Case CJ, King DL, Gage LM. Online privacy and security at the fortune 500: an empirical examination of practices. ASBBS E-J. 2015;11:59–67.
14. Li Y, Stewart W, Zhu J, Ni A. Online privacy policy of the thirty dow jones corporations: compliance with FTC fair information practice principles and readability assessment. Commun IIMA. 2012;12:26.
15. Schwaig KS, Kane GC, Storey VC. Compliance to the fair information practices: how are the fortune 500 handling online privacy disclosures? Inf Manage. 2006;43(7):805–20. doi:10.1016/j.im.2006.07.003.
16. Smith HJ, Dinev T, Xu H. Information privacy research: an interdisciplinary review. MIS Q. 2011;35(4):989–1015. doi:10.2307/41409970.
17. Bélanger F, Crossler RE. Privacy in the digital age: a review of information privacy research in information systems. MIS Q. 2011;35(4):1017–41. doi:10.2307/41409971.
18. Yun H, Lee G, Kim DJ. A chronological review of empirical research on personal information privacy concerns: an analysis of contexts and research constructs. Inf Manage. 2019;56(4):570–601. doi:10.1016/j.im.2018.10.001.
19. Dinev T, McConnell AR, Smith HJ. Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO". Box Inf Syst Res. 2015;26(4):639–55. doi:10.1287/isre.2015.0600.
20. Baruh L, Secinti E, Cemalcilar Z. Online privacy concerns and privacy management: a meta-analytical review. J Commun. 2017;67(1):26–53. doi:10.1111/jcom.12276.
21. Kokolakis S. Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. Comput Secur. 2017;64:122–34. doi:10.1016/j.cose.2015.07.002.
22. U.S. Department of Justice. Privacy Act of 1974 [Internet]. 2014 [accessed 2022 Mar 16]. https://www.justice.gov/opcl/privacy-act-1974
23. Federal Trade Commission. Privacy online: a report to congress [Internet]. [place unknown]: Washington (DC); 1998. http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf
24. Klemovitch J, Sciabbarrasi L, Peslak A. Current privacy policy attitudes and fair information practice principles: a macro and micro analysis. Issues Inf Syst. 2021;22(3):145–59. doi:10.48009/3_iis_2021_159-174.
25. Solove DJ. HIPAA turns 10: analyzing the past, present and future impact. J AHIMA. 2013;84:22–28.
26. Milne GR, Culnan MJ. Using the content of online privacy notices to inform public policy: a longitudinal analysis of the 1998-2001 U.S. Web surveys. Inf Soc. 2002;18(5):345–59. doi:10.1080/01972240290108168.
27. Nemati HR, Van Dyke T. Do privacy statements really work? The effect of privacy statements and fair information practices on trust and perceived risk in E-commerce. Int J Inf Secur Priv. 2009;3(1):45–64. doi:10.4018/jisp.2009010104.
28. Peslak AR. Internet privacy policies: a review and survey of the fortune 50. Inf Resour Manage J. 2005;18(1):29–41. doi:10.4018/irmj.2005010103.
29. Peslak AR. Internet privacy policies of the largest international companies. J Electron Commer Organ. 2006;4(3):46–62. doi:10.4018/jeco.2006070103.
30. Zhang X, Sakaguchi T, Kennedy M. A cross-cultural analysis of privacy notices of the global 2000. J Inf Priv Secur. 2007;3:18–36.

31. Al-Jamal M, Abu-Shanab E. Privacy policy of E-Government websites: an itemized checklist proposed and tested. Manage Res Pract. 2015;7:17.
32. Fawaz K, Linden T, Harkous H. The applications of machine learning in privacy notice and choice. Proceedings of the 2019 11th International Conference on Communication Systems & Netwo COMSNETS; 2019; Bengaluru, India. p. 118–24. doi:10.1109/COMSNETS.2019.8711280
33. Harkous H, Fawaz K, Lebret R, Schaub F, Shin KG, Aberer K. Polisis: automated analysis and presentation of privacy policies using deep learning. Proc 27th USENIX Secur Symp USENIX Secur 18 [Internet]; 2018; Baltimore, MD, USA. p. 531–48. [accessed 2022 Mar 10]. https://www.usenix.org/conference/usenixsecurity18/presentation/harkous
34. Kaur J, Dara RA, Obimbo C, Song F, Menard K. A comprehensive keyword analysis of online privacy policies. Inf Secur J Glob Perspect. 2018;27(5–6):260–75. doi:10.1080/19393555.2019.1606368.
35. Sadeh N, Acquisti A, Breaux TD, Cranor LF, McDonald AM, Reidenberg JR, Smith NA, Liu F, Russell NC, Schaub F, et al. The usable privacy policy project [Internet]. Pittsburgh (PA): Carnegie Mellon University; 2013. http://ra.adm.cs.cmu.edu/anon/usr0/ftp/home/anon/isr2013/CMU-ISR-13-119.pdf.
36. Zaeem RN, German RL, Barber KS. PrivacyCheck: automatic summarization of privacy policies using data mining. ACM Trans Internet Technol. 2018;18(4):1–18. doi:10.1145/3127519.
37. Linden T, Khandelwal R, Harkous H, Fawaz K. The privacy policy landscape after the GDPR. Proc Priv Enhancing Technol. 2020;2020(1):47–64. doi:10.2478/popets-2020-0004.
38. Zaeem RN, Barber KS. The effect of the GDPR on privacy policies: recent progress and future promise. ACM Trans Manage Inf Syst. 2020;12(1):1–20. doi:10.1145/3389685.
39. Li Y. Empirical studies on online information privacy concerns: literature review and an integrative framework. Commun Assoc Inf Syst [Internet]. 2011;28(1). doi:10.17705/1CAIS.02828.
40. Federal Trade Commission. How to comply with the privacy of consumer financial information rule of the Gramm-Leach-Bliley Act [Internet]. 2002 [accessed 2022 Mar 10]. https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf
41. MSCI. Global Industry Classification Standard (GICS®) methodology. MSCI Inc: New York, NY, USA; 2020. https://www.msci.com/documents/1296102/11185224/GICS+Methodology+2020.pdf/9caadd09-790d-3d60-455b-2a1ed5d1e48c?t=1578405935658
42. Miyazaki AD, Fernandez A. Internet privacy and security: an examination of online retailer disclosures. J Public Policy Mark. 2000;19(1):54–61. doi:10.1509/jppm.19.1.54.16942.
43. Rains SA, Bosch LA. Privacy and health in the information age: a content analysis of health web site privacy policy statements. Health Commun. 2009;24(5):435–46. doi:10.1080/10410230903023485.
44. Ryker R, Lafleur E, McManis B, and Cox KC. Online privacy policies: an assessment of the fortune E-50. J Comput Inf Syst. 2002; 42(4):15-20. doi: 10.1080/08874417.2002.11647048.
45. Milne GR, Culnan MJ. Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices. J Interact Mark. 2004;18(3):15–29. doi:10.1002/dir.20009.
46. Sheehan KB. In poor health: an assessment of privacy policies at direct-to-consumer web sites. J Public Policy Mark. 2005;24(2):273–83. doi:10.1509/jppm.2005.24.2.273.
47. Vail MW, Earp JB, Antón AI. An empirical study of consumer perceptions and comprehension of web site privacy policies. IEEE Trans Eng Manage. 2008;55(3):442–54. doi:10.1109/TEM.2008.922634.
48. K-W W, Huang SY, Yen DC, Popova I. The effect of online privacy policy on consumer privacy concern and trust. Comput Hum Behav. 2012;28(3):889–97. doi:10.1016/j.chb.2011.12.008.
49. ed. p. Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. Government Information Quarterly, 35(3), 445–459. https://doi.org/10.1016/j.giq.2018.04.002
50. Marotta-Wurgler F. Self-regulation and competition in privacy policies. J Leg Stud. 2016;45(S2):S13–S39. doi:10.1086/689753.
51. Fox AK, Royne MB. Private information in a social world: assessing consumers' fear and understanding of social media privacy. J Mark Theory Pract. 2018;26(1–2):72–89. doi:10.1080/10696679.2017.1389242.
52. Pilton C, Faily S, Henriksen-Bulmer J. Evaluating privacy - determining user privacy expectations on the web. Comput Secur [Internet]. 2021;105:102241. doi:10.1016/j.cose.2021.102241.
53. Ohlhausen MK. Privacy challenges and opportunities: the role of the Federal Trade Commission. J Public Policy Mark. 2014;33(1):4–9. doi:10.1509/jppm.33.1.4.