UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY

CLTC WHITE PAPER SERIES

Representing Privacy Legislation as Business Risks

HOW TECHNOLOGY COMPANIES DISCUSS THE GDPR AND CCPA IN INVESTMENT RISK DISCLOSURES

RICHMOND WONG AND ANDREW CHONG

CLTC WHITE PAPER SERIES

Representing Privacy Legislation as Business Risks

HOW TECHNOLOGY COMPANIES DISCUSS THE GDPR AND CCPA IN INVESTMENT RISK DISCLOSURES

RICHMOND WONG AND ANDREW CHONG

January 2024

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Contents

Executive Summary

Concerns over consumers' data privacy have increased in recent years, as evidenced by the passage of legislation such as the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the California Privacy Rights Act (CPRA). Yet how decisions around data privacy are made within technology companies largely remains unclear, even though these practices represent a significant lever by which privacy rights can be protected. While technology companies have faced public and regulatory pressure to protect data privacy rights, it is not fully clear how companies assess these privacy concerns as risks, or how they make decisions that integrate privacy concerns as business risks.

To better understand how technology companies assess and frame issues related to privacy as business risks, we leveraged Form 10-K documents, annual regulatory reports for investors that publicly traded companies must file with the U.S. Securities and Exchange Commission (SEC).[1] Form 10-K documents offer a perspective into how tech companies view and frame various risks related to privacy, and serve as a starting point to understand how they integrate these risks into their decision-making in response to laws like the GDPR and CCPA.

We conducted a qualitative analysis of Form 10-K filings from nine technology companies: Microsoft, Salesforce, Facebook (now Meta),[2] Google (now Alphabet), Apple, Amazon, Uber, Airbnb, and DoorDash. This report outlines five framings that companies use to make their privacy practices legible to investors as business risks:

1. Regulatory risks: Describing potential direct penalties and legal consequences the company might face, such as fines or government investigation.
2. Reputational risks: Describing how the company's reputation among the public may be adversely affected if the company is found to have violated data privacy laws.
3. Risks related to internal business practices: Describing how the laws may affect the company's existing business practices, such as making targeted advertising practices more costly.

1 Based on work by Richmond Wong, Andrew Chong, and R. Cooper Aspegren in: "Privacy Legislation as Business Risks: How GDPR and CCPA are Represented in Technology Companies' Investment Risk Disclosures." (2023). ACM Press. *Proceedings of the ACM on Human-Computer Interaction, 7* (CSCW1). https://doi.org/10.1145/3579515.

2 We refer to the company as "Facebook" in most of this paper, as the documents we analyzed were published before the company was renamed as "Meta."

4. Risks related to external stakeholders and ecosystems: Describing how the laws may increase costs or risks in their relationships with stakeholders outside of the company, such as additional data privacy auditing or training that the company has to do with vendors.
5. Cybersecurity risks: Describing new steps or reporting requirements that the company may need to conduct in relation to cybersecurity.

In analyzing how technology companies discuss privacy risks, we find the following main take-aways and implications:

- Companies disclose both direct ways (such as legal fines and penalties) and indirect ways (such as reputational harms) that their business may be affected by privacy and data protection legislation, suggesting that privacy legislation has a range of effects that extend beyond regulatory compliance.
- Form 10-K filings provide insight into companies' practices related to privacy, including privacy legislation's impact on companies' business models and data collection practices.
- Researchers and designers might consider new interventions and designs that help investors and business decision-makers make more privacy-preserving decisions.
- Privacy advocates and practitioners could more effectively use the rhetorical framings of business risk when advocating for more privacy-preserving business practices.
- New forms of disclosures and transparency reporting may help address data privacy as a part of corporate governance.

Introduction

Technology consumers and users increasingly cite concerns about the privacy of their personal information when interacting with technology companies that create software or online products and services. In 2019, 81% of Americans felt that they had little or no control over the data that companies collect, according to a poll by Pew Research.[3] Despite these widely shared concerns, media reports of violations of privacy by large or popular technology companies remain common.[4]

Concerns over power exercised by large technology companies over the collection and use of personal data has led to the passage of legislation such as the EU's General Data Protection Regulation (GDPR) in 2016 and the California Consumer Privacy Act (CCPA) in 2018. However, it is still unclear to what extent these laws have changed or affected technology companies' practices.

To better address problems of privacy related to large technology companies (whether through technical, social, or policy-based means), research is needed to understand how companies represent their decision-making and frame risks in response to existing privacy legislation. Financial motivations are a strong influence on technology companies' actions. Thus, this paper investigates how companies represent risks related to privacy and data protection regulation to financial investors.

To accomplish this, we conducted a qualitative document analysis of nine major technology companies' annual Form 10-K regulatory filings with the U.S. Securities and Exchange Commission (SEC), an agency that regulates financial markets. The Form 10-K is a document required by law for publicly traded companies in the U.S. to inform potential and current investors, and includes disclosures about the company's business practices, financial condition, and potential business risks.

3 Auxier, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information." Pew Research, 2019. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

4 Doffman, Zak. "Why You Shouldn't Use Google Chrome After New Privacy Disclosure." *Forbes*, March 20, 2021. https://www.forbes.com/sites/zakdoffman/2021/03/20/stop-using-google-chrome-on-apple-iphone-12-pro-max-ipad-and-macbook-pro/?sh=1a1d5fb54d08; Elkind, Peter, Jack Gillum, and Craig Silverman. "How Facebook Undermines Privacy Protections for Its 2 Billion WhatsApp Users." *ProPublica*, September 7, 2021. https://www.propublica.org/article/how-facebook-undermines-privacy-protections-for-its-2-billion-whatsapp-users.

We asked: How are privacy and data protection laws, specifically the GDPR and CCPA, represented as business risks in the Form 10-K risk disclosures of technology companies?

We found that companies disclose that privacy and data protection regulation could lead to both direct potential impacts (such as legal fines and penalties) and indirect impacts (such as reputational harms). In this paper, we outline five common framings that companies used to make the GDPR and CCPA legible to investors as business risks. We discuss how these findings can provide insight into issues related to corporate practice and governance, and can expand the possibilities for privacy research, design, practice, and policy.

Background

RESEARCH BACKGROUND

Much of the prior research on data privacy and privacy risk has focused on a user-centered perspective.[5] Privacy scholars Gürses and Hoboken, however, argue that in addition to user perspectives on privacy, it is also important to understand the contexts and practices where technologies are produced. They argue that research "into [technology] production can help us better engage with new configurations of power that have implications for fundamental rights and freedoms, including privacy." Their research uses case studies to illustrate how agile software development practices create new considerations for data privacy.[6]

This paper extends this line of research by looking at companies' communications with shareholders and investors as a practice where particular conceptions and definitions of privacy (and risks related to privacy) are shared and promoted.

COMPANIES' FORM 10-K FILINGS WITH THE U.S. SECURITIES AND EXCHANGE COMMISSION

We investigated companies' Form 10-K, annual reports that are filed with the U.S. Securities and Exchange Commission (SEC), a government agency that helps regulate financial markets against manipulation. Publicly traded companies are required to file truthful annual reports for current and potential investors (and regulators) to read. The SEC's regulatory framework is based on mandatory disclosure to provide potential investors with information about a company's practices.

5 Degeling, Martin, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. "We Value Your Privacy . . . Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy." *Informatik Spektrum* 42, no. 5 (October 2019): 345–46. https://doi.org/10.1007/s00287-019-01201-1; Vitak, Jessica, Michael Zimmer, Anna Lenhart, Sunyup Park, Richmond Y. Wong, and Yaxing Yao. "Designing for Data Awareness: Addressing Privacy and Security Concerns About 'Smart' Technologies." In *Companion Publication of the 2021 Conference on Computer Supported Cooperative Work and Social Computing*, 364–67. New York, NY, USA: ACM, 2021. https://doi.org/10.1145/3462204.3481724; Wang, Yang. "The Third Wave? Inclusive Privacy and Security." In *Proceedings of the 2017 New Security Paradigms Workshop — NSPW 2017*, 122–30. New York, New York, USA: ACM Press, 2017. https://doi.org/10.1145/3171533.3171538.

6 Gürses, Seda, and Joris Van Hoboken. "Privacy After the Agile Turn." In *Cambridge Handbook of Consumer Privacy*, edited by Jules Polonetsky, Omer Tene, and Evan Selinger. Cambridge University Press, 2017. https://doi.org/10.31235/osf.io/9gy73.

The framework of disclosure for individual decision-making has been used in other domains in the U.S. beyond financial investing, such as providing privacy policies to users.[7] We note that this type of disclosure framework has limitations; some privacy scholars have argued that disclosures may place too great a burden on consumers and may not do a good job of informing users.[8] While there is debate about the efficacy of this framework, disclosure is presumed "to promote market efficiency and ensure a well-informed investing population," according to lawyer Rebecca Rabinowitz.[9]

Companies' Form 10-Ks are filed annually and are publicly accessible via the SEC's database. A Form 10-K must include 15 sections that disclose information including the company's business practices, financial data, and potential business risks, among other details. Form 10-Ks are written by a company's management (or in practice, by legal attorneys on their behalf), and the CEO and CFO must sign and certify the accuracy of the 10-K. The SEC reviews the 10-K to ensure compliance. The main audiences that read these documents include investors or potential investors, financial analysts, and finance media reporters.

We looked specifically at the section of the Form 10-K that discusses potential risks that companies face: 1A, Risk Factors. This section generally qualitatively describes the nature of the risk, but does not always include a description of how the company is addressing that risk. The concept of risk stems from recognizing inherent uncertainty about the future and the types of responses people can take in the present to address or manage that risk.[10] In the business risk disclosure context, the definition of risk disclosure tends to be broad, informing the reader of "any opportunity or prospect, or of any hazard, danger, harm, threat or exposure, that has already impacted upon the company or may impact upon the company in the future."[11]

Prior research has investigated categories of risk disclosure, including: business risks, such as uncertainty about the demand for products and the price of production; financial risks, such as changes in market prices or uncertainty about credit obligations; operational risks (related to internal processes and people, or external events), such as the potential for technology failures

7 Calo, M. Ryan. "Against Notice Skepticism in Privacy (and Elsewhere)." *Notre Dame Law Review* 87, no. 3 (2012): 1027–72.

8 McDonald, Aleecia M., and Lorrie Faith Cranor. "The Cost of Reading Privacy Policies." *I/S: A Journal of Law and Policy for the Information Society* 4, no. 3 (2008): 543–68.; Solove, Daniel J. "Privacy Self-Management and the Consent Dilemma." *Harvard Law Review* 126 (2013): 1880–1903.

9 Rabinowitz, Rebecca. "From Securities to Cybersecurity: The SEC Zeroes In on Cybersecurity." *Boston College Law Review* 61, no. 4 (2020): 1535.

10 Beck, Ulrich. "Living in the World Risk Society." *Economy and Society* 35, no. 3 (2006): 329–45. https://doi.org/10.1080/03085140600844902.

11 Linsley, Philip M., and Philip J. Shrives. "Risk Reporting: A Study of Risk Disclosures in the Annual Reports of UK Companies." *The British Accounting Review* 38, no. 4 (December 2006): 387–404. https://doi.org/10.1016/j.bar.2006.05.002.

or fraud by management and employees; and legal and regulatory compliance risks, such as facing lawsuits or increased costs from new regulations.[12]

The main purpose of Form 10-Ks is to ensure that companies disclose truthful information, rather than provide biased statements and perspectives as might be found in advertisements or press releases. In Form 10-Ks, companies must provide accurate information about events that have previously happened or that are currently happening, but they have some protection from legal liability when making forward-looking statements (including statements about future risks) due to uncertainty about the future. Some critics have voiced concerns that companies are allowed to disclose generic and extensive boilerplate text by listing all possible uncertainties, or present outright misleading forward-looking risk statements.[13] Others' research suggests that disclosure of risks, even if uncertain, nevertheless improves market efficiency.[14] While there is debate about the efficacy of risk disclosures, this paper focuses on the discourses and framings of risk factors, rather than their effects.

There are some guardrails against providing misleading and false information in Form 10-Ks. The SEC has the authority to bring enforcement actions against companies that submit misrepresentative or misleading statements, including those made in risk disclosures. In 2019, the SEC issued a $100 million penalty against Facebook for presenting misuse of user data as a hypothetical, instead of disclosing that they knew misuse had actually occurred when Cambridge Analytica misused user data.[15] The SEC has also taken measures to try to improve the quality of information in the "Risk Factors" sections of the form, for example by adding amendments to make companies disclose "material" risks and provide summaries of risks when they go beyond a certain length. Investors may also bring lawsuits against a company for providing false or misleading statements.

12 Onoja, Anthony, and Godwin O Agada. "Voluntary Risk Disclosure in Corporate Annual Reports: An Empirical Review." *Research Journal of Finance and Accounting* 6, no. 17 (2015): 1–8.

13 Bao, Yang, and Anindya Datta. "Simultaneously Discovering and Quantifying Risk Types from Textual Risk Disclosures." *Management Science* 60, no. 6 (June 2014): 1371–91. https://doi.org/10.1287/mnsc.2014.1930.; Ferraro, Matthew F. "'Groundbreaking' or Broken? An Analysis of SEC Cybersecurity Disclosure Guidance, Its Effectiveness, and Implications." *Albany Law Review* 77 (2014).; Morales Olazábal, A. N.N. "False Forward-Looking Statements and the PSLRA's Safe Harbor." *Indiana Law Journal* 86, no. 2 (2011): 595–643.

14 Dietrich, J. Richard, Steven J. Kachelmeier, Don N. Kleinmuntz, and Thomas J. Linsmeier. "Market Efficiency, Bounded Rationality, and Supplemental Business Reporting Disclosures." *Journal of Accounting Research* 39, no. 2 (September 2001): 243–68. https://doi.org/10.1111/1475-679X.00011.

15 U.S. Securities and Exchange Commission. "Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data," 2019. https://www.sec.gov/news/press-release/2019-140.

Since the 1970s, the Federal Trade Commission (FTC) has been the main U.S. regulator to consider issues related to digital privacy,[16] but in 2011, the SEC began to publish voluntary guidelines for companies to specifically discuss cybersecurity risks and incidents. The SEC's guidance suggested that companies had a duty to disclose information related to cybersecurity risks to potential investors.[17] This guidance was updated in 2018, in part to emphasize the importance of companies having cybersecurity policies and procedures in place.[18] While some scholars have questioned the effectiveness of these disclosures in improving companies' cybersecurity practices (in part due to the voluntary nature of the guidelines),[19] researchers have found that companies have increased discussion of cybersecurity in their Form 10-Ks over time based on the presence and length of cybersecurity-related disclosures, and that companies increase their discussion of cybersecurity in Form 10-Ks after experiencing a cybersecurity incident or breach.[20]

While prior research has analyzed cybersecurity discourses in SEC disclosures, comparatively little has focused specifically on privacy. One exception is Fathaigh et al.'s analysis, which used Form 10-Ks filed by mobile app companies between 2008-2017 to understand their data collection and use practices; the researchers found that these companies disclosed their compliance with privacy laws as part of their risk factors. They argued that "[c]onsidering the growing business and financial market implications of privacy governance and regulation, which the SEC has also recognized, we believe SEC disclosure analysis has become an important additional source of information for privacy research (and practice)."[21] They also argued that SEC filings can provide evidence of the impact of the law on companies' business models and data practices, and that SEC filings "tend to reveal more information [. . .] than the information contained in a company's privacy policy."[22] We utilize their approach of SEC disclosure analysis to specifically understand how the GDPR and CCPA are discussed.

16 Hoofnagle, Chris Jay. "Online Privacy." In *Federal Trade Commission Privacy Law and Policy*, 145–92. Cambridge: Cambridge University Press, n.d. https://doi.org/10.1017/CBO9781316411292.007.

17 U.S. Securities and Exchange Commission. "CF Disclosure Guidance: Topic No. 2: Cybersecurity," 2011. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

18 U.S. Securities and Exchange Commission. "Commission Statement and Guidance on Public Company Cybersecurity Disclosures." 17 CFG Parts 229 and 249, 2018.

19 Avellan, Norah C. "The Securities and Exchange Commission and the Growing Need for Cybersecurity in Modern Corporate America." *Washburn Law Journal* 54, no. 1 (2014): 193–226.; Ferraro, Matthew F. "'Groundbreaking' or Broken? An Analysis of SEC Cybersecurity Disclosure Guidance, Its Effectiveness, and Implications." *Albany Law Review* 77 (2014).

20 Li, He, Won Gyun No, and Tawei Wang. "SEC's Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors." *International Journal of Accounting Information Systems* 30 (September 2018): 40–55. https://doi.org/10.1016/j.accinf.2018.06.003.

21 Ó Fathaigh, Ronan, Joris van Hoboken, and Nico van Eijk. "Mobile Privacy and Business-to-Platform Dependencies: An Analysis of SEC Disclosures." *Journal of Business and Technology Law* 14, no. 1 (2018): 49–105.

22 Ibid.

GDPR AND CCPA

In this section, we provide a brief background of the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). The GDPR's lineage starts with the 1995 Data Protection Directive, which aimed to provide personal data protections to individuals living in the EU. In 2012, the European Commission published the proposal that would evolve into the GDPR. The GDPR was ultimately passed in May 2016 and went into effect in May 2018.[23]

The CCPA resulted from a ballot initiative that was negotiated into a legislative measure in the California State Legislature. The CCPA was passed into law in 2018. After undergoing several amendments, the law went into effect in 2020. That year, a separate ballot initiative, Proposition 24 or the California Privacy Rights Act (CPRA), passed in California, which amended and replaced the CCPA by establishing a California Privacy Protection Agency and increasing consumer rights of action. The CPRA went into effect in 2023. (However, since most of the documents we analyzed were published before the California Privacy Rights Act ballot initiative passed, few companies in our corpus discussed the CPRA.)

The GDPR and CCPA provide similar protections to consumers while having several key differences.[24] The regulations are based upon similar definitions of personal data and information, mandate similar requirements for company data security, provide similar data portability and deletion rights, and invoke penalties against companies that violate them. The GDPR fines companies the higher of 20M Euros or 4% of worldwide company revenue, while the CCPA currently charges $2,500 to $7,500 per violation while offering companies a 30-day period to correct their mistakes to avoid being fined.[25] The GDPR also allows for individuals to claim damages from companies following certain types of data breaches. The GDPR offers a broader array of rights to consumers than the CCPA, including the right to rectification (the right to have inaccurate data about you updated), and the right to object to automated decision-making. The GDPR is rooted in a human rights framework and applies to any company or entity that processes the personal data of E.U. residents. The CCPA is rooted in a consumer protection framework, and more narrowly applies to businesses that meet certain thresholds related to revenue or the number of California residents' personal information they collect. Most large technology companies are subject to both laws as they operate in both the US and EU.

23 Hoofnagle, Chris Jay, Bart van der Sloot, and Frederik Zuiderveen Borgesius. "The European Union General Data Protection Regulation: What It Is and What It Means." *Information & Communications Technology Law* 28, no. 1 (January 2, 2019): 65–98. https://doi.org/10.1080/13600834.2019.1573501.

24 Goldman, Eric. "Introduction to the California Consumer Privacy Act (CCPA)," 2020. https://ssrn.com/abstract=3211013.; Jehl, Laura, and Alan Friel. "CCPA and GDPR Comparison Chart." Practical Law, 2019.

25 The newer CPRA removed this 30 day "cure" period.

Data and Methods

While companies across multiple industries are affected by privacy and data protection regulation because they handle personal data, we decided to focus on large technology companies that produce platforms for online collaboration, work, communication, and social activity. We aimed to purposively curate a sample of companies that would capture the breadth and diversity of this type of company, rather than attempt a complete accounting or a statistically representative sample of all technology companies.

We considered such factors as the age of the company, the main business model or source of revenue, and whether a company might have an outsized influence on best practices due to its high media visibility or regulatory scrutiny. After several discussions among the authors, we selected nine companies, which are described in Table 1.

Table 1. List of Companies Analyzed

Company Name	Initial Public Offering Year	Main Revenue-Generating Product(s) or Service(s)	Years of Form 10-K Analyzed[26]
Microsoft	1986	Software and Services	2015–2020
Salesforce	2004	Software and Services	2015–2020
Facebook (now Meta)	2012	Advertising	2015–2020
Google (now Alphabet)	2004	Advertising	2015–2020
Apple	1980	Hardware Products and Services	2015–2020
Amazon	1997	eCommerce (Products and Services)	2015–2020
Uber	2019	Gig Economy Platform	2019–2020
Airbnb	2020	Gig Economy Platform	2020
DoorDash	2020	Gig Economy Platform	2020

The GDPR was passed in 2016 and went into effect in 2018; the CCPA was passed in 2018 and went into effect in 2020. We downloaded companies' annual Form 10-Ks starting from 2015 (pre-dating the GDPR's passage) until 2020, using the SEC's public database. Because only publicly traded companies are required to file a Form 10-K, three companies with more recent initial public offerings — Uber, DoorDash, and Airbnb — had fewer years' worth of filings.

26 Each company files its Form 10-K annually in a month based on their fiscal year calendar. We refer to companies' Form 10-K based on the calendar year when they filed their documents.

In total, our corpus contains 40 Form 10-Ks from the nine companies from between 2015 and 2020. We formally analyzed the Risk Factors sections (Item 1A), and skimmed other sections of the documents (such as the Item 1, Business description), to contextualize our understanding of the risks. The Risk Factors sections from these combined Form 10-Ks represent 672 total pages. (A more detailed accounting of our analysis methods can be found in our research paper.[27])

When analyzing the discourse of the risks, we specially looked at the following qualities:

- *What is the risk factor(s) stated?* For instance, risks posed by reputational damage, government investigations, data breaches, evolving regulation, etc.
- *What stakeholders are mentioned?* For example, customers, users, regulators, employees, contractors, third-party developers, etc.
- *What circumstances surrounding the risk are mentioned?* This includes additional details about the context of the risk factor. For instance, companies might note decisions by courts or regulatory authorities, the introduction of new products, the company's current data practices, types of data misuse by third parties, etc.
- *What are the stated impacts to the company based on this risk factor?* For example, facing fines and penalties, increased legal liability, brand or reputational damage, limited adoption or use of products, limited international growth, etc.

We note that our analysis is based on a limited sample of companies. While we purposively chose technology companies that we thought would provide breadth and diversity in their discussions of privacy, the GDPR, and the CCPA, it is possible that the inclusion of additional technology companies, or looking at filings from before 2015, would provide new conceptions of risk that we did not find.

27 Wong, R. Y., Chong, A., & Aspegren, R. (2023). "Privacy Legislation as Business Risks: How GDPR and CCPA are Represented in Technology Companies' Investment Risk Disclosures." ACM Press. *Proceedings of the ACM on Human-Computer Interaction, 7* (CSCW1). https://doi.org/10.1145/3579515.

Findings Part 1: When the GDPR and CCPA Emerged as Sources of Risks

We first explored when the GDPR and CCPA were specifically mentioned and discussed in the companies' Form 10-Ks. Privacy and data protection laws and regulations were mentioned across all companies, across all years. However, the frequency of specific references to the GDPR and CCPA varied across companies and years. Figure 2 provides an overview of when each company mentioned the GDPR and CCPA in their respective 10-Ks.

	2015	2016	2017	2018	2019	2020
Legislation Timeline		*GDPR Passed*		*GDPR Takes Effect* *CCPA Passed*		*CCPA Takes Effect*
Microsoft	○	○	●	●	● ●	● ●
Salesforce	○	○	○	●	● ●	● ●
Facebook	○	●	●	●	● ●	● ●
Google	○	●	●	●	● ●	● ●
Apple	○	○	○	○	○	○
Amazon	○	○	○	○	○	○
Uber (starts in 2019)					● ●	● ●
Airbnb (starts in 2020)						● ●
Doordash (starts in 2020)						●
Key:	○ generally mentions privacy laws		● mentions GDPR		● mentions CCPA	

Fig. 2. An overview of whether a Form 10-K for a given company and year mentioned the GDPR or CCPA.

In 2015, no companies explicitly mentioned the GDPR and CCPA, as neither law had been adopted at that point. Facebook came closest to mentioning the GDPR, noting that there was an incoming "data protection regulation that is pending final approval by the European legislature that may include operational requirements for companies that receive or process personal data that are different than those currently in place in the European Union, and that will include significant penalties for non-compliance" (Facebook 2015).

On the whole, however, companies focused on describing various aspects of privacy, such as a general description that different jurisdictions have considered or are considering privacy laws. Some also mentioned the EU's "right to be forgotten" directive, which required that companies delete data for specific customers in a timely manner once those customers request that they do so. Google noted that European Court rulings favoring the right to be forgotten permit customers "to demand that Google remove search results about them in certain instances, [and] may limit the content we can show to our users" (Google 2015). Salesforce mentioned the E.U. Data Protection Directive of 1995.

In 2016, with the passage of the GDPR, Facebook and Google began more explicitly describing the challenges posed by the GDPR. Facebook mentioned the GDPR in terms of decreased engagement or acceptance of terms of service, limiting its ad targeting, and being part of a suite of complex and evolving laws and regulations (both in the U.S. and internationally). Google indicated that the GDPR posed potential operational risks or legal risks.

In 2017, Microsoft joined Facebook and Google in explicitly mentioning the impact the GDPR could have on its operations. In doing so, the company noted that the law could "impede the adoption of our services or result in increased costs, legal claims, or fines against us." That year, Google raised concerns about the GDPR in a section devoted to "complex and evolving U.S. and international laws and regulation regarding privacy and data protection."

In 2018, the GDPR came into effect (meaning that it was now enforceable), while the CCPA was signed into law in California (though it would not come into effect for two more years). As a consequence, Google mentioned the CCPA as a new or existing regulation that could harm its business. That year, Google removed its reference to the GDPR in the risk factor block describing new or existing laws and regulations, but continued to reference it as an international law or regulation that served as a risk factor.

It is worth mentioning that, at this point in time, and across the remainder of years studied, the Form 10-Ks for Amazon and Apple carried no explicit references to either the GDPR and CCPA. This exclusion does not appear to result from a lower exposure to risks from international operations or reduced concerns over privacy and data protection. Rather, both companies referred to laws and regulations pertaining to privacy and data protection issues in the abstract, without mentioning specific acts or countries legislating them.

The year 2019 saw the beginning of additional mentions of the CCPA on the part of Microsoft, Salesforce, Facebook, Google, and Uber. Facebook began to devote an entire risk factor block

to discussing the GDPR and the CCPA; Salesforce would do the same in 2020. It was relatively common for companies to describe the risks posed by the CCPA in the same blocks in which they mentioned the GDPR, suggesting that these companies viewed the GDPR and CCPA similarly.

In 2020, the CCPA came into effect. Companies were largely consistent in terms of how they discussed the impacts of the GDPR and CCPA from the previous year. DoorDash, which had its IPO in 2020, mentioned the CCPA, but not the GDPR. This is likely because DoorDash did not operate in a significant fashion in Europe in 2020. The rest of the companies in the sample had operations in the E.U. (and other parts of the world), and their Form 10-Ks' mentions of the GDPR indicate that they have commensurate responsibilities to follow international data privacy laws.

Findings Part 2: How Companies Frame Discussion of Risks Related to the GDPR and CCPA

In this section, we detail five areas where companies' risk disclosures discussed privacy and data protection legislation: (1) regulatory risks, (2) reputational risks, (3) risks related to business practices, (4) risks related to external stakeholders, and (5) security risks. While these framings can overlap in practice, we discuss them separately for analytical clarity. We summarize these areas in Table 2, and expand on each framing below.

Table 2. Framings of Risks Posed by Privacy and Data Protection Regulation in Analyzed Documents

Framing	Key Concern(s)	Example
Regulatory Risks	What are the direct penalties and legal consequences we might face?	New fines or legal investigations may occur under the GDPR and CCPA that could present financial and legal risks.
Reputational Risks	How do the laws indirectly affect our reputation?	Being found in violation of a privacy or data protection law brings new public relations risks
Risks Related to Internal Business Practices	How do the laws affect how we conduct our business practices and develop our products?	The laws make it more costly to use certain business models (such as generating revenue from targeted advertising), creating financial risk.
Risks Related to External Stakeholders and Ecosystems	How do the laws affect relationships with stakeholders outside of our company?	The laws impose new obligations on enterprise clients, creating new legal liabilities for our company.
Cybersecurity Risks	How do the laws affect our cybersecurity practices?	Introduction of new data breach reporting requirements may increase the costs of responding to a data breach.

FRAMING 1: DIRECT REGULATORY RISKS

Companies frequently framed privacy regulation as a potential source of direct regulatory risks, highlighting the immediate legal penalties and fines that companies could face if found to be in violation of the law. Even before the enactment of the GDPR, companies cited other laws and regulations related to privacy and data protection, including the California Online Privacy Protection Act, the E.U. Data Protection Directive (the precursor to the GDPR), the E.U. ePrivacy

Directive, credit card processing laws, and the U.S. Federal Trade Commission's power to investigate certain privacy-related incidents.

After the passage and enactment of the GDPR and CCPA, most companies updated their existing risk factor statements related to regulatory risks to include explicit mention of the GDPR and CCPA. These framings of regulatory risk emphasized the potential costs and penalties that could result from violating these laws, including regulatory fines, increased claims and suits, and the potential for further subsequent government investigations.

Some companies also added new risk factors specifically about the GDPR and CCPA, suggesting that they were viewed as significant enough to emphasize for investors. In 2019, Facebook and Google both dedicated a new risk factor block to privacy and data protection laws, and Facebook and Salesforce additionally dedicated a new risk factor block specifically to the GDPR and CCPA.

Furthermore, companies chose to emphasize specific penalties from the GDPR or CCPA. DoorDash, Google, Microsoft, and Uber explicitly mentioned the financial penalties companies can face from regulators if found in violation of the GDPR (20 million Euros or 4% of total worldwide annual revenue, whichever is greater) or the CCPA (up to $7,500 per violation). Interestingly, Airbnb, Salesforce, and Uber also identified the CCPA's private right of action and statutory damages following a data breach. Unlike in the GDPR, the CCPA's private right of action allows individual consumers to pursue damages against companies ranging from $100–$750 after certain types of data breaches and incidents. Depending on the number of people affected by a data breach, the costs of damages under the CCPA could theoretically end up being greater than the GDPR's financial penalties.[28] Hence, companies saw different regulatory mechanisms — monetary fines by a regulatory agency, in the case of the GDPR, versus private lawsuits from individuals in the CCPA — as posing different financial risks for companies and their investors, and chose to outline them explicitly in their risk disclosures.

FRAMING 2: REPUTATIONAL RISKS

Companies were also sensitive to how privacy and data protection regulations could increase potential damage to their public reputations. In contrast to individual user complaints about violations of privacy, privacy legislation allows for a more collective shared conception of privacy

28 Kemp, Tom. "Comparing Enforcement: GDPR vs. CCPA vs. CPRA." Tom Kemp's Blog, 2020. https://www.tomkemp.ai/blog/2020/06/04/comparing-enforcement-gdpr-vs-ccpa-vs-cpra.

to come into play: if a company is found to have violated a privacy or data protection law, then that legal violation could affect a company's reputation among a broader public.

Some companies considered how legislation could lead to shared conceptions of privacy violations prior to the enactment of the GDPR and CCPA. In 2015, Facebook noted how U.S. and foreign laws and regulations related to privacy and data protection could result in "negative publicity." In later years, Facebook updated this risk factor to specifically note that the GDPR and CCPA were among the laws they were concerned about.

Other companies, however, added new discussions about reputational and brand risk to their Form 10-Ks after the GDPR came into effect. Microsoft, Google, Facebook and Salesforce all added new language discussing how violating the GDPR specifically could create reputational risks. For instance, in 2018, Google wrote:

> "If our operations are found to be in violation of the GDPR's requirements, we may [. . .] be subject to significant civil penalties, business disruption, and *reputational harm*, any of which could have a material adverse effect on our business." (Google 2018, emphasis added)

By 2020, these same four companies began to mention the CCPA alongside the GDPR. These framings of reputational risk under the GDPR and CCPA stemmed from the potential negative publicity that could result from the broad shared public attention of being investigated or being found in violation of the law, rather than from violating individual users' expectations or perceptions of privacy.

Interestingly, companies were also sensitive to how *perceived* violations of privacy could increase their business risk, often using language such as "actual or perceived" with regards to security and privacy breaches. DoorDash noted that privacy and security incidents even among competitors could affect its reputation, as such events would damage the "public perception" of the industry as a whole:

> "[A]ny negative publicity, whether such incident occurred on our platform or on our competitors' platforms, could adversely affect our reputation and brand or public perception of our industry as a whole, which could negatively affect demand for platforms like ours, and potentially lead to increased regulatory or litigation exposure." (Doordash, 2020)

Privacy legislation is thus framed as introducing reputational risks in multiple ways, including more direct risks if a company is found in violation of a law, and indirect risks, resulting from shifting public perceptions about a company or the technology industry more broadly.

FRAMING 3: RISKS RELATED TO INTERNAL BUSINESS PRACTICES

In their Form 10-K filings, the companies described how privacy regulation increased risk related to their internal business practices, such as by requiring new data transfer procedures that increased costs and potential liability, reducing the efficacy of their existing practices, or increasing risks associated with new product lines that could expose companies to greater scrutiny around privacy.

Five companies (Airbnb, Facebook, Google, Microsoft, and Salesforce) noted **potential challenges to their business practice of cross-border data transfers**. The EU-US Privacy Shield governed the transfer of personal data from the E.U. to the U.S., but faced a series of legal challenges and was invalidated in 2020 by the E.U. Court of Justice, which broadly found that its data transfer mechanisms did not provide E.U. citizens with a high enough level of protection, based on the GDPR. This suggests that the Court's decision increased business costs and potential liability risks for the many companies that transfer personal data between countries.

Companies also described how privacy legislation had a direct effect on their existing business practices. **Companies that relied on advertising reported in particular how the GDPR and CCPA, among other regulations, impacted their ability to track and target users and thereby had a direct impact on revenue**. Facebook, which also reported in their Form 10-K that 97% of their fourth quarter 2020 revenue came from advertising, explicitly described how the GDPR and CCPA, among other regulations, impacted its ability to track and target users and had a direct impact on its revenue:

> "Our advertising revenue is dependent on targeting and measurement tools that incorporate these [user activity data] signals, and any changes in our ability to use such signals will adversely affect our business. For example, legislative and regulatory developments, such as the GDPR, ePrivacy Directive, and CCPA, *have impacted*, and we expect will continue to impact, our ability to use such signals in our ad products. [. . .] These developments *have limited our ability to target and measure the effectiveness of ads on our platform, and negatively impacted our advertising revenue*." (Facebook 2020, emphasis added)

Google and Facebook also both noted how new privacy-enhancing technologies like ad blockers presented financial risk by negatively affecting their advertising revenue.

Companies that use advertising to grow their user base described effects and risks from privacy legislation. Airbnb described that their long-term growth strategy in part involved practices to "invest in growing the size and quality of our host community" and to "grow and engage our guest community" (Airbnb 2020); DoorDash described their goals to increase their consumer reach, which included paid marketing campaigns. However, Airbnb went on to describe how the GDPR could make it more difficult to market to potential new platform users and achieve this growth:

> "The GDPR also imposes conditions on obtaining valid consent [. . .]. Widespread adoption of regulations that significantly restrict our ability to use performance marketing technology could adversely affect our ability to market effectively to current and prospective hosts and guests, and thus materially adversely affect our business [. . .]." (Airbnb 2020)

In contrast, **companies for whom enterprise clients formed a large part of their business described how privacy legislation could increase the costs of educating customers** on new laws and regulations. For example, Salesforce noted the potential risk of increased costs of "education regarding privacy and data protection laws and regulations" (Salesforce 2015) during the sales process.

More broadly, companies described how **privacy legislation and privacy concerns could create new risks to consider in the development of new data-intensive products**. In 2015, Google and Microsoft noted how their increased number of web- and cloud-based offerings meant that more personal data was being collected, leading to greater potential for privacy and data protection breaches, which could in turn lead to legal liability or reputational harm. In following years, Microsoft and Salesforce included a new risk factor discussing ethical risks related to their development and deployment of artificial intelligence (AI) systems, including privacy:

> "We are building AI into many of our offerings and we expect this element of our business to grow. [. . .] If we enable or offer AI solutions that are controversial because of their impact on human rights, *privacy*, employment, or other social issues, we may experience brand or reputational harm." (Microsoft 2018, emphasis added)

Overall, we find that this rhetorical framing helps us understand how companies with different business models — such as generating advertising revenue, versus trying to grow a user or subscriber base, or sell to enterprise clients — were affected in different ways by the privacy legislation.

FRAMING 4: RISKS RELATED TO EXTERNAL STAKEHOLDERS AND ECOSYSTEMS

Companies also discussed how privacy legislation such as the GDPR and CCPA might present risks to existing relationships with external stakeholders, including users, enterprise clients, contractors, or third-party developers. Different companies related the legislation to different ecosystems of stakeholders with which they interact.

Several companies described **business risks stemming from their own users' actions to exercise their privacy rights**. Airbnb noted that the effectiveness of its digital marketing could be negatively affected if users decided not to accept "cookies," small files used for tracking online behavior. Facebook specifically described how the GDPR had led to greater numbers of users opting out of some forms of advertising:

> "We rely on data signals from user activity on websites and services that we do not control in order to deliver relevant and effective ads to our users. [. . .] *In particular, we have seen an increasing number of users opt out of certain types of ad targeting in Europe following adoption of the GDPR*, and we have introduced product changes that limit data signal use for certain users in California following adoption of the CCPA." (Facebook 2020, emphasis added).

Facebook noted that these opt-outs negatively impacted its ability to target and measure advertisements and "negatively impacted our advertising revenue" (Facebook 2020). In this framing, users exercising their data protection rights under the GDPR were framed as a business risk to Facebook, as their actions resulted in reduced advertising revenue.

Other companies face **risks and challenges stemming from the practices of their enterprise clients**. Salesforce described new risks emerging from enterprise clients (described as "customers") in a GDPR and CCPA context:

> "Although we [. . .] have invested in addressing these developments, such as GDPR and CCPA readiness, these laws may require us to make additional changes to our services to enable Salesforce *or our customers* to meet the new legal requirements, and may also increase our potential liability exposure through higher potential penalties for non-compliance. [. . .] These and other requirements could [. . .] impact our ability or our customers' ability to offer our services in certain locations, to deploy our solutions, to reach current and prospective customers, or to derive insights from customer data globally." (Salesforce, 2019, emphasis added)

Salesforce noted that the responsibility of complying with GDPR and CCPA rules extended to its enterprise customers. This could indirectly increase Salesforce's exposure to legal liability, and also limited how Salesforce was able to use data originally collected by enterprise customers.

Companies also noted **risks stemming from other platforms' efforts to address privacy**, highlighting the interconnectedness and reliance that major technology companies have on other companies' platforms and services. Facebook discussed how its advertising revenue depended in part on services not controlled by the company, such as Apple's and Google's mobile operating systems and browsers. In particular, these companies had made privacy-related changes that made it more difficult to track and advertise to users.

> "[M]obile operating system and browser providers, such as Apple and Google, have announced product changes as well as future plans to limit the ability of application developers to collect and use these signals to target and measure advertising." (Facebook 2020)

Similarly, other companies that greatly relied on mobile apps — including Airbnb, Facebook, DoorDash and Uber — noted how privacy-preserving data policy changes in Apple's or Google's mobile operating systems and browsers could present potential business risks.

Some companies, particularly gig economy companies Airbnb, DoorDash, and Uber, also described **privacy tradeoffs among different groups of users**, such as drivers and riders, or hosts and guests. These companies act as custodians of the privacy interests of different groups on their platform, making decisions that can result in trade-offs between them. For instance, Airbnb was explicit about the privacy risks that can result from interactions related to hosts and guests. They described the use of screening procedures such as background checks to reduce risks of privacy violations by Airbnb hosts, which included, for example, the use of "undisclosed hidden cameras" at properties used by hosts to watch guests. However, they noted that "the evolving regulatory landscape . . . in the data privacy space" (Airbnb 2020) may make it more difficult to perform such screening.

Similarly, DoorDash described its reliance on third-party providers that provided background checks on its drivers as a safety mechanism for customers and merchants on the platform, but noted how the extent of background checks differentially increased risks for different sets of stakeholders. On one hand, "less thorough" checks may result in facing "negative publicity or becom[ing] subject to litigation" in the future, especially if people misuse the platform (DoorDash 2020). On the other hand, DoorDash expressed awareness that more thorough checks

could generate pushback from deliverers, who may find such checks overly invasive of their privacy. Furthermore, they described how third parties conducting background checks may themselves be subject to privacy violations or data security breaches.

Airbnb's and DoorDash's discussions of privacy concerns as they relate to the different groups their platforms serve reflect the complex ways that privacy concerns affect companies. The actions to protect the safety and privacy of one group (such as customers or riders) may potentially increase the risks of privacy violations for another group (such as drivers or hosts subject to background checks). Their discussion underlines tensions in the custodial role these companies perform in balancing the privacy interests of different sets of users, and how evolving privacy legislation may make it easier or harder to address the needs of these different groups.

FRAMING 5: CYBERSECURITY RISKS

Companies disclosed cybersecurity risks in 10-K filings before the enactment of the GDPR and CCPA, due to prior SEC guidelines recommending that companies include risk disclosures about cybersecurity. While the GDPR and CCPA focus on data protection and privacy, they have provisions related to cybersecurity, including: new obligations to protect the security of data, requirements to report data breaches to regulatory authorities, and, in some cases, payments to consumers affected by the data breaches. We found that companies added mentions of the GDPR and CCPA to their existing risk disclosures about cybersecurity.

Primarily, companies described that the laws created new requirements for companies to follow in the event of a security breach. Other companies used their Form 10-Ks to disclose security breaches they had experienced, following the guidelines set forth by the SEC about cybersecurity disclosures.[29] For example Facebook disclosed that it was under investigation by the Irish Data Protection Commission, the authority in Ireland in charge of enforcing the GDPR, in the aftermath of a cyberattack in September 2018 (Facebook 2018).

While the GDPR and CCPA are commonly discussed in terms of data protection and privacy, they also emerge in companies' discussion of security, particularly because of the laws' provisions related to data breaches.

29 U.S. Securities and Exchange Commission. "Commission Statement and Guidance on Public Company Cybersecurity Disclosures." 17 CFG Parts 229 and 249, 2018.

What Can We Learn about Privacy from SEC Filings?

Several insights emerged from analyzing technology companies' Form 10-Ks. Notably, the types of risks discussed in these documents focused on potential harms that a company might face, rather than the types of risks that might lead to a violation of privacy. Our analysis of how privacy legislation is framed as business risks reveals the complex accounting that takes place within companies.

PRIVACY AND DATA PROTECTION LAWS POSE INDIRECT RISKS, BEYOND DIRECT REGULATORY RISKS

We found that privacy legislation and regulation affect technology companies in multi-faceted ways. Prior research studied how companies have complied with the GDPR and CCPA.[30] While these are useful evaluations, they focus on the direct effects of regulation.

Analyzing Form 10-Ks shows how companies frame the effects and risks from privacy legislation as going beyond direct regulatory effects, such as fines and penalties. Such laws also indirectly affect companies, for instance by introducing reputational risks. By setting a public legal standard of privacy against which firms can be measured, such laws create new opportunities for negative media coverage and for public opinion to shift on companies' privacy and data protection behaviors. This may create new incentives for companies to act in privacy-preserving ways, as companies may also be wary of news headlines that state that they have broken the law or violated consumers' privacy.

Other companies described how the GDPR and CCPA create risks specific to their own operations and business models. For instance, Salesforce noted that the laws created additional obligations to educate their enterprise clients, and DoorDash and Airbnb noted how privacy legislation may make it difficult for them to rely on targeted advertising to grow their user base.

30 Samarin, Nikita, Shayna Kothari, Zaina Siyed, Primal Wijesekera, and Jordan Fischer. "Investigating the Compliance of Android App Developers with the CCPA." Workshop on Technology and Consumer Protection (ConPro '21), 2021.; Wong, Janis, and Tristan Henderson. "The Right to Data Portability in Practice: Exploring the Implications of the Technologically Neutral GDPR." International Data Privacy Law 9, no. 3 (August 1, 2019): 173–91. https://doi.org/10.1093/idpl/ipz008.

Privacy and data protection laws are thus framed in somewhat contradictory ways by companies. At some points, *violating* user privacy is framed as potentially harmful to companies due to the consequences they may face, particularly in the regulatory, reputational, and cybersecurity risk framings. However, at other points, *providing* users with increased privacy is framed as potentially harmful to the companies due to increased costs or decreased revenue resulting from changing their business practices, particularly in the internal business practices and external stakeholders risk framings. These tensions reflect corporate decision-making weighing different tradeoffs and costs related to privacy. Rather than framing privacy as something that is "good for the user," this discourse depicts privacy as a more complicated business decision that presents multiple types of business risks.

PROVIDING INSIGHT INTO COMPANY PRACTICES RELATED TO PRIVACY

While the "Risk Factors" sections of companies' annual reports contain forward-looking statements that describe things that could happen, they also contain statements of fact that help shed light on actual company practices and provide contextual information about their privacy practices. This builds on Fathaigh et al.'s insight that "SEC filings can provide evidence of specific impact on a company's business model and data collection practices."[31]

Some risk factors also provide factual disclosures. For instance, Facebook noted specific practices that it changed in response to the GDPR, including changing its consent process in Europe or its inability to use certain tracking signals. Several companies also disclosed regulatory investigations they faced and breaches of privacy or security that occurred.

The risk factor disclosures also help provide contextual information that suggests why companies are sensitive to different concepts of privacy or why they instill or prioritize some protections over others. For instance, Google and Facebook noted in their Form 10-Ks that 80% of their 2020 revenue — and 97% of their fourth-quarter 2020 revenue — came from advertising. This helps contextualize the magnitude of business risks they faced when privacy tools like ad blockers and privacy legislation made their tracking and advertising practices more difficult. Furthermore, Facebook reported facing negative impacts on their advertising revenue after the passage of the GDPR, which suggested that the GDPR's efforts have been successful in making it more difficult for companies to utilize targeted advertising. It also suggests that

31 Ó Fathaigh, Ronan, Joris van Hoboken, and Nico van Eijk. "Mobile Privacy and Business-to-Platform Dependencies: An Analysis of SEC Disclosures." *Journal of Business and Technology Law* 14, no. 1 (2018): 49–105.

legislation that prioritizes online behavioral tracking as a dominant privacy issue will have a greater effect on these particular companies.

Gig economy companies like Airbnb, DoorDash, and Uber provide contextual information that suggests they are sensitive to the intersection of physical security and privacy of different types of users on their platforms. For instance, the use of background checks on Airbnb hosts and DoorDash drivers/dashers potentially poses risks of privacy violations of those platform users, even as they are intended to assure guests or customers of their physical safety. In these instances, the promotion of privacy or safety for one group of stakeholders can impose privacy or safety costs on another group of stakeholders.

The factual information provided in Form 10-K Risk Factors can help researchers better understand some of the motivations behind companies' actions, and provides some evidence of *how* privacy and data protection legislation is affecting companies' practices.

HIGHLIGHTING THE INTERCONNECTEDNESS AMONG TECHNOLOGY COMPANIES AND PLATFORMS

Our analysis highlights dependencies between technology companies and how their business models may come into conflict. Airbnb, DoorDash, Facebook, and Uber noted how they are dependent on Apple and Google's mobile operating systems and platforms for their mobile applications. In particular, Apple's publicized privacy-related changes to iOS in 2021[32] that allowed users to opt out of targeted advertising from apps were noted by these other companies as a business risk, since those changes made it harder to track or advertise to users. Further contextualizing these efforts, Airbnb and DoorDash both noted that their growth strategy included gaining more consumer reach through advertisements. Thus privacy-enhancing actions taken by one company or platform can present business risks to another company.

This perspective helps highlight the interconnectedness of platforms, and suggests that researchers might also consider addressing privacy at a platform or multi-platform level, rather than at an individual user level. Changing privacy procedures or policies at a platform level can have outsized effects by also affecting other companies that rely on that platform. Likewise, a privacy-insensitive decision by a platform may create new risks to other services and companies that rely on it.

32 See https://www.vox.com/recode/22404323/ios-14-app-tracking-transparency-opt-out

Implications

We consider implications for multiple audiences:

IMPLICATIONS FOR RESEARCHERS AND DESIGNERS

First, we suggest that **efforts to change privacy outcomes must engage in thinking about privacy through a broader set of lenses beyond individual users**. Much of technology research focuses on privacy as a problem of user-centered design and individuals' decision-making.[33] Our analysis of how companies publicly frame business risks to (financial) stakeholders suggests that privacy is framed as more than a user-centered issue, but is also framed in terms such as regulatory compliance, public relations and reputation, or its effects on business models. By understanding how companies frame and represent business risks, researchers can consider a range of technical, social, or policy interventions that might work within companies' governance systems.

Second, **studying discourses and practices related to financial investment in technology companies provides new insights into the practices of technology production**. For instance, major large institutional investors have made statements that they will make investment decisions in part based on companies' environmental sustainability practices, potentially shifting corporate sustainability practices.[34] What might it take for institutional investors to view issues related to privacy and other digital harms as important enough to consider as they make investment decisions?[35] How do these investment and business decisions result in changes in the technical design and user experiences of digital platforms?

Third, this research suggests opportunities for **interaction designers to design for a new audience: investors and other stakeholders involved in financial investment processes**. Most prior research on interaction design and privacy focuses on designing to help empower

33 Wong, Richmond Y., and Deirdre K. Mulligan. "Bringing Design to the Privacy Table: Broadening 'Design' in 'Privacy by Design' Through the Lens of HCI." In CHI Conference on Human Factors in Computing Systems (CHI 2019), 2019. https://doi.org/10.1145/3290605.3300492.

34 BlackRock. "The Tectonic Shift to Sustainable Investing." Accessed July 15, 2022. https://www.blackrock.com/institutions/en-us/insights/investment-actions/sustainable-investing-shift.; Kaissar, Nir. "Institutional Investors Are Flexing Their ESG Muscles." Bloomberg, 2022. https://www.bloomberg.com/opinion/articles/2022-04-13/institutional-investors-are-flexing-their-esg-muscles.

35 For more, see Famularo, Jordan. Future Directions in Corporate Disclosure on Digital Responsibility, 2023. https://cltc.berkeley.edu/publication/future-directions-in-corporate-disclosure-on-digital-responsibility/; and Famularo, Jordan. A Template for Voluntary Corporate Reporting on Data Governance, Cybersecurity, and AI, 2023. https://cltc.berkeley.edu/2023/08/07/a-template-for-voluntary-corporate-reporting-on-data-governance-cybersecurity-and-ai/.

users and consumers to improve their privacy or make more informed choices about their privacy.[36] With this new lens, interaction designers might consider, for example, what the design space might look like for creating tools or visualizations to encourage institutional investment firms to consider issues of data privacy when making investment decisions. Designing to create change at an investor level may help influence the privacy implications of technology platforms at a broader scale than designing for individual users.

IMPLICATIONS FOR PRIVACY ADVOCATES AND PRACTITIONERS

First, **understanding how privacy is translated into business risks can help provide discursive communication and framing tactics for privacy practitioners**. An understanding of how companies consider privacy laws as business risks allows practitioners to better propose and advocate for privacy reform in ways that are legible and actionable for companies. A user-centered or human-centered argument to advance privacy interests may not convince a corporate decision-maker. Prior research has shown how technology workers, such as user experience professionals, make use of rhetorical strategies to convince decision-makers to make alternate design decisions,[37] including reframing user-centered arguments in terms of a business case.[38] Given the power of such business-oriented narratives in the technology industry, we propose that privacy advocates and practitioners might explore tactically utilizing business risk language that aligns with investor disclosure discourses. For instance, when talking to a decision-maker, taking steps to address privacy might be usefully framed as "a way to avoid regulatory and reputational risks," rather than as being "good for the user."

Second, this analysis helps us **consider how data privacy may be addressed as a part of good corporate governance**. Multiple theories exist about what corporate governance models should be adopted by companies, and how decisions should be made and in whose interest.[39] In the United States, shareholder models of corporate governance have been

36 Wong, Richmond Y., and Deirdre K. Mulligan. "Bringing Design to the Privacy Table: Broadening 'Design' in 'Privacy by Design' Through the Lens of HCI." In *CHI Conference on Human Factors in Computing Systems* (*CHI 2019*), 2019. https://doi.org/10.1145/3290605.3300492.

37 Rose, Emma, and Josh Tenenberg. "Arguing about Design: A Taxonomy of Rhetorical Strategies Deployed by User Experience Practitioners." In Proceedings of the 34th ACM International Conference on the Design of Communication - SIGDOC '16, 1–10. New York, New York, USA: ACM Press, 2016. https://doi.org/10.1145/2987592.2987608.

38 Wong, Richmond Y. "Tactics of Soft Resistance in User Experience Professionals' Values Work." Proceedings of the ACM on Human-Computer Interaction 5, no. CSCW2 (2021): 28. https://doi.org/10.1145/3479499.

39 Borlea, Sorin Nicolae, and Monica-Violeta Achim. "Theories of Corporate Governance." Economics Series 23, no. 1 (2013): 117–28.; Onoja, Anthony, and Godwin O. Agada. "Voluntary Risk Disclosure in Corporate Annual Reports: An Empirical Review." *Research Journal of Finance and Accounting* 6, no. 17 (2015): 1–8.

dominant since Friedman's 1970 argument that the "social responsibilities" of businesses are to create profits for shareholders.[40] However, alternatives, such as the "stakeholder model," posit that companies have social responsibilities to a broader set of actors, such as employees, suppliers, customers, and governments.[41] As more companies recognize stakeholder models of governance, there may be opportunities to consider how different stakeholders' viewpoints of privacy might be in tension or agreement with one another, such as how users' pursuit of privacy protections that reduce ad revenue may pose business risks for investors.

Third, drawing attention to the discourses and practices of investment suggests **new ways to shape institutions' data privacy practices through disclosures and transparency reporting**. Investment practices have been seen as potential sites of action to create ethics- and values-oriented change, such as practices of activist shareholding, where investors use their stake in a company to try to shape management's decisions. Shareholder activism has been successful in shaping how companies disclose climate change risks[42] and in shifting Apple's and Microsoft's practices regarding the right to repair.[43] In addition to trying to directly affect a company's privacy practices (whether through design changes or through organizational compliance processes), privacy advocates might look to intervene by working with existing activist shareholder groups or proxy advisory firms,[44] or by working to convince large institutional shareholders to reconsider how they evaluate privacy-related risks in the companies they invest in. U.S. financial securities regulation has previously been used to promote human rights, with changes to laws enacted in 2010 that imposed requirements on companies to disclose their supply chain connections with conflict minerals.[45] Privacy advocates may consider using financial securities regulation as a lever to promote digital human rights within companies, including privacy.

Most stocks of major U.S. corporations are not owned by individual "retail" investors, but rather by large institutional investors (companies and organizations such as hedge funds or

40 Friedman, Milton. "A Friedman Doctrine - The Social Responsibility of Business Is to Increase Its Profits." New York Times Magazine, September 13, 1970. https://www.nytimes.com/1970/09/13/archives/a-friedman-doctrine-the-social-responsibility-of-business-is-to.html.

41 Freeman, R. Edward, and David L. Reed. "Stockholders and Stakeholders: A New Perspective on Corporate Governance." *California Management Review* 25, no. 3 (April 1, 1983): 88–106. https://doi.org/10.2307/41165018.

42 Flammer, Caroline, Michael W. Toffel, and Kala Viswanathan. "Shareholder Activism and Firms' Voluntary Disclosure of Climate Change Risks," 2020. http://www.elsevier.com/locate/scp.

43 Bergen, Mark. "Microsoft Will Allow More Repair Shops After Activist Protests." Bloomberg, October 7, 2021. https://www.bloomberg.com/news/articles/2021-10-07/microsoft-will-allow-more-repair-shops-after-activist-protests; Stone, Maddie. "The Shareholder Fight That Forced Apple's Hand on Repair Rights." The Verge, November 17, 2021. https://www.theverge.com/2021/11/17/22787336/apple-right-to-repair-self-service-diy-reason-microsoft.

44 E.g., https://theactivistinvestor.com/The_Activist_Investor/Proxy_Advisors.html.

45 Sarfaty, Galit. "Human Rights Meets Securities Regulation." *Virginia Journal of International Law* 54 (2013): 97–126.

endowments). As of 2019, institutional investors owned 80% of stock in the Standard and Poor's (S&P) 500 index.[46] A growing number of institutional investors have expressed interest in investing in companies that meet particular social or ethical standards, often through the concepts of "environmental, social, and governance" (ESG) or "corporate social responsibility" (CSR). While much ESG and CSR interest originates in sustainability, ESG and CSR monitoring organizations have begun to analyze companies' actions related to human rights and digital harms, including data privacy and security.[47]

Companies can communicate information about their practices and outlook with current and potential investors (and other stakeholders) through a variety of means, including disclosure documents and reports. These include annual shareholder reports, financial documents and balance sheets, human rights transparency reports, ESG reports, and regulatory filings. Some documents, like transparency reports and ESG reports, are voluntary, and the forms of information shared varies widely across companies, though there have been attempts to standardize or evaluate the types of information disclosed.[48]

IMPLICATIONS FOR POLICYMAKERS

Our research has a range of implications for policymakers. First, **securities regulation may provide a way to force companies to disclose more about their digital human rights practices, including privacy**. Currently, companies' disclosures about practices such as privacy, data governance, and cybersecurity are largely voluntary.[49] Securities and regulation or SEC guidance may provide opportunities to require or encourage companies to make more concrete disclosures about the data privacy practices in their Form 10-K disclosures. The 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act created new human rights requirements for publicly traded companies to disclose if their products use conflict materials, such as sourcing materials from the Democratic Republic of Congo.[50] The SEC has already

46 Greenspon, Jacob. "How Big a Problem Is It That a Few Shareholders Own Stock in So Many Competing Companies?" *Harvard Business Review*, 2019. https://hbr.org/2019/02/how-big-a-problem-is-it-that-a-few-shareholders-own-stock-in-so-many-competing-companies.

47 Famularo, Jordan. "Sustainability Reporting on Digital Harm: State of Play and Future Agenda." UC Berkeley Center for Long-Term Cybersecurity (blog), July 1, 2022. https://cltc.berkeley.edu/publication/sustainability-reporting-on-digital-harm-state-of-play-and-future-agenda/.

48 E.g., Ranking Digital Rights. "2020 RDR Index Methodology," 2020. https://rankingdigitalrights.org/index2020/methodology.

49 Famularo, Jordan. Future Directions in Corporate Disclosure on Digital Responsibility, 2023. https://cltc.berkeley.edu/publication/future-directions-in-corporate-disclosure-on-digital-responsibility/; and Famularo, Jordan. A Template for Voluntary Corporate Reporting on Data Governance, Cybersecurity, and AI, 2023. https://cltc.berkeley.edu/2023/08/07/a-template-for-voluntary-corporate-reporting-on-data-governance-cybersecurity-and-ai/.

50 Sarfaty, Galit A. "Human rights meets securities regulation." *Va. J. Int'l L.* 54, 2013.

provided voluntary guidance to companies to disclose their cybersecurity policies and procedures;[51] such guidance could be updated to also include policies and procedures related to data privacy.

Second, our analysis suggests that **policymakers should consider the indirect ways that law and regulation can influence corporate behavior**. One of the surprising things we found is that companies' discussion of business risks mentioned the GDPR and CCPA in ways beyond regulatory risk. The laws *indirectly* influence companies' behaviors, as well. Lawrence Lessig's discussion of code as law notes how the law can indirectly regulate behaviors — by shaping social norms, markets, and technology design, which in turn affect behaviors.[52] Companies' discussion of reputational risks related to privacy suggest that the GDPR and CCPA promote new social norms about the importance of privacy. Facebook's and Google's discussion of their advertising practices becoming less effective due to the laws, leading to lower revenue, suggest that the GDPR and CCPA affect the economic tradeoffs and make online behavioral advertising more costly (or less effective). We suggest that future lawmakers and policymakers consider the potential for these indirect effects to shape corporate behavior when crafting new data privacy regulations, particularly how these regulations might create social norms or market conditions to help shift companies' behaviors.

51 U.S. Securities and Exchange Commission. "Commission Statement and Guidance on Public Company Cybersecurity Disclosures." 17 CFG Parts 229 and 249, 2018.

52 Lessig, Lawrence. Code V.2. Chapter 7. 2006.

Conclusion

Decision-makers at large technology companies have an outsized impact on how privacy is designed and protected on major platforms and services. At for-profit entities, how privacy concerns are regarded as business risks provide a fundamental driving force for how privacy-related decisions are made.

In our analysis of major technology companies, we found five ways that companies make privacy legislation such as the GDPR and CCPA legible to investors as risks: direct regulatory risks, reputational risks, risks related to internal business practices, risks related to external stakeholders and ecosystems, and cybersecurity risks. This analysis leads us to consider a range of questions for future research:

- Do these framings of the GDPR and CCPA as business risks extend to companies in other sectors that handle consumer data (such as vehicle manufacturers, hotels and airlines, or retail companies)?
- Have the framings changed since the introduction of the California Privacy Rights Act (CPRA)?
- How might other sections in the Form 10-K provide useful information or datasets to understand technology companies' data practices?
- How do other types of digital human rights and technology ethics issues get framed and discussed as business risks in a Form 10-K, such as issues around responsible innovation or AI harms?

For privacy practitioners and advocates, this paper illustrates how such efforts can be framed or designed in a way that maps to business risks for technology companies, and hence play a larger role in shaping decision-making. This provides an important lever alongside other key approaches (such as law, activism, and designing better user experiences of privacy) to address and protect data privacy.

Acknowledgments

This report is adapted from the following research paper:

Richmond Y. Wong, Andrew Chong, and R. Cooper Aspegren. 2023. "Privacy Legislation as Business Risks: How GDPR and CCPA are Represented in Technology Companies' Investment Risk Disclosures." *Proceedings of the ACM, Human-Computer Interaction* 7, CSCW1, Article 82 (April 2023), 26 pages. https://doi.org/10.1145/3579515.

Thank you to R. Cooper Aspegren for his contributions to the research and analysis. Thank you also to Jordan Famularo, Jeeyun Sophia Baik, Sijia Xiao, Jillian Kwong, Steve Weber, Chris Hoofnagle, and participants at the 2022 Center for Long-Term Cybersecurity "Comparing Effects of and Responses to GDPR and CCPA/CPRA" symposium for feedback and comments on earlier drafts of this work. This work was supported by the UC Berkeley Center for Long-Term Cybersecurity (CLTC) and gift funding from Meta to CLTC for independent academic research. The researchers retained full discretion on the design, implementation, and expenditures for all research activities enabled by gift funding.

About the Authors

Richmond Wong is an Assistant Professor of Digital Media at Georgia Tech's School of Literature, Media, and Communication. He directs the Creating Ethics Infrastructures Lab, where his research seeks to create social, cultural, and organizational environments that can support technologists and designers in ethical decision-making. Recent projects include studying how technology workers attempt to address ethical issues within organizational contexts, and creating design activities to help people talk through issues related to privacy and surveillance. Richmond completed his PhD at the UC Berkeley School of Information, and previously worked as a postdoctoral researcher at the UC Berkeley Center for Long-Term Cybersecurity.

Andrew Chong is a PhD candidate at the UC Berkeley School of Information. Drawing on interdisciplinary approaches from the fields of human-computer interaction (HCI) and economics, his work examines the increasing role that technology-mediated marketplaces managed by platform companies play in economic life, and their wider implications for fairness, efficiency, and competition.


CLTC
Center for Long-Term
Cybersecurity
UC Berkeley