### Title
Privacy Legislation as Business Risks: How GDPR and CCPA are Represented in Technology Companies' Investment Risk Disclosures




### Journal
Proceedings of the ACM on Human-Computer Interaction, 7(CSCW1)



### Authors
Wong, Richmond Y
Chong, Andrew
Aspegren, R. Cooper



### Publication Date
2023-04-01

Peer reviewed

# Privacy Legislation as Business Risks: How GDPR and CCPA are Represented in Technology Companies' Investment Risk Disclosures



RICHMOND Y. WONG, Georgia Institute of Technology, USA
ANDREW CHONG, University of California Berkeley, USA
R. COOPER ASPEGREN, New York University, USA

Power exercised by large technology companies has led to concerns over privacy and data protection, evidenced by the passage of legislation including the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). While much privacy research has focused on how users perceive privacy and interact with companies, we focus on how privacy legislation is discussed among a different set of relationships—those between companies and investors. This paper investigates how companies translate the GDPR and CCPA into business risks in documents created for investors. We conduct a qualitative document analysis of annual regulatory filings (Form 10-K) from nine major technology companies. We outline five ways that technology companies consider GDPR and CCPA as business risks, describing both direct and indirect ways that the legislation may affect their businesses. We highlight how these findings are relevant for the broader CSCW and privacy research communities in research, design, and practice. Creating meaningful privacy changes within existing institutional structures requires some understanding of the dynamics of these companies' decision-making processes and the role of capital.

CCS Concepts: • **Social and professional topics** → **Computing / technology policy**; • **Security and privacy** → *Social aspects of security and privacy*; Economics of security and privacy.

Additional Key Words and Phrases: privacy, law, GDPR, CCPA, risk, finance, capital, investors, infrastructure

**ACM Reference Format:**
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. *Proc. ACM Hum.-Comput. Interact.* 7, CSCW1, Article 82 (April 2023), 26 pages. https://doi.org/10.1145/3579515

## 1 INTRODUCTION

Technology consumers and users increasingly cite concerns about the privacy of their personal information when interacting with technology companies—in 2019, 81% of Americans felt that they had little or no control over the data that companies collect [1]. Despite these widely shared concerns, media reports of violations of privacy by large or popular technology companies remain common [19, 21, 36].

Growing research in CSCW and related fields recognizes that privacy is not just a problem of user behavior and interface design, but also a problem of power and politics [45, 52, 63–65]. Concerns over structural power imbalances 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

Authors' addresses: Richmond Y. Wong, rwong34@gatech.edu, Georgia Institute of Technology, Digital Media, Atlanta, Georgia, USA; Andrew Chong, University of California Berkeley, School of Information, Berkeley, California, USA, qchong@berkeley.edu; R. Cooper Aspegren, New York University, School of Law, New York, New York, USA, rca9753@nyu.edu.


2573-0142/2023/4-ART82
https://doi.org/10.1145/3579515

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 technology 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 conduct a qualitative document analysis of nine major technology companies' annual reports (Form 10-K) filed with the U.S. Securities and Exchange Commission (SEC), a regulatory agency of 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. We specifically ask: 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 find that companies disclose both direct ways (such as legal fines and penalties) and indirect ways (such as brand and reputational harms) that their business may be affected by privacy and data protection legislation, outlining five framings used to make 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 the privacy and CSCW communities in research, design, and practice. This contributes to CSCW research that considers the intersections of: practices by and within technology companies [60, 65, 73], privacy law and policy [45, 47, 96], and the infrastructures that help maintain and support technology companies and platforms [34, 44, 97].

## 2 RELATED WORK AND BACKGROUND

This paper builds on prior CSCW research focusing on practices of technology production, capitalism, and policy [26, 34, 45, 47, 51, 67, 99, 104], particularly research which considers how social values are expressed and contested through these processes.

Prior research studies the practices and politics of technology companies through different "entry points" [10]. This includes studying the politics of artifacts created by companies (such as newsfeeds [11] and algorithms [54]), or of workers' practices within technology companies (such as user experience professionals [16, 106] , data workers [68, 73, 74], privacy and security professionals [53, 100], or AI ethics advocates [60, 61, 66] ). Recent projects on technology ethics and justice call for studying processes at levels beyond individual workers, moving to studying meso- and macro-levels in organizations (e.g., [93]). These projects suggest that the study of the production of technology should also engage with an understanding of companies' organizational context and strategy.

We build on research from CSCW and adjacent fields that utilizes analysis of documents to understand the practices, social values, and politics embedded in technology companies' processes. For instance, research on AI ethics has turned to analysis of corporate documents to understand how companies construct conceptions of diversity and inclusion [15, 37] or ethical AI work [110]. Hoffmann highlights how discourse has material impacts, describing forms of "discursive violence" that stem from the choices and norms of language use in corporate diversity and inclusion initiatives [37]. This paper expands on this research by analyzing how technology companies discuss risks related to privacy legislation in documents created for investors and regulators.

Below, we briefly discuss prior research studying privacy from the lens of technology production and motivate this paper's study of documents associated with practices of financial investment. We

then provide background on the type of document we analyze, Form 10-K filings, and on recent privacy legislation.

### 2.1 Understanding Privacy by Studying Technology Production

Much research in CSCW and HCI focuses on users' conceptions of privacy that occur when designing for users, needs, practices, and behaviors in different social contexts (e.g., [3, 82, 102, 103, 113]). When concepts of risk and harm are invoked in relation to privacy, they generally refer to those faced by users (or stakeholders affected by the use of technology systems).

Privacy scholars Gürses and Hoboken argue that in addition to user perspectives on privacy, understanding the configurations of technology and data flows requires an understanding of the context of production. 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," using case studies to illustrate the effects of agile development practices on data privacy [35].

CSCW researchers McDonald and Forte follow this shift, turning their attention to platforms' discourses of privacy, studying how social media companies "construct narratives about users and their privacy expectations." [65] Through a critical discourse analysis of social media companies' blogs aimed at users, the media, and general public, they describe how the platforms create narratives around identity to construct particular ideas about what privacy should be (which might be at odds with legal conceptions or users' experiences of privacy) [65].

Building on these perspectives, this paper investigates how technology companies construct narratives about business risks related to privacy and data protection legislation when communicating with current and potential investors. We focus on how privacy becomes conceptualized and made legible as a part of "risk" to companies, rather than as a risk faced by users or consumers.

### 2.2 Financial Investment and Corporate Disclosures

We extend CSCW's lenses for studying platform infrastructures to include practices related to financial investment in those platforms. Infrastructures include the technologies, social institutions, policies, and practices that produce, maintain, and support sociotechnical systems [9, 44, 94]. Prior CSCW research on infrastructural practices spans consideration of managerial and organizational practices [27, 97], breakdown and repair work [40, 46, 79], and policy and governance [56, 108]. However, practices related to finance have had less direct study as an infrastructural practice in CSCW (although they have been in adjacent fields, e.g., [59]).

More broadly, scholars analyzing the politics of technologies and technology companies have called for greater engagement with questions of political economy [20], investigating for whose benefit technologies are developed, who does the labor, and the role of capital in technology development [26, 42, 43, 51, 88, 95]. Additionally, scholars have called for research studying how platforms are shaped by people, places, and institutions [13]. This paper investigates investment practices as a part of technology platforms' infrastructures, by analyzing the discourses utilized by technology companies in their disclosures to investors.

*2.2.1 Investment as a Site of Debate over Technology Values.* Investment practices have been seen as potential sites of action to create ethics and values-oriented change, such as practices of activist shareholding, where company 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 [25] and in shifting Apple's and Microsoft's practices regarding the right to repair [6, 98]. 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

endowments). As of 2019, institutional investors owned 80% of stock in the Standard and Poor's (S&P) 500 index [33]. 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 and social good (ESG)" or "corporate social responsibility" (CSR) [49, 83]. 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 [41, 77].

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. Other documents like regulatory filings are required by U.S. law and are subject to more strict and structured reporting requirements. We look more closely at a particular type of regulatory filing, the Form 10-K.

*2.2.2 Companies' Form 10-K Filings with The U.S. Securities and Exchange Commission.* We investigate companies' Form 10-K, annual reports that are filed with the U.S. Securities and Exchange Commission (SEC) which is 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.[1] While there is debate about the efficacy of this framework, disclosure is presumed "to promote market efficiency and ensure a well-informed investing population." [76]

Companies' Form 10-Ks are filled annually and are publicly accessible via the SEC's database. A Form 10-K must include 15 items that disclose information including the company's business practices, financial data, and potential business risks among other items. 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 for compliance. The main audiences that read these documents include investors or potential investors, financial analysts, and finance media reporters.

We look specifically at the sections of the Form 10-K that discuss potential risks that companies face: Item 1A, Risk Factors. These sections generally qualitatively describe the nature of the risk, but do 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 [5]. 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." [58] Prior research has investigated categories of risk disclosure, including: risks related to the production and demand of products, financial risks, operational risks (related to internal processes and people, or external events), and legal and regulatory compliance risks [72].

The main purpose of Form 10-Ks is the disclosure of truthful information, rather than providing opinionated statements and perspectives as might be found in advertisements or press releases. In

[1]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 [12]. We note that this type of disclosure framework has limitations, such as critiques made by privacy scholars arguing that disclosures may place too great of a burden on consumers and may not do a good job informing users, e.g., [62, 92].

Form 10-Ks, companies must provide truthful information about things that have previously or are currently happening, but have some protection from legal liability when making forward-looking statements (including statements about future risks) due to uncertainty about the future. Some voice concerns that companies may disclose generic and extensive boilerplate text by listing all possible uncertainties, or even outright present misleading forward-looking risk statements [4, 23, 71]. Others' research suggest that disclosure of risks, even if uncertain, nevertheless improve market efficiency [18]. 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.

However, 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 have 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 [86]. The SEC has also taken measures to try to improve the quality of information in Risk Factors sections, for example by adopting amendments to make companies disclose "material" risks and provide summaries of risks when they go beyond a certain length [87]. Investors may also bring lawsuits against a company for providing false or misleading statements.

While the Federal Trade Commission (FTC) has been the main U.S. regulator to consider issues related to digital privacy [38], in 2011 the SEC began to publish voluntary guidelines for companies to specifically discuss cybersecurity risks and incidents. The SEC provided guidance suggesting that companies had a duty to disclose information related to cybersecurity risks to potential investors [84]. This guidance was updated in 2018, in part to emphasize the importance of companies having cybersecurity policies and procedures [85]. 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) [2, 23], 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, as well as after companies experience a cybersecurity incident [55].

While prior research has analyzed cybersecurity discourses in SEC disclosures [2, 23, 30, 55], comparatively little has focused on privacy. One exception is Fathaigh et al.'s analysis of Form 10-Ks filed by mobile app companies between 2008-2017 to understand their data collection and use practices, finding that these companies disclosed their compliance with privacy laws as part of their risk factors [22]. They argue 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)." [22, pg.53-54]. They argue that SEC filings can provide evidence of the impact of the law on a companies' business model 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.

### 2.3 Background on GDPR and CCPA

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 in the EU. However, the regulation faced challenges catering to the needs of the entire 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 [39].

The CCPA resulted from a grassroots 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 is expected to go into effect in 2023 [17].[2]

The GDPR and CCPA provide similar protections to consumers while having several key differences [32, 48]. The regulations involve 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 who 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 cure period to correct their mistakes to avoid being fined. The GDPR also allows for individuals to claim damages from companies after certain types of data breaches. The GDPR offers a broader array of rights to consumers than the CCPA, including the right to rectification, right to object to processing, and 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 personal data of EU residents. CCPA is rooted in a consumer protection framework, and more narrowly applies to businesses that meet certain thresholds related to revenue or 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.

## 3 METHODS

### 3.1 Corpus Selection and Description

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 of particular relevance to CSCW research, including those that produce platforms for online collaboration, work, communication, and social activity. We aimed to purposively curate a sample of companies that would capture breadth and diversity, rather than a complete accounting or a statistically representative sample of all technology companies.

We considered factors such 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 high media visibility or regulatory scrutiny. After several discussions among the authors, we selected nine companies, described in Table 1.[3] [4]

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 GDPR's passage) until 2020 using the SEC's public database. Because only publicly traded companies are required to file a Form 10-K, several companies with more recent initial public offerings (Uber, DoorDash, Airbnb) had fewer years' worth of filings. We considered analyzing companies' quarterly filings (Form 10-Qs) but found that there was not enough change in the

[2]As the most of the documents we analyze were published before the California Privacy Rights Act ballot initiative passed, few companies in our corpus discussed CPRA.

[3]Note that "Main Revenue-Generating Product(s) or Service(s) is an analytical category by the authors to categorize the companies, based on either companies' description of their business or revenue in their Form 10-Ks, or based on public knowledge about the companies. We aim for diversity here, as different types of products and services may require different types of uses of personal data.

[4]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 file their documents.

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 |
|---|---|---|---|
| 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 |

documents each quarter to warrant four times the analysis; the major changes in the quarterly documents were also reflected in the annual Form 10-Ks.

In total, our corpus contains 40 Form 10-Ks from nine companies between 2015 and 2020. We formally coded the Risk Factors sections, and skimmed other sections of the documents (such as the Item 1 Business description) to contextualize our understandings of the risks. The Risk Factors sections from these combined Form 10-Ks represent 672 total pages.

### 3.2 Data Analysis

We conducted a thematic analysis through several rounds of interpretive qualitative analysis and coding. In a first round of analysis, the first two authors skimmed through several companies' Form 10-Ks to understand the documents' organization and content. Both authors took and shared notes about potential emergent themes, including the language companies use to describe risks, the potential impact or harm, and what types of stakeholders are discussed.

Figure 1 shows a screenshot of an excerpt from Item 1A "Risk Factors" from a Form 10-K. The risk factors contain one or more sentences of bolded text that describe the risk (which we call the risk factor statement), followed by one or more paragraphs describing the risk in more detail (the risk factor description). We refer to the combined bolded risk factor statement and paragraph(s) of risk factor description as a risk factor block.

In a second round of analysis, all authors used qualitative coding software to code the Form 10-Ks. We first considered whether a block was relevant for our analysis or not. Blocks were considered relevant if they mentioned: a privacy or data protection law, including "GDPR," "CCPA"; the words "privacy" or "data protection"; or other terms related to privacy, such as "personal data/information," "personally identifiable information," or "sensitive data/information." We then openly coded relevant blocks for the following:

- *What is the risk factor(s) stated in the block?* For instance, risks posed by reputational damage, by government investigations, by data breaches, by evolving regulation, etc.
- *What stakeholders are mentioned in the block?* For example, customers, users, regulators, employees, contractors, third party developers, etc.

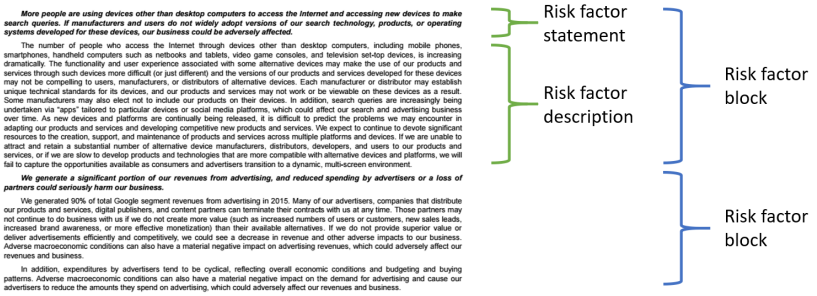


Fig. 1. A screenshot of a page of Risk Factors from the Google (Alphabet) Form 10-K in 2015, highlighting the sections we call "risk factor statement," "risk factor description," and "risk factor block."

- *What circumstances surrounding the risk are mentioned in the block?* 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 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 started by coding the earliest Form 10-K we had for each company. Two authors coded each Form 10-K independently. Disagreements were resolved during meetings among all authors. We then coded subsequent years to see what changed over time. Analyzing filings by year draws on Fathaigh et al.'s method analyzing mobile app companies' Form 10-Ks [22]. While Fathaigh worked backwards from 2017, we worked forward from 2015 to see how the filings changed as GDPR and CCPA came into effect. Companies often edited their risk factors each year. Sometimes new risk factor blocks would be added (or deleted), or edits caused a risk factor block to become relevant to our analysis. Relevant blocks that were new or had significant edits were re-coded according to the schema. Using these criteria, we analyzed and coded 365 risk factor blocks in total.

In a third round of analysis, all three authors conducted a close reading of the relevant risk factor blocks, writing and sharing textual memos about emerging themes based on the codes in those blocks. Through this thematic analysis process, we identified a set of patterns and themes that responded to our research questions.

## 4 FINDINGS: HOW COMPANIES FRAME DISCUSSION OF RISKS RELATED TO GDPR AND CCPA

While we initially expected privacy legislation to only be reflected as a regulatory risk, we find a broader set of risk framings where privacy and data protection legislation are discussed. We detail five areas where companies' risk disclosures discuss privacy and data protection legislation: (1) regulatory risks, (2) brand and 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 throughout Section 4.

We also note that all the companies in our corpus discussed risks related to privacy before the enactment of GDPR and CCPA, suggesting that they were attuned to privacy concerns before these pieces of legislation were passed. All the companies in our corpus except for Apple and Amazon explicitly mention the GDPR and CCPA by the time those laws went into effect (DoorDash, which

only operated in the US in 2020, only mentions the CCPA as it was not under the jurisdiction of GDPR), as shown in Figure 2.

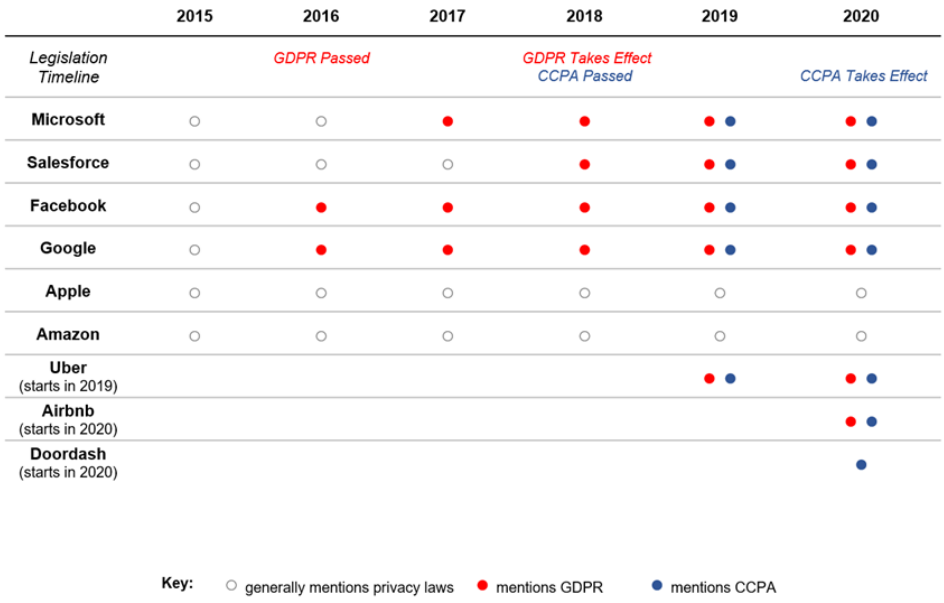


Fig. 2. An overview of whether a 10-K for a given company and year mentions the GDPR or CCPA.

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 GDPR and CCPA presenting financial and legal risks. |
| Brand and Reputational Risks | How do the laws indirectly affect our brand and reputation? | Being found in violation of a privacy or data protection law brings new reputational 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 risks. |
| 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. |

### 4.1 Direct Regulatory Risks

Companies frequently framed privacy regulation as direct regulatory risks, highlighting the immediate legal penalties and fines that companies face if found in violation of the law. We find that even before the enactment of GDPR, companies made references to 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 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 GDPR and CCPA, most companies updated their existing risk factor statements related to regulatory risks to include explicit mention of 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 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, with Facebook and Salesforce additionally dedicating 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 after a data breach. Unlike 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 [50]. Hence, companies saw different regulatory mechanisms —monetary fines by a regulatory agency in GDPR versus private lawsuits from individuals in CCPA— as posing different financial risks for companies and to investors, choosing to outline them explicitly in their risk disclosures.

### 4.2 Brand and Reputational Risks

Companies were also sensitive to how privacy and data protection regulations could increase brand and reputation risks. In contrast to individual user complaints about violations of privacy, privacy legislation allows for a more collective shared conception of privacy 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 led to shared conceptions of privacy violations before the enactment of 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 GDPR and CCPA were among the laws they were concerned about. In this example, GDPR and CCPA fit easily into the ways Facebook was already thinking about the relations between privacy regulation, shared conceptions of privacy violations, and reputational harm.

Other companies, however, added new discussions about reputational and brand risk after GDPR came into effect. Microsoft, Google, Facebook and Salesforce all added new language discussing how violating 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 companies also mentioned the CCPA alongside GDPR. These framings of brand and reputational risk under GDPR and CCPA stem 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. This suggests that privacy legislation may help make it easier to amass public pressure or reputational damage against companies with privacy-insensitive practices.

Interestingly, companies were also sensitive to how perceived violations of privacy could also increase business risks, often using language such as "actual or perceived" with regards to security and privacy breaches. DoorDash noted how privacy and security incidents even among competitors could affect their brand and reputation, and 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 posing reputational risks in multiple ways, including more direct risks if a company is found in violation of a law, and more indirect risks if they help shift public perceptions about a company or the technology industry more broadly.

### 4.3 Risks Related to Internal Business Practices

Companies also described how privacy regulation increased risks around their internal business practices, such as by requiring new data transfer procedures, 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 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 the risk for the many companies that transfer personal data between countries.

Companies also described how privacy legislation had a direct effect on 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 had a direct impact on revenue.** Facebook, which also reported in their 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 their long-term growth strategy in part involved practices to "invest in growing the size and quality of our host community" and "grow and engage our guest community" (Airbnb 2020); DoorDash described their goals to increase their consumer reach, which included paid marketing campaigns. Airbnb went on to describe how GDPR can make it more difficult for it to market itself to potential new platform users:

> "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 costs of educating customers** on new laws and regulations. For example, Salesforce noted risk of increased costs of "education regarding privacy and data protection laws and regulations" (Salesforce 2015) during the sales process.

More broadly, companies also described how **privacy legislation and privacy concerns may create new risks to consider in the development of new data-intensive products**. In 2015 Google and Microsoft noted how their shifts to increased 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 framing helps provide insight into specific business practices that have been affected by privacy legislation, which varies based on companies' products and business models.

### 4.4 Risks Related 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 marketing cookies could be negatively affected if users decided not to opt-in. 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 how these changes had negatively impacted their ability to target and measure advertisements and "negatively impacted our advertising revenue" (Facebook 2020). In this framing, users exercising their data protection rights under GDPR were framed as a business risk to Facebook, in the form of reduced advertising revenue.

Other companies face **risks and challenges stemming from their enterprise clients**. Salesforce described new risks from enterprise clients (described as its 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 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 their 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 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—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, also described **privacy tradeoffs among different groups of users**. 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, DoorDash expressed awareness that more thorough checks may generate pushback from drivers, who may find them overly invasive of their privacy. Furthermore, they described how third parties conducting background checks may themselves be subject to privacy or data security breaches.

Airbnb and DoorDash's discussions of privacy concerns as they relate to the different groups that their platforms serve reflect the complex way privacy concerns affect companies. The actions to protect the safety and privacy of one group (such as customers and riders) may potentially increase the risks of privacy violations for another group (such as the drivers and hosts subject to background checks). Their discussion underlines tensions in the custodial role they perform 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.

### 4.5 Cybersecurity Risks

Finally, companies related GDPR and CCPA to existing business risk factors discussing cybersecurity, which tended to predate and be better represented in 10-K filings due to earlier SEC guidelines recommending that companies include risk disclosures about cybersecurity. While 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 monetary damages.[5]

The enactment of these laws is reflected in how companies framed business risks related to security, primarily by describing the new consequences of a security breach. Uber (2019) noted how both the GDPR and CCPA require them to meet "stringent requirements" and other procedures and practices with regards to preventing and reporting on data breaches, increasing costs.

Other companies use their Form 10-K's to disclose security breaches they had actually experienced, following the guidelines set forth by the SEC about cybersecurity disclosures [84, 85]. For example in 2018, Facebook disclosed how 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 cyber-attack 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.

## 5 DISCUSSION

We now turn to key reflections based on our analysis. We discuss takeaways and implications for research in CSCW, as well as for privacy advocacy, design, and practice.

### 5.1 What Can We Learn About Privacy from SEC Filings?

We reflect on several insights enabled by analyzing technology companies' Form 10-Ks. Notably, the types of risks discussed in these documents focus 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 made legible as business risks reveal the complex accounting that takes place

[5]It is worth noting that historically, regulatory privacy and data protection principles often included statements related to security. The Fair Information Practices (FIPs), which originated as a set of principles in the 1970s in the U.S. to protect the privacy of personal data in government computer systems, included a statement about assuring "the reliability of the data for their intended use"; future restatements of the FIPs such as the OECD's 1980s guidelines explicitly included a security safeguards principle [31]. Current day laws and regulations, including the GDPR and CCPA, have a lineage from the FIPs, and promote many of the same principles.

within companies, and helps illustrate the complex, dynamic assemblage surrounding technology companies and law and the multifaceted relationships between them.

*5.1.1 Privacy and Data Protection Laws Pose More Than Regulatory Risks.* We find that privacy legislation and regulation affect technology companies in multi-faceted ways. Prior research has studied how companies have complied with the GDPR and CCPA [80, 105]. 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 in these documents. Law also indirectly affects companies, for instance when companies discuss GDPR and CCPA as reputational risks. By setting a public legal standard of privacy against which to be measured, there are new opportunities for negative media coverage and for public opinion to shift on companies' privacy and data protection behaviors. This may create incentives other than legal fines and penalties 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." Other companies describe how GDPR and CCPA create risks specific to their own operations and business models—for instance Salesforce notes how it creates additional obligations to educate their enterprise clients; DoorDash and Airbnb note how privacy legislation may make it difficult for them to rely on targeted advertising to grow their user base.

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 of changing their business practices or decreased revenue, 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.

*5.1.2 Providing Insight into Company Practices Related to Privacy.* While Risk Factors contain forward-looking statements that describe things that may or could happen, the Risk Factors 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." [22]

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

The risk factor disclosures also help provide contextual information that can help researchers better understand why companies are sensitive to different concepts of privacy or why they instill or prioritize some protections over others. For instance, Google and Facebook note in their 10-Ks how 80% of their 2020 revenue and 97% of their fourth quarter 2020 revenue, respectively, comes from advertising. This helps contextualize the magnitude of business risks they face when privacy tools like ad blockers and privacy legislation make their tracking and advertising practices more difficult. Furthermore, Facebook reports facing negative impacts to their advertising revenue after the passage of GDPR, which suggests that the GDPR's efforts have been successful in the advertising domain. It also suggests that legislation that prioritizes online behavioral tracking as the dominant privacy problem will have a greater effect on these particular companies.

Gig economy companies like Airbnb, DoorDash, and Uber provide contextual information that suggests that 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, in order to try to assure guests or customers of their physical safety. In these instances, the promotion of privacy or safety with 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 are affecting companies' practices.

*5.1.3 Highlighting the Interconnectedness of Technology Companies and Platforms.* Our analysis highlights dependencies between technology companies and how their business models may come into conflict. Airbnb, DoorDash, Facebook, Uber note 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 that allow users to opt out of targeted advertising from apps are noted by these companies as a business risk, since those changes make it harder to track or advertise to users. Further contextualizing these efforts, Airbnb and DoorDash both note that their growth strategy includes 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.

*5.1.4 Shaping a More-Than-User-Centered Privacy Discourse.* The analysis of Form 10-Ks focuses on discussing privacy as a type of business risk, rather than a positive good to provide to users (which is how privacy tends to be discussed in user-facing documents such as privacy policies). While a lot of privacy research focuses on the relationships between platforms and users, this paper's analysis opens up practices related to corporate governance as part of privacy infrastructures. Additional stakeholders beyond users are involved in these conversations. This more-than-user-centered discourse is primarily aimed at investors and regulators, but privacy researchers and advocates may benefit from participating in these discourses as well.

Multiple theories and debate exist about what corporate governance models—how decisions should be made and in whose interest—should be adopted by companies [8, 72]. In the United States, shareholder models of corporate governance have been dominant since Friedman's 1970 argument that the "social responsibilities" of businesses are to create profits for shareholders [29]. 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 [28]. 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.

Considering practices of financial investment as part of the infrastructure of technology platforms helps provide new perspectives on the power and politics of platforms. This opens up ways

for research on privacy and values in design to operate at levels beyond the user interface. Understanding practices of production invites new ways to consider the politics of technology [35, 45]. This analysis helps give insight into why companies make certain privacy-enhancing changes in their products and business practices (for instance to avoid direct regulatory or reputational risks), but also why they may be reluctant to do so (for instance due to the some of the risks related to internal business practices). These relationships give rise to multiple mechanisms that can be used to change company behavior and practices. As we push for a better understanding of the "mutually constitutive relations between design, practice and policy" [45], understanding how privacy legislation is presented by technology companies to their investors is vital towards achieving effective forms of change.

### 5.2 Implications

We consider implications for multiple audiences in the CSCW and privacy communities.

*5.2.1 Implications for Researchers.* First, we suggest **that efforts to change privacy design outcomes must engage in thinking about privacy through a broader set of lenses.** 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. This builds on existing CSCW research at the intersection of policy and design (e.g., [14, 45]).

Second, **studying discourses and practices related to financial investment in technology companies provides new insights into infrastructures and the politics of production**. CSCW has highlighted and debated the effects of corporate investment in HCI research [34]; similar lenses can be used to investigate the influence of investors in technology companies' decisions. For instance, major large institutional investors have made recent statements that they will make investment decisions in part based on companies' environmental sustainability practices, potentially shifting corporate sustainability practices [7, 49]. 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? Building on CSCW's interest in infrastructures [97, 101], what are the roles and politics of *financial* infrastructures in the creation and support of technology platforms?

*5.2.2 Implications for Designers.* Most prior research on design and privacy focuses on designing to help empower users to improve their privacy or make more informed choices about their privacy [111], although recent CSCW and related research acknowledge how privacy is often a problem of social power [52, 63, 65]. This paper first suggests **designing for a new audience with outsized social and financial power: investors and other stakeholders involved in financial investment processes**. For example, what might the design space look like for creating tools (or visualizations or other artifacts) 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 values and ethical implications of technology platforms at a broader scale than designing for individual users.

Second, **an understanding of business risks can help improve "ethics in design" tools and activities**. Prior CSCW research has studied and created tools that are aimed at practitioners and support consideration of values and ethics, including privacy [69, 89, 90, 107]. Many of these tools embed an assumption that once an ethical issue is surfaced during the design process, resources will be allocated to address it. However, research findings show that technology workers who wish to advance and address ethical issues from within their companies often face barriers from

organizational decision-makers that make it difficult to get the resources and time to address these issues [16, 61, 106]. There is a design opportunity to create more effective ethics in design tools that connect user-facing harms to framings of business risk that may be more familiar and legible to organizational decision-makers.

Third, **corporate risk factors might serve as productive inspiration material for design futuring around privacy and other ethical issues.** Prior design research in CSCW and HCI has created fictional and speculative products [112], platform APIs [91], and other artifacts [24, 75] to explore how privacy and ethical issues might arise among various situations and populations. With calls for speculative design research to engage more with issues of infrastructures and institutional politics [109], Form 10-Ks and their forward-looking risks could serve as inspiration for future speculative design work that explores the implications of different business practice choices and how they could affect different user and stakeholder populations.

*5.2.3 Implications for Privacy Advocates and Practitioners .* First, drawing attention to the discourses and practices of investment opens up **new sites and levers for shaping and changing institutions**. Investment practices have been seen as potential sites of action to create ethics and values-oriented change, such as practices of activist shareholding, where a company investor(s) uses 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 [25] and in shifting Apple's and Microsoft's practices regarding the right to repair [6, 98]. 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,[6] 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 in 2010 that imposed requirements on companies to disclose supply chain connections with conflict minerals [81]. Privacy advocates may consider using financial securities regulation as a lever to promote digital human rights within companies, including privacy.

Second, **understanding how privacy is translated into business risks can help provide tactical discursive moves for privacy practitioners within companies**. 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 [78], including reframing user-centered arguments in terms of a business case [106]. 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 framed as "a way to avoid regulatory and reputational risks," rather than as being "good for the user."

We acknowledge that this set of interventions still largely works within existing institutions and systems of capital. We envision these as complementing a broad range of intervention practices and theories of change that researchers, workers, regulators, advocates, and other stakeholders might engage in, including those that are more directly adversarial to current configurations and institutions of capital. However, we also hope that tactical interventions in investment practices

[6] e.g., https://theactivistinvestor.com/The_Activist_Investor/Proxy_Advisors.html

still hold the possibility to create new openings and gaps for critical action, while acknowledging the ongoing presence and power of neoliberal capitalism [57].

### 5.3 Limitations and Future Directions

This paper's analysis has several limitations. First, the qualitative thematic analysis is shaped by the positionality and experiences of the authors, who are based in U.S. academic institutions. While the authors have expertise in studying privacy, economics, platforms, business strategy, and issues related to technology law and policy, we are reading and analyzing these documents from a perspective outside of the companies where the documents are authored.

Second, the 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, GDPR, and CCPA, it is possible the inclusion of additional technology companies or looking at filings before 2015 would provide new conceptions of risk that we did not find.

Table 3. Documents Describing Aspects of Companies' Privacy Practices

| Document Type | Main Audience(s) | Potential Insights for Researchers |
|---|---|---|
| Form 10-K | Investors, financial regulators, media | - Identify factors that create risks for a business' operations<br>- Identify specific impacts a law has had on a company's business models and practices<br>- Provide insight into financial motivations for product design decisions |
| Privacy/data protection impact assessments | Internal company stakeholders, privacy regulators | - Identify factors that create risks leading to a breach of privacy or security<br>- Identify measures taken to mitigate those risks |
| Privacy Policies | Users, privacy regulators | - Understand how a company collects and processes data<br>- Identify what options users have to manage their data |
| Blog posts | Users, media, other societal groups | - Identify different conceptions of privacy utilized by companies (e.g., why is privacy important, whose privacy matters)<br>- Understand companies' opinions |
| Human rights and transparency reports | Human rights advocates, ESG investors | - Understand companies' self-reported practices on upholding and promoting human rights (including digital privacy) |

Third, while analyzing companies' Form 10-Ks helps us understand how technology companies talk to investors, these documents alone do not fully explain the reasoning or motivation for companies to frame risks in these ways. SEC filings require certain types of disclosures by law and are signed under oath, we thus trust the validity of information presented in the Form 10-Ks. However it is still possible for companies to provide boilerplate statements [2]. In this sense, we see this paper's analysis of Form 10-K risk factors as one entry point among many studying the politics of technology companies and their privacy-related practices. Table 3 describes other documents produced by companies that can provide additional viewpoints in future work, including

privacy/data protection impact assessments [70], privacy policies, companies' blog posts [65], and human rights and transparency reports [77].

Future work can expand on this paper's analysis in several directions. Quantitative analysis techniques could be used to study a broader sample of Form 10-Ks over a longer time period to see if additional patterns in the discussion of privacy, GDPR, or CCPA emerge. Future qualitative or quantitative analysis may look at the same corpus to analyze the discussion of issues and themes beyond privacy. This may be particularly useful to study other themes that have a policy or regulatory component, such as copyright, free speech and content moderation, AI ethics, or how labor laws may affect the role of gig workers on platforms.

While analyzing Form 10-Ks provides insight into how companies publicly represent and frame their practices and risks to public (financial) audiences, a limitation of this approach is that it does not give as much insight into organizations' internal decision-making processes. While recognizing that it can be difficult to get access to study corporate practices, future work may seek to further study internal decision-making related to privacy and other risks, asking questions such as: what forms of internal decision-making and stakeholder involvement can best help companies make progress on protecting user privacy? Why do some privacy design interventions seem more or less favorable to a company given its business model?

## 6 CONCLUSION

This paper analyzed nine major technology companies' annual reports (Form 10-K) filed with the US Securities and Exchange Commission, to investigate how these companies represent issues related to privacy legislation to potential financial investors, regulators, and other external stakeholders as forms of business risks. We outline five ways that companies make privacy legislation such as GDPR and CCPA legible to investors as risks: direct regulatory risks, reputational and brand risks, risks related to internal business practices, risks related to external stakeholders and ecosystems, and cybersecurity risks.

More broadly, the paper argues that studying the discourses, practices, and artifacts related to financial investment in technology companies can provide new insights into their politics. Such an approach can also provide insight into how new technology-related laws are interpreted by companies. The paper also suggests that investment practices may serve as new sites of action for the CSCW community to shape and change companies and institutions towards more ethics-conscious ends. Considering corporate governance and financial investment practices as sites of ethical contestation can help address issues like privacy at scale by acknowledging the role of capital in corporate decision-making. As researchers, practitioners, regulators, and advocates push for more responsible decision-making at technology companies, understanding companies' representations to investors can help provide important indicators, strategies, and tactics for how to advocate for more effective privacy design and policy within these companies.

## ACKNOWLEDGMENTS

Thank you to Jordan Famularo, Jeeyun Sophia Baik, Sijia Xiao, Jillian Kwong, Steve Weber, Chris Hoofnagle, the reviewers, other colleagues, and participants at the 2022 Center for Long-Term Cybersecurity "Comparing Effects of and Responses to GDPR and CCPA/CPRA" symposium for valuable 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.

## REFERENCES


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

[2] Norah C. Avellan. 2014. The Securities and Exchange Commission and the Growing Need for Cybersecurity in Modern Corporate America. *Washburn Law Journal* 54, 1 (2014), 193–226.

[3] Karla Badillo-Urquiola, Yaxing Yao, Oshrat Ayalon, Bart Knijnenurg, Xinru Page, Eran Toch, Yang Wang, and Pamela J. Wisniewski. 2018. Privacy in Context: Critically Engaging with Theory to Guide Privacy Research and Design. In *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing* (Jersey City, NJ, USA) *(CSCW '18)*. Association for Computing Machinery, New York, NY, USA, 425–431. https://doi.org/10.1145/3272973.3273012

[4] Yang Bao and Anindya Datta. 2014. Simultaneously Discovering and Quantifying Risk Types from Textual Risk Disclosures. *Management Science* 60, 6 (6 2014), 1371–1391. https://doi.org/10.1287/mnsc.2014.1930

[5] Ulrich Beck. 2006. Living in the world risk society. *Economy and Society* 35, 3 (2006), 329–345. https://doi.org/10.1080/03085140600844902

[6] Mark Bergen. 2021. Microsoft Will Allow More Repair Shops After Activist Protests. https://www.bloomberg.com/news/articles/2021-10-07/microsoft-will-allow-more-repair-shops-after-activist-protests

[7] BlackRock. 2021. The tectonic shift to sustainable investing. https://www.blackrock.com/institutions/en-us/insights/investment-actions/sustainable-investing-shift [Online; accessed 2022-07-15].

[8] Sorin Nicolae Borlea and Monica-Violeta Achim. 2013. Theories of corporate governance. *Economics Series* 23, 1 (2013), 117–128.

[9] Geoffrey C. Bowker, Karen Baker, Florence Millerand, and David Ribes. 2010. Toward Information Infrastructure Studies: Ways of Knowing in a Networked Environment. In *International Handbook of Internet Research*. Springer Netherlands, Dordrecht, 97–117. https://doi.org/10.1007/978-1-4020-9789-8_5

[10] Jenna Burrell. 2009. The Field Site as a Network: A Strategy for Locating Ethnographic Research. *Field Methods* 21, 2 (18 Feb. 2009), 181–199. https://doi.org/10.1177/1525822X08329699

[11] Jenna Burrell, Zoe Kahn, Anne Jonas, and Daniel Griffin. 2019. When Users Control the Algorithms: Values Expressed in Practices on Twitter. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (7 11 2019), 1–20. https://doi.org/10.1145/3359240

[12] M. Ryan Calo. 2012. Against Notice Skepticism in Privacy (and Elsewhere). *Notre Dame Law Review* 87, 3 (2012), 1027–1072.

[13] Robyn Caplan, Meredith Clark, and William Partin. 2020. Against Platform Determinism: A Critical Orientation. https://points.datasociety.net/against-platform-determinism-899acdf88a3d

[14] Alissa Centivany. 2016. Policy as Embedded Generativity: A Case Study of the Emergence and Evolution of HathiTrust. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing - CSCW '16*. ACM Press, New York, New York, USA, 924–938. https://doi.org/10.1145/2818048.2820069

[15] Nicole Chi, Emma Lurie, and Deirdre K. Mulligan. 2021. Reconfiguring Diversity and Inclusion for AI Ethics. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (Virtual Event, USA) *(AIES '21)*. Association for Computing Machinery, New York, NY, USA, 447–457. https://doi.org/10.1145/3461702.3462622

[16] Shruthi Sai Chivukula, Chris Rhys Watkins, Rhea Manocha, Jingle Chen, and Colin M. Gray. 2020. Dimensions of UX Practice That Shape Ethical Awareness. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376459

[17] Privacy Rights Clearinghouse. 2020. California Consumer Privacy Act Basics.

[18] J Richard Dietrich, Steven J. Kachelmeier, Don N. Kleinmuntz, and Thomas J. Linsmeier. 2001. Market Efficiency, Bounded Rationality, and Supplemental Business Reporting Disclosures. *Journal of Accounting Research* 39, 2 (9 2001), 243–268. https://doi.org/10.1111/1475-679X.00011

[19] Zak Doffman. 2021. Why You Shouldn't Use Google Chrome After New Privacy Disclosure. *Forbes* (20 March 2021). https://www.forbes.com/sites/zakdoffman/2021/03/20/stop-using-google-chrome-on-apple-iphone-12-pro-max-ipad-and-macbook-pro/

[20] Hamid Ekbia and Bonnie Nardi. 2016. Social Inequality and HCI: The View from Political Economy. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 4997–5002. https://doi.org/10.1145/2858036.2858343

[21] Peter Elkind, Jack Gillum, and Craig Silverman. 2021. How Facebook Undermines Privacy Protections for Its 2 Billion WhatsApp Users. *ProPublica* (7 Sept. 2021). https://www.propublica.org/article/how-facebook-undermines-privacy-protections-for-its-2-billion-whatsapp-users

[22] Ronan O Fathaigh, Joris van Hoboken, and Nico van Eijk. 2018. Mobile Privacy and Business-to-Platform Dependencies: An Analysis of SEC Disclosures. *Journal of Business and Technology Law* 14, 1 (2018), 49–105.

[23] Matthew F. Ferraro. 2014. "Groundbreaking" or Broken? An Analysis of SEC Cybersecurity Disclosure Guidance, its Effectiveness, and Implications. *Albany Law Review* 77 (2014), 51 pages.

[24] Casey Fiesler. 2019. Ethical Considerations for Research Involving (Speculative) Public Data. *Proceedings of the ACM on Human-Computer Interaction* 3, GROUP (5 12 2019), 1–13. https://doi.org/10.1145/3370271

[25] Caroline Flammer, Michael W. Toffel, and Kala Viswanathan. 2021. *Shareholder activism and firms' voluntary disclosure of climate change risks.* Technical Report 10. 1850–1879 pages. https://doi.org/10.1002/smj.3313 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/smj.3313

[26] Sarah E. Fox, Vera Khovanskaya, Clara Crivellaro, Niloufar Salehi, Lynn Dombrowski, Chinmay Kulkarni, Lilly Irani, and Jodi Forlizzi. 2020. Worker-Centered Design: Expanding HCI Methods for Supporting Labor. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '20)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/3334480.3375157

[27] Sarah E. Fox, Kiley Sobel, and Daniela K. Rosner. 2019. Managerial Visions: Stories of Upgrading and Maintaining the Public Restroom with IoT. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3290605.3300723

[28] R. Edward Freeman and David L. Reed. 1983. Stockholders and Stakeholders: A New Perspective on Corporate Governance. *California Management Review* 25, 3 (1 4 1983), 88–106. https://doi.org/10.2307/41165018

[29] Milton Friedman. 1970. A Friedman doctrine - The Social Responsibility of Business Is to Increase Its Profits. *New York Times Magazine* (13 Sept. 1970).

[30] Lei Gao, Thomas G. Calderon, and Fengchun Tang. 2020. Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems* 38 (2020), 100468. https://doi.org/10.1016/j.accinf.2020.100468

[31] Robert Gellman. 2022. *Fair Information Practices: A Basic History (vr. 2.22).* Technical Report. https://doi.org/10.2139/ssrn.2415020

[32] Eric Goldman. 2020. *Introduction to the California Consumer Privacy Act (CCPA).* Technical Report. Santa Clara University Legal Studies Research Paper. https://doi.org/10.2139/ssrn.3211013

[33] Jacob Greenspon. 2019. Big a Problem Is It That a Few Shareholders Own Stock in So Many Competing Companies. https://hbr.org/2019/02/how-big-a-problem-is-it-that-a-few-shareholders-own-stock-in-so-many-competing-companies [Online; accessed 2022-07-09].

[34] Critical Platform Studies Group, Lilly Irani, Niloufar Salehi, Joyojeet Pal, Andrés Monroy-Hernández, Elizabeth Churchill, and Sneha Narayan. 2019. Patron or Poison? Industry Funding of HCI Research. In *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing* (Austin, TX, USA) *(CSCW '19)*. Association for Computing Machinery, New York, NY, USA, 111–115. https://doi.org/10.1145/3311957.3358610

[35] Seda Gürses and Van Joris Hoboken. 2017. Privacy After the Agile Turn. In *Cambridge Handbook of Consumer Privacy*, Jules Polonetsky, Omer Tene, and Evan Selinger (Eds.). Cambridge University Press. https://doi.org/10.31235/osf.io/9gy73

[36] Drew Harwell. 2019. Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns. *The Washington Post* (28 8 2019).

[37] Anna Lauren Hoffmann. 2021. Terms of inclusion: Data, discourse, violence. *New Media & Society* 23 (2021), 146144482095872. Issue 12. https://doi.org/10.1177/1461444820958725

[38] Chris Jay Hoofnagle. 0. Online privacy. In *Federal Trade Commission Privacy Law and Policy*. Cambridge University Press, Cambridge, 145–192. https://doi.org/10.1017/CBO9781316411292.007

[39] Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen Borgesius. 2019. The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law* 28, 1 (2 1 2019), 65–98. https://doi.org/10.1080/13600834.2019.1573501

[40] Lara Houston, Steven J. Jackson, Daniela K. Rosner, Syed Ishtiaque Ahmed, Meg Young, and Laewoo Kang. 2016. Values in Repair. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 1403–1414. https://doi.org/10.1145/2858036.2858470

[41] Global Reporting Initiative. 0. GRI Standards - English. https://www.globalreporting.org/how-to-use-the-gri-standards/gri-standards-english-language/ [Online; accessed 2022-07-09].

[42] Lilly Irani. 2018. "Design Thinking": Defending Silicon Valley at the Apex of Global Labor Hierarchies. *Catalyst: Feminism, Theory, Technoscience* 4, 1 (2018), 1–19. https://doi.org/10.28968/cftt.v4i1.29638

[43] Lilly C. Irani and M. Six Silberman. 2013. Turkopticon: Interrupting Worker Invisibility in Amazon Mechanical Turk. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Paris, France) *(CHI '13)*. Association for Computing Machinery, New York, NY, USA, 611–620. https://doi.org/10.1145/2470654.2470742

[44] Steven J. Jackson, Paul N Edwards, Geoffrey C. Bowker, and Cory P. Knobel. 2007. Understanding infrastructure: History, heuristics and cyberinfrastructure policy. *First Monday* 12, 6 (4 6 2007), 1–8. https://doi.org/10.5210/fm.v12i6.1904

[45] Steven J. Jackson, Tarleton Gillespie, and Sandy Payette. 2014. The Policy Knot. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Baltimore, Maryland, USA) *(CSCW '14)*. Association for Computing Machinery, New York, NY, USA, 588–602. https://doi.org/10.1145/2531602.2531674

[46] Steven J. Jackson and Laewoo Kang. 2014. Breakdown, obsolescence and reuse. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14* (2014). Association for Computing Machinery, New York, NY, USA, 449–458. https://doi.org/10.1145/2556288.2557332

[47] Steven J. Jackson, Stephanie B. Steinhardt, and Ayse Buyuktur. 2013. Why CSCW Needs Science Policy (and Vice Versa). In *Proceedings of the 2013 Conference on Computer Supported Cooperative Work* (San Antonio, Texas, USA) *(CSCW '13)*. Association for Computing Machinery, New York, NY, USA, 1113–1124. https://doi.org/10.1145/2441776.2441902

[48] Laura Jehl and Alan Friel. 2019. CCPA and GDPR Comparison Chart. https://iapp.org/media/pdf/resource_center/CCPA_GDPR_Chart_PracticalLaw_2019.pdf [Online; accessed 2022-01-11].

[49] Nir Kaissar. 2022. Institutional Investors Are Flexing Their ESG Muscles. https://www.bloomberg.com/opinion/articles/2022-04-13/institutional-investors-are-flexing-their-esg-muscles [Online; accessed 2022-07-09].

[50] Tom Kemp. 2020. Comparing Enforcement: GDPR vs. CCPA vs. CPRA. https://tomkemp.blog/2020/06/04/comparing-enforcement-gdpr-vs-ccpa-vs-cpra/ [Online; accessed 2022-01-10].

[51] Vera Khovanskaya, Lynn Dombrowski, Jeffrey Rzeszotarski, and Phoebe Sengers. 2019. The Tools of Management: Adapting Historical Union Tactics to Platform-Mediated Labor. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (7 11 2019), 1–22. https://doi.org/10.1145/3359310

[52] Jennifer King. 2019. "Becoming Part of Something Bigger": Direct to consumer genetic testing, privacy, and personal disclosure. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (7 11 2019), 1–33. https://doi.org/10.1145/3359260

[53] Laura Kocksch, Matthias Korn, Andreas Poller, and Susann Wagenknecht. 2018. Caring for IT Security. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–20. https://doi.org/10.1145/3274361

[54] Min Kyung Lee, Daniel Kusbit, Evan Metsky, and Laura Dabbish. 2015. Working with Machines: The Impact of Algorithmic and Data-Driven Management on Human Workers. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 1603–1612. https://doi.org/10.1145/2702123.2702548

[55] He Li, Won Gyun No, and Tawei Wang. 2018. SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems* 30 (9 2018), 40–55. https://doi.org/10.1016/j.accinf.2018.06.003

[56] Silvia Lindtner and Seyram Avle. 2017. Tinkering with Governance: Technopolitics and the Economization of Citizenship. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (6 12 2017), 1–18. https://doi.org/10.1145/3134705

[57] Silvia Lindtner, Shaowen Bardzell, and Jeffrey Bardzell. 2018. Design and Intervention in the Age of "No Alternative". *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (11 2018), 1–21. https://doi.org/10.1145/3274378

[58] Philip M. Linsley and Philip J. Shrives. 2006. Risk reporting: A study of risk disclosures in the annual reports of UK companies. *The British Accounting Review* 38, 4 (12 2006), 387–404. https://doi.org/10.1016/j.bar.2006.05.002

[59] Alex Loftus and Hug March. 2019. Integrating what and for whom? Financialisation and the Thames Tideway Tunnel. *Urban Studies* 56, 11 (30 8 2019), 2280–2296. https://doi.org/10.1177/0042098017736713

[60] Michael Madaio, Lisa Egede, Hariharan Subramonyam, Jennifer Wortman Vaughan, and Hanna Wallach. 2022. Assessing the Fairness of AI Systems: AI Practitioners' Processes, Challenges, and Needs for Support. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW1 (30 3 2022), 1–26. https://doi.org/10.1145/3512899

[61] Michael A. Madaio, Luke Stark, Jennifer Wortman Vaughan, and Hanna Wallach. 2020. Co-Designing Checklists to Understand Organizational Challenges and Opportunities around Fairness in AI. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376445

[62] Aleecia M McDonald and Lorrie Faith Cranor. 2008. The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society* 4, 3 (2008), 543–568.

[63] Nora McDonald, Karla Badillo-Urquiola, Morgan G. Ames, Nicola Dell, Elizabeth Keneski, Manya Sleeper, and Pamela J. Wisniewski. 2020. Privacy and Power: Acknowledging the Importance of Privacy Research and Design for Vulnerable Populations. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '20)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/3334480.3375174

[64] Nora McDonald and Andrea Forte. 2020. The Politics of Privacy Theories: Moving from Norms to Vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376167

[65] Nora McDonald and Andrea Forte. 2021. Powerful Privacy Norms in Social Network Discourse. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (13 10 2021), 1–27. https://doi.org/10.1145/3479565

[66] Jacob Metcalf, Emanuel Moss, and danah boyd. 2019. Owning ethics: Corporate logics, Silicon Valley, and the institutionalization of ethics. *Social Research* 86, 2 (2019), 449–476.

[67] Milagros Miceli, Julian Posada, and Tianling Yang. 2022. Studying Up Machine Learning Data: Why Talk About Bias WhenWe Mean Power? *Proceedings of the ACM on Human-Computer Interaction* 6, GROUP (14 1 2022), 1–14. https://doi.org/10.1145/3492853

[68] Milagros Miceli, Martin Schuessler, and Tianling Yang. 2020. Between Subjectivity and Imposition: Power Dynamics in Data Annotation for Computer Vision. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (14 10 2020), 1–25. https://doi.org/10.1145/3415186

[69] Michael Muller. 2014. Whose Values? Whose Design? (2014). http://ethicsworkshopcscw2014.files.wordpress.com/2013/10/muller-whose-values.pdf

[70] U.S. Department of Homeland Security. 2010. Privacy Impact Assessments: The Privacy Office Official Guidance (June 2010). https://www.dhs.gov/sites/default/files/publications/privacy_pia_guidance_june2010_0.pdf [Online; accessed 2017-01-01].

[71] Ann Morales Olazábal. 2011. False forward-looking statements and the PSLRA's safe harbor. *Indiana Law Journal* 86, 2 (2011), 595–643.

[72] Anthony Onoja and Godwin O Agada. 2015. Voluntary risk disclosure in corporate annual reports: An empirical review. *Research Journal of Finance and Accounting* 6, 17 (2015), 1–8.

[73] Samir Passi and Steven J Jackson. 2018. Trust in Data Science: Collaboration, Translation, and Accountability in Corporate Data Science Projects. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (1 11 2018), 1–28. https://doi.org/10.1145/3274405

[74] Samir Passi and Phoebe Sengers. 2020. Making data science systems work. *Big Data and Society* 7, 2 (2020), 13 pages. https://doi.org/10.1177/2053951720939605

[75] James Pierce. 2019. Lamps, Curtains, Robots: 3 scenarios for the future of the smart home. In *Proceedings of the 2019 on Creativity and Cognition - C&C '19* (2019). ACM Press, New York, New York, USA, 423–424. https://doi.org/10.1145/3325480.3329181

[76] Rebecca Rabinowitz. 2020. From Securities to Cybersecurity: The SEC Zeroes In on Cybersecurity. *Boston College Law Review* 61, 4 (2020), 1535.

[77] Ranking Digital Rights. 2020. 2020 RDR Index methodology. https://rankingdigitalrights.org/index2020/methodology [Online; accessed 2022-07-09].

[78] Emma Rose and Josh Tenenberg. 2016. 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* (2016). ACM Press, New York, New York, USA, 1–10. https://doi.org/10.1145/2987592.2987608

[79] Daniela K. Rosner and Morgan Ames. 2014. Designing for repair? Infrastructures and materialities of breakdown. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing - CSCW '14* (2014). ACM Press, New York, NY, USA, 319–331. https://doi.org/10.1145/2531602.2531692

[80] Nikita Samarin, Shayna Kothari, Zaina Siyed, Primal Wijesekera, and Jordan Fischer. 2021. *Investigating the Compliance of Android App Developers with the CCPA*. Technical Report. Workshop on Technology and Consumer Protection (ConPro '21). https://www.ieee-security.org/TC/SPW2021/ConPro/papers/samarin-conpro21.pdf

[81] Galit Sarfaty. 2013. Human Rights Meets Securities Regulation. *Virginia Journal of International Law* 54 (2013), 97–126.

[82] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. 2015. A Design Space for Effective Privacy Notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)* (2015). 1–17.

[83] Philipp Schreck. 2013. Disclosure (CSR Reporting). In *Encyclopedia of Corporate Social Responsibility*, Samuel O Idowu, Nicholas Capaldi, Liangrong Zu, and Das Ananda Gupta (Eds.). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-28036-8

[84] US Securities and Exchange Commission. 2011. CF Disclosure Guidance: Topic No. 2: Cybersecurity. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm [Online; accessed 2021-02-16].

[85] US Securities and Exchange Commission. 2018. Commission Statement and Guidance on Public Company Cybersecurity Disclosures. https://www.sec.gov/rules/interp/2018/33-10459.pdf

[86] US Securities and Exchange Commission. 2019. Division of Enforcement 2019 Annual Report. https://www.sec.gov/files/enforcement-annual-report-2019.pdf

[87] US Securities and Exchange Commission. 2020. SEC Adopts Rule Amendments to Modernize Disclosures of Business, Legal Proceedings, and Risk Factors Under Regulation S-K. https://www.sec.gov/news/press-release/2020-192 [Online; accessed 2022-07-09].

[88] Phoebe Sengers, Kaiton Williams, and Vera Khovanskaya. 2021. Speculation and the Design of Development. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (13 4 2021), 1–27. https://doi.org/10.1145/3449195

[89] Katie Shilton. 2018. Values and Ethics in Human-Computer Interaction. *Foundations and Trends® in Human–Computer Interaction* 12, 2 (2018), 107–171. https://doi.org/10.1561/1100000073

[90] Katie Shilton, Jes A. Koepfler, and Kenneth R. Fleischmann. 2014. How to see values in social computing: Methods for Studying Values Dimensions. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*. ACM, New York, NY, USA, 426–435. https://doi.org/10.1145/2531602.2531625

[91] Michael Skirpan and Casey Fiesler. 2018. Ad Empathy: A Design Fiction. In *Proceedings of the 2018 ACM Conference on Supporting Groupwork (GROUP '18)* (2018). ACM Press, New York, New York, USA, 267–273. https://doi.org/10.1145/3148330.3149407

[92] Daniel J Solove. 2013. Privacy Self-Management and the Consent Dilemma. *Harvard Law Review* 126 (2013), 1880–1903.

[93] Danny Spitzberg, Kevin Shaw, Colin Angevine, Marissa Wilkins, M Strickland, Janel Yamashiro, Rhonda Adams, and Leah Lockhart. 2020. Principles at Work: Applying "Design Justice" in Professionalized Workplaces. *CSCW 2020 Workshop on Collective Organizing and Social Responsibility* (2020), 1-5 pages. https://doi.org/10.21428/93b2c832.e3a8d187

[94] Susan Leigh Star and Karen Ruhleder. 1996. Steps Toward an Ecology of Infrastructure: Design and Access for Large Spaces Information. *Information Systems Research* 7, 1 (1996), 111–134.

[95] Luke Stark, Daniel Greene, and Anna Lauren Hoffmann. 2021. Critical Perspectives on Governance Mechanisms for AI/ML Systems. In *The Cultural Life of Machine Learning*. Springer International Publishing, Cham, 257–280. https://doi.org/10.1007/978-3-030-56286-1_9

[96] Luke Stark, Jen King, Xinru Page, Airi Lampinen, Jessica Vitak, Pamela Wisniewski, Tara Whalen, and Nathaniel Good. 2016. Bridging the Gap between Privacy by Design and Privacy in Practice. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. ACM Press, New York, New York, USA, 3415–3422. https://doi.org/10.1145/2851581.2856503

[97] Stephanie B Steinhardt. 2016. Breaking Down While Building Up: Design and Decline in Emerging Infrastructures. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16* (2016). ACM Press, New York, New York, USA, 2198–2208. https://doi.org/10.1145/2858036.2858420

[98] Maddie Stone. 2021. The shareholder fight that forced Apple's hand on repair rights. *The Verge* (17 Nov. 2021). https://www.theverge.com/2021/11/17/22787336/apple-right-to-repair-self-service-diy-reason-microsoft

[99] Lucy Suchman. 1993. Working relations of technology production and use. *Computer Supported Cooperative Work* 2, 1-2 (23 March 1993), 21–39. https://doi.org/10.1007/BF00749282

[100] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Privacy Champions in Software Teams: Understanding Their Motivations, Strategies, and Challenges. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI'21)* (2021-05-06). ACM, New York, NY, USA, 1–15. https://doi.org/10.1145/3411764.3445768

[101] Janet Vertesi and Paul Dourish. 2011. The Value of Data: Considering the Context of Production in Data Economies. In *Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work* (Hangzhou, China) *(CSCW '11)*. Association for Computing Machinery, New York, NY, USA, 533–542. https://doi.org/10.1145/1958824.1958906

[102] Jessica Vitak, Michael Zimmer, Anna Lenhart, Sunyup Park, Richmond Y. Wong, and Yaxing Yao. 2021. 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* (2021-10-23). ACM, New York, NY, USA, 364–367. https://doi.org/10.1145/3462204.3481724

[103] Yang Wang. 2017. The Third Wave? Inclusive Privacy and Security. In *Proceedings of the 2017 New Security Paradigms Workshop - NSPW 2017* (2017). ACM Press, New York, New York, USA, 122–130. https://doi.org/10.1145/3171533.3171538

[104] Christine T. Wolf, Mariam Asad, and Lynn S. Dombrowski. 2022. Designing within Capitalism. In *Designing Interactive Systems Conference* (2022-06-13). ACM, New York, NY, USA, 439–453. https://doi.org/10.1145/3532106.3533559

[105] Janis Wong and Tristan Henderson. 2019. The right to data portability in practice: exploring the implications of the technologically neutral GDPR. *International Data Privacy Law* 9, 3 (aug 2019), 173–191. https://doi.org/10.1093/idpl/ipz008

[106] Richmond Y Wong. 2021. Tactics of Soft Resistance in User Experience Professionals' Values Work. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 28. https://doi.org/10.1145/3479499

[107] Richmond Y Wong, Karen Boyd, Jake Metcalf, and Katie Shilton. 2020. Beyond Checklist Approaches to Ethics in Design. In *Conference Companion Publication of the 2020 on Computer Supported Cooperative Work and Social Computing* (2020-10-17). ACM, New York, NY, USA, 511–517. https://doi.org/10.1145/3406865.3418590

[108] Richmond Y. Wong and Steven J. Jackson. 2015. Wireless Visions: Infrastructure, Imagination, and U.S. Spectrum Policy. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '15)* (2015). ACM Press, New York, NY, USA, 105–115. https://doi.org/10.1145/2675133.2675229

[109] Richmond Y Wong, Vera Khovanskaya, Sarah E Fox, Nick Merrill, and Phoebe Sengers. 2020. Infrastructural Speculations: Tactics for Designing and Interrogating Lifeworlds. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (2020-04-21). ACM, New York, NY, USA, 1–15. https://doi.org/10.1145/3313831.3376515

[110] Richmond Y Wong, Michael A Madaio, and Nick Merrill. 2023. Seeing Like a Toolkit: How Toolkits Envision the Work of AI Ethics. *Proceedings of the ACM on Human-Computer Interaction* 7 (2023), 27 pages. Issue CSCW1. https://doi.org/10.1145/3579621

[111] Richmond Y. Wong and Deirdre K. Mulligan. 2019. 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). ACM Press, New York, NY, USA. https://doi.org/10.1145/3290605.3300492

[112] Richmond Y. Wong, Deirdre K. Mulligan, Ellen Van Wyk, James Pierce, and John Chuang. 2017. Eliciting Values Reflections by Engaging Privacy Futures Using Design Workbooks. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 111 (Dec 2017), 26 pages. https://doi.org/10.1145/3134746

[113] Yaxing Yao, Richmond Wong, Pardis Emami-Naeini, Nick Merrill, Xinru Page, Yang Wang, and Pamela Wisniewski. 2019. Ubiquitous Privacy: Research and Design for Mobile and IoT Platforms. In *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing* (Austin, TX, USA) *(CSCW '19)*. Association for Computing Machinery, New York, NY, USA, 533–538. https://doi.org/10.1145/3311957.3359430

Received January 2022; revised July 2022; accepted November 2022