Routledge
Taylor & Francis Group

Information, Communication & Society

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rics20

Data privacy and political distrust: corporate ‘pro liars,’ ‘gridlocked Congress,’ and the Twitter issue public around the US privacy legislation

Jeeyun (Sophia) Baik

To cite this article: Jeeyun (Sophia) Baik (2020): Data privacy and political distrust: corporate ‘pro liars,’ ‘gridlocked Congress,’ and the Twitter issue public around the US privacy legislation, Information, Communication & Society, DOI: 10.1080/1369118X.2020.1850839

To link to this article: https://doi.org/10.1080/1369118X.2020.1850839

Published online: 29 Nov 2020.

INFORMATION, COMMUNICATION & SOCIETY
https://doi.org/10.1080/1369118X.2020.1850839

Data privacy and political distrust: corporate 'pro liars,' 'gridlocked Congress,' and the Twitter issue public around the US privacy legislation

Jeeyun (Sophia) Baik

Annenberg School for Communication and Journalism, University of Southern California, Los Angeles, CA, USA

ABSTRACT

This study explores how emerging US data privacy regulations are discussed at state and federal levels, examining Twitter discourse around Senate public hearings on data privacy and public forums on the California Consumer Privacy Act (CCPA). The recent legal steps reflect growing public outcry over corporate data misuses and lack of appropriate legislation. The findings suggest that the issue public of Twitter users in this study largely considered corporations and the government as untrustworthy actors for privacy legislation. The political distrust was raising doubts over regulatory capture and if a future US federal privacy law will be weaker than state laws (e.g., CCPA) while overriding them. The study explores implications of the findings on the current deadlock over the state preemption clause in developing a comprehensive federal privacy law. I argue that the emerging regulatory efforts on data privacy may not be effective unless the public trust in institutions is regained in the US and that the continuing absence of a federal law amid the political distrust can leave people with limited individual privacy strategies as a result.

ARTICLE HISTORY
Received 12 February 2020
Accepted 18 October 2020

KEYWORDS
Data privacy; Twitter; issue public; political trust; CCPA

Introduction

In the United States, courts have interpreted there is an implicit individual right to privacy from government surveillance in the penumbra of the US Constitution (Cheney-Lippold, 2018). However, regarding individual privacy in the private sector, the US framework has favored corporate self-regulations with minimal government interventions; only a few industries specifically considered dealing with sensitive personal data are regulated through rules such as the Gramm-Leach-Bliley-Act (GLBA) for financial information (1999), the Health Insurance Portability and Accountability Act (HIPAA) for health information (1996), and the Fair Credit Reporting Act (FCRA) for credit information (1970). Due to such a 'sectoral approach,' there exists 'no generalized protection' in the United States that shields individuals from the 'collection, processing, and sale of their personal data by the private sector' (Yeh, 2018, p. 286). Reidenberg (2000) and

CONTACT Jeeyun (Sophia) Baik jeeyunba@usc.edu Annenberg School for Communication and Journalism, University of Southern California, Los Angeles, CA 90089, USA

Westin (1966) defined data privacy as the ability of individuals to self-determine their information flow by controlling the data's whereabouts, yet increasing cases of data breaches and misuse have led the public to question whether they are enjoying rights to data privacy in the current information age (Auxier et al., 2019).

One high-profile case that caught wide public attention was the Cambridge Analytica scandal disclosed in March 2018. It was revealed that the personal data of millions of Facebook users were collected *without* users' consent to target voters with psychographic messages during the 2016 US presidential election. Facebook encountered a huge backlash as a result of the scandal, and Mark Zukerberg, CEO of Facebook, testified on Facebook's data protection protocol at a Senate hearing in April 2018. Digital platforms including Facebook have made important decisions on the collection and flow of personal data, earning enormous profits with ad-based business models and sharing user information with third parties, yet there is no clear legal protection that regulates the private sector's unwarranted data practices in the US

With growing public concerns, protection of data privacy has emerged as one of the most pressing issues in regards to the governance of digital space (Minkkinen, 2019; Youm & Park, 2016). The European Union (EU) replaced its 1995 Data Protection Directive with the General Data Protection Regulation (GDPR) in May 2018. In the US, California introduced the California Consumer Privacy Act (CCPA) in June 2018, becoming the first state in the country to enact its own data privacy law. The CCPA went into effect early 2020, but some have raised concerns, predicting a 'convoluted regulatory disaster' due to each state's potentially divergent local approach to data privacy (Allan, 2018). The CCPA has accordingly prompted debates in Congress regarding the establishment of an omnibus federal-level privacy law. Recent years imply a critical moment to shape and crystallize the US data privacy governance as such.

These legal processes are still in their initial stages, and few studies have closely investigated the emerging regulatory efforts in the US This study is the first one to closely look at the case of the California law in juxtaposition with the federal-level discourse on data privacy. It focuses on Twitter discourse in order to likely capture diverse views within a segment of the issue public on data privacy; the study does not claim to analyze a representative sample or generalize the findings to the whole public discourse. It aims to answer the following two main questions, exploring publicly available tweets: (1) Do the tweets on data privacy public hearings reflect or imply the Twitter users' (dis)trust of institutional actors such as corporations and the US government? and (2) Is the (dis)-trust similarly or differently presented in the federal and the California discourses? Throughout this article, the words 'data privacy' and 'data protection' will be used interchangeably in presenting the literature and findings of this study, mostly following the original texts cited. Data protection is generally considered a specific policy measure to safeguard data privacy (Bennett, 2008), but the debate over the terms is not within the scope of this study.

Governance of data privacy

In the past decades, corporations in the US have found ways to work around the issue of data privacy through self-regulatory measures such as corporate privacy policies and terms of service; in Europe, privacy has been traditionally protected by the State

(Drezner, 2004; Fernback & Papacharissi, 2007; Youm & Park, 2016). As the GDPR of the EU enforced in 2018 applies to any organizations holding personal data on EU citizens, however, companies with a transnational consumer base started to take data privacy more seriously, in preparation for compliance with the new EU law. Shortly after the enforcement of the GDPR, the CCPA was signed by then-Governor Jerry Brown in June 2018 and went into effect on 1 January 2020. During the CCPA rulemaking process, corporate stakeholders such as tech companies, trade associations, and advertising industries heavily lobbied against it, out of a concern that it would become a *de facto* national standard (Middleton, 2018). The battle clearly demonstrated that negotiating data privacy regulations involves both 'large-scale trends' and 'the debate, lobbying and decisions of actors relevant to privacy protection' (Minkkinen, 2019, p. 985). While the CCPA elicited the federal versus state conflict over data privacy regulations in the United States, other states such as Vermont, New York, and Washington followed suit after California, introducing similar state laws to the CCPA. Considering the emerging efforts to govern data privacy in different parts of the world within and beyond the United States, it would be meaningful to examine how the newly introduced US privacy regulations are understood by the public.

Institutional privacy and political (dis)trust

The current data privacy regulations proposed in the US stem from a societal debate on how we would govern 'institutional privacy' by limiting companies' or the government's access to information of individuals (Raynes-Goldie, 2010). The focus of this study is the US government's privacy regulation of corporate data practices, and it thus speaks to 'institutional trust' or the trust people have in 'institutions, government agencies, or corporate entities' (p. 51). On one hand, the institutional trust regarding privacy regulations of the private sector pertains to the entity that *should be regulated*: the corporations. Privacy is known to build trust for information-sharing (Waldman, 2018), and studies have identified 'trust' to be a core value for people to negotiate whether and to what extent one would share personal information with institutions (Marwick & Hargittai, 2019). Frequent cases of corporate data breaches and data sharing for invasive targeted advertising these days have, therefore, contributed to the public's growing distrust of corporations and the societal demand for attendant privacy regulations.

On the other hand, the institutional trust is about the entity that *should be regulating*: the US government or legislature. The institutional trust here particularly represents a form of 'political trust' defined as 'confidence that authorities will observe the rules of the game and serve the general interest' (Citrin & Muste, 1999, p. 465). Political trust is critical to a well-functioning democracy (Almond & Verba, 2015), as it concerns the 'institutions' and 'procedures' that 'link overarching democratic principles to the everyday actors and policies' (van der Meer, 2017, p. 5). That is, political trust indicates how much institutional actors and procedures governed by the institutions are being validated by the constituency of a democracy. A representative democracy, for example, cannot work properly unless people trust that the institutional bodies are serving the interests of the public and that every voice is duly reflected into the democratic process with procedural justice. A democratic society can face challenges for creating and enforcing policies and laws for the governance of citizens when political distrust is prevalent

(Boulianne, 2019). It is, therefore, the public belief in democracy that is fundamentally at stake in matters of privacy and its regulations discussed in this paper. Privacy has been considered an important value to a democratic system (Regan, 1995), yet whether the recent efforts to legislate privacy protections would be in the interest of the general public is in question.

In the United States, Americans' general trust in many institutions have been declining, and Congress (12%) and big business (21%) were the institutions enjoying the lowest level of trust in a 2018 Gallup survey (Knight Commission on Trust, Media and Democracy, 2019). When it comes to personal data protection in particular, it has been reported that people in the US tend to distrust both the federal government and social media sites (Geiger, 2018). The political distrust in the US was proven warranted, for example, when the Senate privacy hearing in 2018 did not invite any consumers, while listening to only giant technology companies such as Apple, Google, Amazon, Twitter, and AT&T. The stark lack of civic presence in the forum raised doubts if the authority is to serve the general public's interest. It naturally invited concerns over 'regulatory capture,' the 'process through which regulated monopolies end up manipulating the state agencies that are supposed to control them' (Dal Bó, 2006, p. 203). In the US history, there were several attempts to pass federal privacy law focused on the private sector such as the Freedom from Behavioral Profiling Act (2000), the Consumer Online Privacy and Disclosure Act (2000), the Consumer Privacy Protection Act (2011, 2015), the Commercial Privacy Bill of Rights Act (2011, 2014), the Data Broker Accountability and Transparency Act (2014), and the Consumer Privacy Bill of Rights Act (2015), but nothing was successful in the end. The recent Congressional questioning of tech giants (i.e., Facebook, Google, Amazon, and Apple) in July 2020[1] also showed that there is a great level of distrust of the giant tech companies among the public.

Political trust has four elements to base the trustor's (or the subject's) evaluation of the trustee (or the object): (1) the subject's trust in the object's 'competence,' (2) trust in the object's benign 'care,' (3) trust that the object's commitment is enforceable ('accountability'), and (4) trust that the object can be predicted ('predictability') (van der Meer, 2017, p. 5). Political (dis)trust can be formed based on the public's level of 'knowledge, expectations, risk, and interests' often informed by not only direct experiences with the institutional actors but also mass media and educational resources (Theiss-Morse et al., 2015, pp. 169–171). One way to examine political (dis)trust can be to explore the trustor's knowledge, expectations, risk, and interests over the trustee's competence, care, accountability, and predictability. This study closely looked into a Twitter discourse on data privacy and identified communication traces that can shed light on the Twitter users' reasoning for institutional (dis)trust over regulations of data privacy.

Method

The study investigated the Twitter discourse on the US data privacy regulations by collecting tweets on (1) two Senate public hearings on the federal data protection held on 26 September 2018 and 27 February 2019, and (2) seven CCPA public forums held between January and March 2019 (see Appendix A for search details). All the tweets were collected through DiscoverText using Twitter's open API. The dataset of the two Senate public hearings resulted in 11,014 tweets, and the dataset of the seven CCPA public forums resulted in 3,624 tweets, after deduplication and exclusion of suspicious bot accounts.[2] The Institutional Review Board (IRB) of the researcher's university approved the study.

There are two reasons this paper chose to focus on Twitter discourse, worth mentioning. First, I tried to likely capture voices of people who may have not attended the state and federal public meetings. The attempts of corporations to override the CCPA by lobbying for the introduction of a less strict federal regulation were constantly reported in the media, implying the possible dominance of corporate voices in the rulemaking process. Also, Senate public hearings didn't invite any civil society actors by early 2019. These led me to explore Twitter discourse to address more diverse voices, if any. Second, based on previous studies on the general public's legal knowledge of data privacy policies, I supposed that asking the general public about data privacy laws through surveys or interviews might be less helpful to answer my research questions. Previous studies on the EU case suggest that the EU citizens' knowledge of data protection policies varied across the EU countries despite its longer history of strong data privacy regulations (Hallinan et al., 2012; Sarikakis & Winter, 2017). The lack of the general public's awareness of data privacy regulations was frequently mentioned by consumer advocates at the CCPA public forums as well (Baik, 2020).

Accordingly, the Twitter users who contributed to the discourse on the US data privacy regulations sampled in this study are rather an 'issue public' composed of people who share the 'relevance of the issue' on data privacy to varying degrees and who shape a constantly evolving collective of voices through 'articulation' of the very issue (Marres, 2015). The Twitter users studied in this article are considered an 'issue public' who share 'a heightened interest' in data privacy and its regulations (McKelvey et al., 2014). Looking at the issue public, this study tried to analyze the perspectives not necessarily limited to corporate or regulatory bodies.

The study conducted a qualitative thematic analysis (Braun & Clarke, 2006) on both datasets, going through three rounds of qualitative thematic coding (see Figure 1). The last round of coding was conducted to check if the themes reached saturation. The size of sampling was determined to ensure manageability for close reading (Wheatley & Vatnoey, 2020). At each round, I closely read the tweets and created themes as they emerged. Throughout each stage, the type of Twitter handles was coded, and I organized the coded themes and relevant examples according to the study's research questions. The study identified two major themes – (1) distrust of institutions and (2) reference to privacy frameworks – and two minor themes – (i) privacy strategy and (ii) consumer awareness and literacy (see Table 1). The most dominant theme in federal and California datasets differed (see Figure 2[3]).

Distrust of institutions: more distrust in the federal discourse, more distrust of corporations[4]

In both datasets, there emerged the theme of distrust of private and public institutions. Coding of the distrust theme was operationalized based on each tweet's expressed 'knowledge,' 'expectations,' 'risk,' or 'interests' over 'competence,' 'care,' 'accountability,' or 'predictability' of the institutions (van der Meer, 2017; Theiss-Morse et al., 2015). For example, as shown in Table 1, a tweet that said 'So many pro liars in one room' was coded

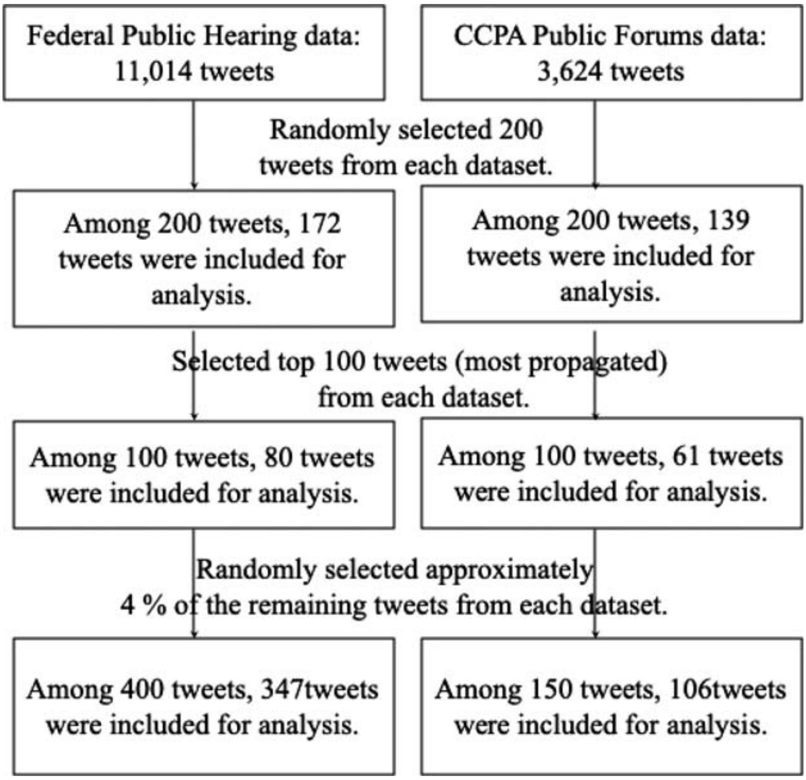
Federal Public Hearing data: 11,014 tweets
CCPA Public Forums data: 3,624 tweets
Randomly selected 200 tweets from each dataset.
Among 200 tweets, 172 tweets were included for analysis.
Among 200 tweets, 139 tweets were included for analysis.
Selected top 100 tweets (most propagated) from each dataset.
Among 100 tweets, 80 tweets were included for analysis.
Among 100 tweets, 61 tweets were included for analysis.
Randomly selected approximately 4 % of the remaining tweets from each dataset.
Among 400 tweets, 347tweets were included for analysis.
Among 150 tweets, 106tweets were included for analysis.

Figure 1. The working trajectory of the qualitative thematic analysis.

Note: Tweets were excluded for analysis when they were either irrelevant, deleted, or suspended.

Table 1. An overview of the four themes.

Themes		Federal public hearings	CCPA public forums
(1) Distrust of institutions	Distrust of corporations	'So many pro liars in one room.'	Facebook's Ad Preference page is useless as long as the user needs to 'click on 1,600 advertisers to fix.'
	Distrust of the government	The Congress is to 'ignore every consumer in the country.'	'Their state proposition bypassed a corrupt, gridlocked Congress.'
(2) Reference to privacy frameworks	EU	'When I asked Amazon, AT&T, Google, Apple, & Twitter execs if they plan on pulling out of Europe or CA because of their stronger privacy laws, they said no … '	Many of the advertising business are located 'outside of California' and we need 'regulation like #GDPR in America.'
	USA	'Tech companies have pushed for a federal data privacy regulation, as it could preempt the California Consumer Privacy Act … '	'California law could be Congress' model for data privacy. Or it could be erased.' 'Texas should copy California: Pass a new internet privacy law like the Golden State's.'
(i) Privacy management strategy		'How much worse can Google get? Use @DuckDuckGo instead!' Use the hashtag #RealPrivacy to show a 'coordinated, real-time' civil response to the Senate hearing.	I don't think behavioral advertising is a big issue – if people don't like ads they can just use 'pop-up blockers' and the problem can be easily solved.
(ii) Consumer awareness and literacy		I urge 'Americans' to 'stay alert' as the federal privacy legislation is being shaped.	The Attorney General should 'ensure that the #CCPA works for consumers.'

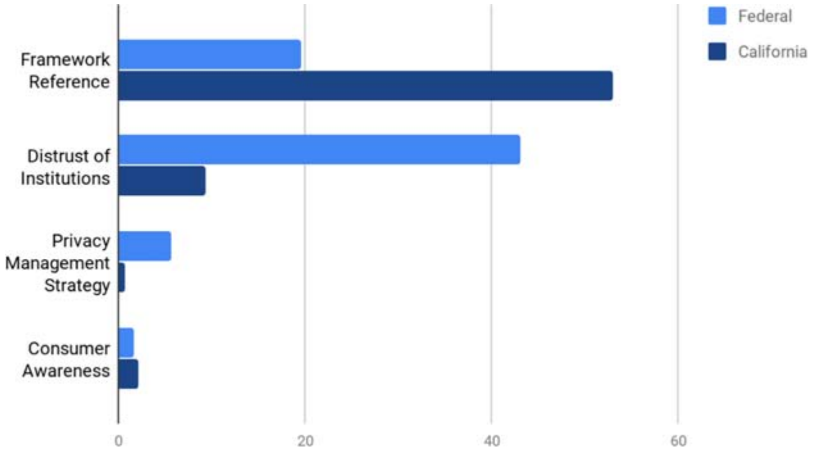

Figure 2. Frequency of the four themes (in percentage).

as showing the distrust of corporations as it implies the user's 'expectation' that the corporations gathering in the Senate public hearing would continue to lie before Congress and the public who is watching it, anticipating their lack of 'accountability' for privacy regulations. Likewise, a tweet that called Congress 'corrupt' and 'gridlocked' was coded as showing the distrust of the government as it reflects the user's 'knowledge' of Congress' corrupt acts, hinting at its 'incompetence' of passing any privacy law. The distrust of corporations was much more prominent than the distrust of government in both datasets (see Figure 3). Such distrust was most salient in the federal dataset, compared to the California dataset. This may be partially due to the larger presence of 'corporation' accounts identified in the California dataset, who wouldn't have necessarily engaged in expressing distrust of institutions when they are the very institutional entities criticized for their data practices.

In the federal dataset, an individual's tweet said that tech companies such as Google, AT&T, Amazon and Apple claim they are making 'robust changes' to their 'privacy mistakes' but in reality the so-called changes are 'essentially nothing but getting the public to

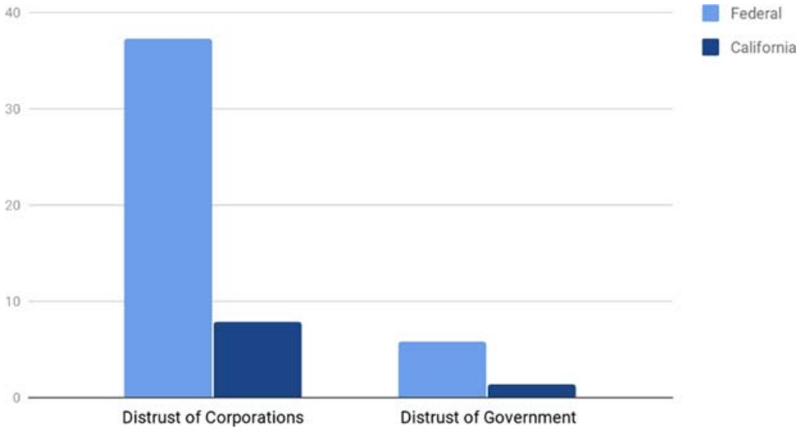

Figure 3. Distrust of institutions (in percentage).

click on new agreements' (25 September 2018). The user was showing distrust in the corporations' 'competence' to act in the interest of the individuals. The same tweet continued to address the problem of making it an individual responsibility to 'click agree' or opt out, when opting out can mean being 'excluded from participating in modern life' (25 September 2018). This addresses how digital services, in reality, function as a public infrastructure required for day-to-day activities (Hintz et al., 2017; Marwick & Hargittai, 2019).

One main reason for the distrust shown in the federal dataset was because the corporations were perceived to prioritize profits over individual privacy, thus not acting in the interest of the public. A tweet from a nonprofit organization claimed that Google is putting profits above 'privacy and safety' of its consumers by building 'vast data profiles on billions of people without their full awareness' all of which is intended for Google to 'make more money' (12 September 2018). Another tweet brought up a similar perspective, saying that Google's business cannot be aligned with privacy as Google will not 'make a product that blocks the gateway for its core business and cash cow' (24 September 2018). This speaks to 'an inherent tension' that exists in data protection laws regarding whether to treat 'data controllers' as 'trusted entities' or 'with distrust' when they are 'custodians of personal information' (Diaz et al., 2013, as cited in Coudert, 2014, p. 73).

Moreover, the tech companies' willingness to work with authoritarian regimes such as China was identified as another critical reason for the growing public distrust of corporations in the tweets. Tweets in the federal dataset frequently alluded to Google's projects in China when expressing their distrust of the corporation. Several tweets shared *The New York Times* article covering that Google allowed its 'partner company in #China to view a person's search history based on his or her phone number' (Conger, 2018); an individual user who shared the same article added, 'how much worse can Google get?' (27 September 2018). Another individual's tweet responded to Google's release of a framework to guide data privacy regulation, saying that 'a company who … is working with Communist China to censor the world is giving advice' (25 September 2018). The users' 'knowledge' of Google's operations in China was making Google an 'unpredictable' trustee as to if it will assist the similar kind of government surveillance in the US and/or if Google's privacy efforts are trustworthy.

In the California dataset, there also existed the distrust of corporations, especially in terms of problematic corporate data practices. A nonprofit organization's tweet addressed 'discrimination in the digital age' such as Facebook's letting advertisers exclude certain ethnic groups including Black and Latino populations from 'seeing information about housing, employment, and credit' (4 March 2019). The same tweet claimed that '#CCPA was a start, but #privacy problems are big' and that California 'needs #PrivacyForAll.' This tweet was raising a specific concern about the discriminatory data practice of corporations that can further marginalize people already disadvantaged in the society, making data privacy a 'luxury commodity' (Papacharissi, 2010) only the wealthy can afford. If the corporations genuinely 'care' about privacy of every user, they shouldn't be conducting such practices, and this was at the core of the political distrust. The other data practice deepening the public distrust was the impractical opt-out options offered to individuals. An individual Twitter user pointed out that Facebook's Ad Preference page, for example, is useless as long as the user needs to 'click on 1,600 advertisers' in order to fix the preference setting (19 February 2019). The impracticality was reiterated by a nonprofit organization which claimed that it is ‘not practical for consumers to opt out of every website they visit’ (5 February 2019). The impractical choices available to users were seen as insincerity or lack of corporate ‘competence’ in safeguarding consumer privacy. Other tweets further asserted ‘#Marketers Must Step Back From Personalization And Automation’ (1 February 2019) and that ‘it’s time for the shadowy world of data brokers to end’ (21 January 2019).

The tweets in both datasets showed distrust of the government as well, though it was less prevalent than distrust of corporations. The government was perceived to offer more opportunities to the giant tech companies than consumers in publicly discussing the best ways to protect data privacy. Several federal tweets shared an article before the September Senate hearing titled, ‘The Game is Rigged: Congress Invites No Consumer Privacy Advocates to its Consumer Privacy Hearing’ (Falcon & McKinney, 2018). The tweets pointed out the problematic lack of consumer voices in the regulatory efforts around federal consumer privacy. The same issue was frequently addressed by other tweets that shared a *LA Times* article, saying it is ‘outrageous’ that Congress ‘ignore[s] every consumer in the country’ (25 September 2018). An individual conceived of the Senate hearing on consumer data privacy as ‘a big-corporations-only platform’ (26 September 2018). It was suggested that the US government will ‘pay attention to the interests of big tech’ following ‘the free market way’ which was highlighted as different from ‘Europe,’ calling it ‘an interesting power dynamic to watch’ (25 September 2018). Overall, the public distrust of the government was centered on the questionable commitment of the authorities to enforce privacy regulations in favor of public interests as it rather appears to align its rulemaking with corporate interests.

Distrust of the government continued around the February Senate hearing as it became known to the public that the telecom industry was planning to throw a fundraising party for the Senate chair right before the hearing. A tweet quoted a news headline, ‘Telecom industry to throw fundraiser for Senate chair the night before data privacy hearing’ (Neidig, 2019), saying it is not a ‘good look’ (25 February 2019). Several tweets from nonprofit organizations explicitly expressed anger at the blatant corporate lobbying and influence-peddling. A tweet emphasized that ‘the fact that the telecom industry is throwing a lavish fundraiser … the night before a hearing … that could affect millions of people’s basic rights … is absolutely outrageous’ (26 February 2019). The tweets were problematizing the corporate dominance and the lack of consumer voice in the rulemaking of data privacy in the US The expressed distrust of the government was grounded on the outlook for the authority’s reinforcement of the power asymmetry between corporations and consumers, maintaining its close relationship with the industry which may likely result in ‘regulatory capture’ (Dal Bó, 2006).

The distrust of the government was expressed in the California dataset too, though very minimally, compared to the federal dataset. An individual user, in describing the CCPA for example, mentioned that the ‘proposition [CCPA] bypassed a corrupt, gridlocked Congress’ (13 January 2019), criticizing the Congress. None of the sampled tweets displayed any specific distrust of California’s authority *per se*. This is likely because the California public forums in early 2019 were held after California officially passed the CCPA in June 2018. The year of 2019 was for different stakeholders to make suggestions to the California Attorney General (AG) about the preferred details of the law. Therefore, it is possible that the public distrust was more geared to corporations who are the stakeholders at the other end of the debate, rather than the California authority who at least introduced the regulatory measure to protect privacy.

Reference to privacy frameworks and the implications for distrust

Another major theme that emerged in both datasets is the reference to different privacy frameworks within and beyond the United States; this was relatively more dominant in the California dataset than the federal dataset. The majority of the tweets in the California dataset was referencing the EU's GDPR, possibly because of the great presence of 'corporation' accounts. While the expectation of the CCPA to be either weaker or stronger than the GDPR varied across the tweets, many of them were generated by corporations trying to figure out the business implications of the CCPA. For example, there were a large number of tweets that announced informational sessions on the GDPR and the CCPA. A corporate tweet shared an informational resource, saying that 'While the #CCPA may seem like the US version of #GDPR, the two have some significant differences that businesses should understand' (7 March 2019). The corporations were largely focusing their attention on compliance issues.

The tweets further provide some insights on the contexts and implications of the political distrust. For example, non-corporate accounts often spoke about the conflicts going on between state and federal privacy frameworks. Especially the tweets generated after the Senate hearings informed how the big tech companies were asking for a possibly weaker federal law. A tweet by an individual user (27 September 2018) shared the headline of a media article titled, 'Google, Amazon, Twitter, other Big Tech to Congress: New California data privacy rules too tough' (Jardin, 2018). Another tweet from a media account said that 'Silicon Valley tech giants including Amazon, Apple and Google are asking the government for federal data protection laws to cut off patchwork laws from states' (26 September 2018). The tweets imply a possible context for the public distrust: the corporations are collectively trying to override California's new law with a weaker federal law by aggressively lobbying for Congress. In this context, it is hard to expect that people can trust the corporations' stated dedication to consumer privacy nor the intentions behind corporate support for a federal privacy law. An individual tweeted, 'California law could be Congress' model for data privacy. Or it could be erased' (11 February 2019). The concern over a future federal law's preemption of stricter state laws was not limited to the erasure of the CCPA but other state privacy laws: an individual said, 'If Congress includes preemption in federal law, this might erase the biometric privacy law in Illinois' (24 February 2019).

A Brookings report (2020) identified preemption as an 'endgame' issue with low consensus among stakeholders. The consumer advocates hope the states to serve as 'a laboratory' for strong privacy regulations considering the slow federal process, whereas the industry wants a 'single national set of rules to follow' (p. 16). In the California dataset, tweets recognized the importance of the CCPA as a stimulus to not only the federal law but also other states' privacy regulations. An individual user tweeted about the legislation proposed by the state of New York, calling it to be 'in the same vein as the #CCPA' (29 January 2019). Another individual in a tweet (12 January 2019) shared a news article that says, 'Texas should copy California: Pass a new internet privacy law like the Golden State's' (Lieber, 2019). When the CCPA is considered a roadmap for both federal and state laws, the key issue at stake is again whether the corporations' desire for a comprehensive federal law that preempts state laws is in fact to comply with a single *strongest* federal law or to *squash* stricter state laws. Considering the aforementioned lack of civic presence in rule-making and ongoing corporate data practices that prioritize profits, work with authoritarian regimes, continue to result in discriminatory impacts and provide impractical privacy options to consumers, it can be hard for the public to trust that the corporate support for a single federal law is to genuinely protect consumer privacy.

Ongoing individual privacy management strategies

A theme of privacy strategy was also identified in both datasets. This theme refers to several *individual* strategies and few *collective* strategies. In regard to individual strategies, tweets in the federal dataset often suggested other Twitter users to use alternate services such as DuckDuckGo or Firefox instead of Google, and Telegram instead of Whatsapp. A Twitter user, pointing out Google's questionable service in China, urged followers to 'Use @DuckDuckGo instead' (27 September 2018). Another individual introduced a link to a list of other services available that can be 'privacy-friendly alternatives to Google products' (26 September 2018).

In the tweets, the issue of data privacy was often understood as individual responsibility of not using the troublesome services. It is not to say that the individual efforts are meaningless; they can signal corporations how much their users are concerned about data privacy and that the users can quit. However, the kind of response that imposes responsibility on individuals cannot eliminate the root causes of privacy-invasive corporate practices (Baruh & Popescu, 2017; West, 2019). In the California dataset, for example, a tweet by a user who identified herself as an attendant of one CCPA public forum said that she didn't think behavioral advertising was a big issue as people can just use 'pop-up blockers,' if they don't like ads, and the problem can be easily solved (20 February 2019). The tweet perceived that privacy can be protected by individual strategies, failing to acknowledge the deeper structural asymmetry between corporations and consumers in controlling one's data.

The tweet reflects the US trajectory of having treated data privacy as a matter of individual choice. Yet digital services have become a public infrastructure widely used and demanded at a societal level (Hintz et al., 2017) and it shouldn't be only individuals who protect privacy from corporate violations. Instead we need a system that recognizes the importance of data infrastructures and provides due privacy protections. In the absence of a federal privacy law and with the existing distrust of institutions regarding data privacy regulations, this study shows that many users were left with limited individual strategies and often sustained the expectation to be individually responsible for one's privacy.

Consumer awareness and literacy

Several tweets in both datasets mentioned the importance of consumer awareness and literacy of the US regulations too. Around the Senate hearing, an individual user urged the 'Americans' to 'stay alert' as the federal privacy legislation is being shaped (26 September 2018), and another highlighted the importance of 'public pressure' in leading companies like Google to 'comply with some basic #privacy rights' (26 September 2018). Another individual's tweet discussed the critical role of 'privacy/trust-fluent' people as a watchdog to implement real changes (26 September 2018). While the federal tweets were largely concerned about the public awareness of the rulemaking, the tweets in the California dataset were rather addressing ways to enhance public literacy of the law itself. For example, a nonprofit organization requested the Attorney General of California 'to ensure that the #CCPA works for consumers' (5 February 2019). Even though the theme was not prevalent across the datasets, it recognizes a common need for improved consumer awareness and literacy of the emerging US data privacy regulations. If a new law implements rules that are designed in ways that are difficult for a general public to decipher or seek rights, the public distrust of institutions would likely persist.

Discussion

Political distrust at the federal level

The tweets sampled in this study show prevalent institutional distrust in terms of developing US data privacy legislation. Looking at the federal dataset with the key elements of trust suggested by Theiss-Morse et al. (2015) and van der Meer (2017), I identified that the Twitter users had the 'knowledge' of the popular corporate business model that is centered around user information sharing and targeted advertising as well as a global corporation's (e.g., Google) cooperation with non-democratic countries like China known for its surveillance over citizens. The knowledge led to the people's 'expectations' that the corporations won't act in the public's best interest, as the industry would rather focus on their own profit-oriented motivations. As it became known to the public that the federal legislating authority did not invite any consumer advocates to data privacy hearings while a fundraising event was planned for Senate chair by industry, the individuals manifested distrust of not only corporations but also the government who appears to favor corporate 'interests.' As such, the political distrust around the federal data privacy hearings came down to concerns over a regulatory capture.

Political distrust at the California level

In the Twitter discourse around the CCPA, the political distrust was mainly of corporations, not the authority, however. Because the CCPA public forums were to solicit preferred details of the law from different stakeholders, the Twitter discourse was rather polarized between consumers and corporations, with few concerns over the California authority. While corporations were worried about the compliance costs possibly imposed by the CCPA, non-corporate Twitter accounts were focusing on the 'risks' involved in trusting the corporations, considering their data practices. The consumer advocates problematized the discriminatory use of data that excludes the marginalized from opportunities or targets dubious products to the vulnerable population (Madden et al., 2017), which gets aggravated without proper data privacy protections. Individuals also raised the impracticality of opt-out of all the platforms as a critical barrier to meaningful enforcement of the CCPA. Likewise, the political distrust at the California level was targeted at the corporations standing at the other end of the regulatory interests.

Political distrust further reinforced

The findings of political distrust at federal and California levels lend critical insights to the current gridlock of the US data privacy governance. First, the CCPA modifications unfolded between late 2019 and early 2020 are introducing increased distrust of the California authority. Even though the CCPA officially went into effect on 1 January 2020, it went through several modifications in October 2019, February, March, and June 2020 until its actual enforcement start date of 1 July 2020. Yet the modification processes of the CCPA appeared to largely reflect corporate suggestions while bills supported by consumer privacy advocacy groups weren't even allowed a single hearing[5] (Chen, 2020; Diaz, 2020). The public distrust of corporations abounds as a coalition of about 60 businesses asked the California Attorney General (AG) to delay the enforcement date further until 2 January 2021, mentioning the COVID-19 pandemic and its economic ramifications (Klein, 2020). This was eventually not accepted by the California AG, but consumer advocates said it was 'a cynical attempt by industry' to avoid the CCPA and that the industry 'shouldn't exploit the health crisis to ignore consumer requests' (*Consumer Reports*, 2020).

The ongoing or reinforced political distrust at the state level has implications for the standoff at the federal level. Because the corporate interests to weaken or delay the CCPA appear obvious, consumer advocates remain hard to believe that the corporate call for a single federal law is aimed at coming up with a *strong* comprehensive law. Consumer advocates have steadily urged that a federal privacy law should 'allow states to enact stricter state laws' (Augustin, 2019). Currently, state preemption is being an 'endgame' issue with low consensus among stakeholders of any federal privacy bills (Kerry et al., 2020). The divergence is manifested in two most well-known federal privacy bills: the Consumer Online Privacy Rights Act (COPRA) introduced by Democratic Sen. Maria Cantwell, and the United States Consumer Data Privacy Act (USCDPA) introduced by Republican Sen. Roger Wicker. The Cantwell bill doesn't preempt state laws whereas the Wicker bill enacts preemption. Privacy advocates evaluated the Cantwell bill as more ideal than the Wicker bill (*Grading on a Curve: Privacy Legislation*, 2020).

As long as the public distrust of corporations and the government exists both at the federal level and at a state level, the agreement on 'state preemption' will be difficult and a comprehensive privacy law may be hard to develop in the US, even though all sides appear to want a national privacy law in principle. The reasons fueling the political distrust identified in this study (e.g., the authority's close relationship with industry lobbying and its lack of invitation of civic members, corporations that prioritize profits, work with authoritarian regimes, generate discriminatory impacts, and do not provide consumers with practical privacy solutions) are hampering a meaningful consideration of and response to the public's concerns over privacy. Political distrust itself is in fact not always bad as the citizenry's 'healthy skepticism of government' and 'willingness … to suspend trust' can rein in the institutional power (Mishler & Rose, 1997, p. 419). The political distrust in legislating privacy protections this study examined, thus, indicates *prerequisites* for any future privacy laws to be effective and secure privacy of the US public.

As long as the root causes of the political distrust prevail, however, establishing a federal privacy law would remain far from possible, and the absence of a comprehensive law can leave individuals with limited individual privacy strategies. This is problematic when safeguarding privacy is pivotal to a democratic system. Regan (1995) claimed that privacy can 'check the arbitrary use of power' and allows 'room for individuality necessary to constitute a publi' (p. 234). Basically, privacy is considered necessary for informed deliberation of public matters and participation in a democratic public sphere (Cohen, 2013). The value of individual 'autonomy' is in jeopardy if 'continuous automated corporate surveillance of individuals' gets normalized, risking the provision of 'the secure starting point of arguments for the value of democracy' (Couldry, 2017, pp. 186–187). As such, the current lack of a federal privacy law illustrates the democratic values at risk and the democratic process in doubt. And understanding the public distrust of institutions is a key to possibly tackling this multifaceted problem.

Conclusion

This study contributes to understanding the complicated dynamics of emerging data privacy regulations and ingrained political distrust. Even though this research has a few limitations such as covering only the period from September 2018 to March 2019 and using sampled Twitter datasets (Morstatter et al., 2013), its findings reflect the individuals' negotiation of relationships with public and private institutions as to data privacy and its legislation. The Twitter discourse implies that emerging regulatory efforts on data privacy may not be as effective as expected unless the trust in institutions is regained in the US This study suggests that there needs to be more active means to build political trust in order to develop a comprehensive privacy law and make sure that any regulations over data privacy can meaningfully provide individuals with enforceable rights to control their personal data.

Notes

1. The hearing was mainly about anti-trust yet it also encompassed privacy issues and data practices of the giant tech companies (Renieris, 2020).
2. Bot detection was conducted as follows. First, top 10 Twitter handles who propagated most tweets of the top 10 exact duplicates were identified (in total, 100 Twitter handles for each dataset). Then, I ran Botometer for the Twitter handles and detected the ones whose score ranked over 2.5 out of 5 (Badawy et al., 2018). I manually checked the timelines of the Twitter accounts with over 2.5 Botometer score, following the method used by Ferrara (2017).
3. Note: A tweet can be coded for more than one theme, and the percentages shown in Figure 2 don't necessarily add up to 100%.
4. All the examplar tweets introduced in the result section were paraphrased to protect the privacy of the Twitter users, unless the tweets are headlines of external sources or from highly public figures such as verified accounts.
5. These bills include AB1760 (Privacy for All bill) and AB3119 (which urged to regulate sharing of data beyond sales of data), both introduced by Assemblywoman Buffy Wicks and supported by privacy and civil rights groups.

Acknowledgements

I would like to thank Dr. Margaret McLaughlin, Dr. Nathaniel (Ming) Curran, Andrea Alarcon, as well as two anonymous reviewers, for their helpful feedback on the earlier versions of this manuscript.

Disclosure statement

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

Notes on contributor

Jeeyun (Sophia) Baik is a doctoral candidate at the Annenberg School for Communication and Journalism at the University of Southern California, and her research focuses on the issues of data privacy and networked surveillance. [email: jeeyunba@usc.edu].

ORCID

Jeeyun (Sophia) Baik http://orcid.org/0000-0001-5057-1432

References

Consumer Reports calls on California Attorney General to uphold CCPA enforcement despite industry efforts to push back during the COVID-19 crisis. (2020, March 23). Consumer Reports.

Grading on a Curve: Privacy Legislation (p. 37). (2020). EPIC.

Allan, D. (2018, October 23). California's new data privacy law could begin a regulatory disaster. *Fortune*. http://fortune.com/2018/10/23/california-data-privacy-law-gdpr/

Almond, G. A., & Verba, S. (2015). *The civic culture: Political attitudes and democracy in five nations*. Princeton University Press.

Augustin, S. (2019, April 19). Civil rights, civil liberties, and consumer groups urge congress to protect marginalized communities from discriminatory privacy abuses. *Lawyers' Committee for Civil Rights Under Law*. https://lawyerscommittee.org/civil-rights-civil-liberties-and-consumer-groups-urge-congress-to-protect-marginalized-communities-from-discriminatory-privacy-abuses/

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Badawy, A., Ferrara, E., & Lerman, K. (2018). *Analyzing the digital traces of political manipulation: The 2016 Russian interference Twitter campaign*. 258–265.

Baik, J. (2020). Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA). *Telematics and Informatics*, *52*. https://doi.org/10.1016/j.tele.2020.101431

Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management. *New Media & Society*, *19*(4), 579–596. https://doi.org/10.1177/1461444815614001

Bennett, C. J. (2008). *The privacy advocates: Resisting the spread of surveillance*. MIT Press.

Boulianne, S. (2019). Building faith in democracy: Deliberative events, political trust and efficacy. *Political Studies*, *67*(1), 4–30. https://doi.org/10.1177/0032321718761466

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Chen, C. (2020, May 11). Does California's privacy and consumer protection committee actually care about privacy? *Private Internet Access*. https://www.privateinternetaccess.com/blog/does-californias-privacy-and-consumer-protection-committee-actually-care-about-privacy/

Cheney-Lippold, J. (2018). *We are data: Algorithms and the making of our digital selves*. NYU Press.

Citrin, J., & Muste, C. (1999). Trust in government. In J. P. Robinson, P. R. Shaver, & L. S. Wrightman (Eds.), *Measures of political attitudes; measures of social psychological attitudes* (Vol. 2, pp. 465–532). Academic Press.

Cohen, J. E. (2013). What privacy is for. *Harvard Law Review*, *126*(7), 1904–1933.

Conger, K. (2018, November 1). Ex-Google employee urges lawmakers to take on company. *The New York Times*. https://www.nytimes.com/2018/09/26/technology/google-privacy-china-congress.html

Coudert, F. (2014). Accountable surveillance practices: Is the EU moving in the right direction? In B. Preneel & D. Ikonomou (Eds.), *Privacy technologies and policy* (pp. 70–85). Springer International Publishing.

Couldry, N. (2017). Surveillance-democracy. *Journal of Information Technology & Politics*, *14*(*2*), 182–188. http://dx.doi.org/10.1080/19331681.2017.1309310

Dal Bó, E. (2006). Regulatory capture: A review. *Oxford Review of Economic Policy*, *22*(2), 203–225. https://doi.org/10.1093/oxrep/grj013

Diaz, J. (2020, May 11). State lawmakers value corporate money over consumer privacy. *San Francisco Chronicle*. https://www.governing.com/security/State-Lawmakers-Value-Corporate-Money-Over-Consumer-Privacy.html

Diaz, C., & Tene, O., & Gurses, S. (2013). Hero or villain: The data controller in privacy law and technologies. *Ohio St. LJ*, *74*(6), 923.

Drezner, D. W. (2004). The global governance of the internet: Bringing the state back in. *Political Science Quarterly*, *119*(3), 477–498. https://doi.org/10.2307/20202392

Falcon, E., & McKinney, I. (2018, September 14). The game is rigged: Congress invites no consumer privacy advocates to its consumer privacy hearing. *Electronic Frontier Foundation*.

Fernback, J., & Papacharissi, Z. (2007). Online privacy as legal safeguard: The relationship among consumer, online portal, and privacy policies. *New Media & Society*, *9*(5), 715–734. https://doi.org/10.1177/1461444807080336

Ferrara, E. (2017). *Disinformation and social bot operations in the run up to the 2017 French presidential election.*

Geiger, A. (2018). *How Americans have viewed surveillance and privacy since Snowden leaks* (Fact Tank). Pew Research Center.

Hallinan, D., Friedewald, M., & McCarthy, P. (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer Law & Security Review*, *28*(*3*), 263–272. http://dx.doi.org/10.1016/j.clsr.2012.03.005

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2017). Digital citizenship and surveillance society: Introduction. *International Journal of Communication*, *11*, 731–739.

Jardin, X. (2018, September 26). Google, Amazon, Twitter, other Big Tech to Congress: New California data privacy rules too tough. *Boing Boing*. https://boingboing.net/2018/09/26/google-amazon-twitter-other.html

Kerry, C., Morris, J. B., Chin, C. T., & Lee, N. E. T. (2020). *Bridging the gaps: A path forward to federal privacy legislation*. Brookings. https://www.brookings.edu/research/bridging-the-gaps-a-path-forward-to-federal-privacy-legislation/

Klein, D. O. (2020, April 17). *CCPA enforcement date remains July 1, 2020*. https://www.mondaq.com/unitedstates/data-protection/919528/ccpa-enforcement-date-remains-july-1-2020

Knight Commission on Trust, Media and Democracy. (2019). *Crisis in democracy: Renewing trust in America*. The Aspen Institute.

Lieber, D. (2019, January 11). Texas should copy California: Pass a new internet privacy law like the Golden State's. *Dallas News*. https://www.dallasnews.com/news/watchdog/2019/01/11/texas-copy-california-pass-new-internet-privacy-law-like-golden-states

Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). *Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans*. *95*, 74.

Marres, N. (2015). *Material Participation: Technology, the Environment and Everyday Publics*. Palgrave Macmillan.

Marwick, A., & Hargittai, E. (2019). Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society*, *22*(12), 1697–1713. https://doi.org/10.1080/1369118X.2018.1450432

McKelvey, K., DiGrazia, J., & Rojas, F. (2014). Twitter publics: How online political communities signaled electoral outcomes in the 2010 US house election. *Information, Communication & Society*, *17*(*4*), 436–450. http://dx.doi.org/10.1080/1369118X.2014.892149

Middleton, C. (2018, August 29). GDPR USA: Why tech industry now lobbying against consumer privacy. *Internet of Business*.

Minkkinen, M. (2019). Making the future by using the future: A study on influencing privacy protection rules through anticipatory storylines. *New Media & Society*, *21*(4), 984–1005. https://doi.org/10.1177/1461444818817519

Mishler, W., & Rose, R. (1997). Trust, distrust and skepticism: Popular evaluations of civil and political institutions in post-communist societies. *The Journal of Politics*, *59*(2), 418–451. https://doi.org/10.2307/2998171

Morstatter, F., Pfeffer, J., Liu, H., & Carley, K. M. (2013, June 28). Is the sample good enough? Comparing data from Twitter's streaming API with Twitter's firehose. *Seventh international AAAI conference on weblogs and social media*. Seventh International AAAI Conference on Weblogs and Social Media.

Neidig, H. (2019, February 22). Telecom industry to throw fundraiser for Senate chair the night before data privacy hearing. *TheHill*. https://thehill.com/policy/technology/431123-telecom-industry-to-throw-fundraiser-for-senate-chair-the-night-before-data

Papacharissi, Z. (2010). Privacy as a luxury commodity. *First Monday*, *15*(8). https://doi.org/10.5210/fm.v15i8.3075

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, *15*(1). https://doi.org/10.5210/fm.v15i1.2775

Regan, P. M. (1995). *Legislating privacy: Technology, social values, and public policy*. Univ of North Carolina Press.

Reidenberg, J. R. (2000). Resolving conflicting international data privacy rules in cyberspace. *Stanford Law Review*, *52*(5), 1315–1372. https://doi.org/10.2307/1229516

Renieris, E. M. (2020, August 6). Tech Execs wield privacy as a shield and a sword in congressional hearing. *Medium*. https://medium.com/berkman-klein-center/tech-execs-wield-privacy-as-a-shield-and-a-sword-in-congressional-hearing-a08a40b420c8

Sarikakis, K., & Winter, L. (2017). Social media users' legal consciousness about privacy. *Social Media + Society*. https://doi.org/10.1177/2056305117695325

Theiss-Morse, E., Barton, D.-G., & Wagner, M. W. (2015). Political trust in polarized times. In B. H. Bornstein & A. J. Tomkins (Eds.), *Motivating cooperation and compliance with authority* (pp. 167–190). Springer.

van der Meer, T. W. G.. (2017). Political Trust and the "Crisis of Democracy". *Oxford Research Encyclopedia of Politics*. https://doi.org/10.1093/acrefore/9780190228637.013.77

Waldman, A. E. (2018). *Privacy as trust: Information privacy for an information age*. Cambridge University Press.

West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society*, *58*(1), 20–41. https://doi.org/10.1177/0007650317718185

Westin, A. F. (1966). Science, privacy, and freedom: Issues and proposals for the 1970's. Part I--The current impact of surveillance on privacy. *Columbia Law Review*, *66*(6), 1003–1050. https://doi.org/10.2307/1120997

Wheatley, D., & Vatnoey, E. (2020). 'It's Twitter, a bear pit, not a debating society': A qualitative analysis of contrasting attitudes towards social media blocklists. *New Media & Society*, *22*(1), 5–25. https://doi.org/10.1177/1461444819858278

Yeh, C.-L. (2018). Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers. *Telecommunications Policy*, *42*(4), 282–292. https://doi.org/10.1016/j.telpol.2017.12.001

Youm, K. H., & Park, A. (2016). The "right to be forgotten" in European Union law: Data protection balanced with free speech? *Journalism & Mass Communication Quarterly*, *93*(2), 273–295. https://doi.org/10.1177/1077699016628824

Appendix A

	Federal public hearings		
Events	26 September 2018	27 February 2019	CCPA public forums
Date of Tweets	From 25 September to 27 September 2018.	From 25 February to 2 March 2019	From 1 January to 12 March 2019
Keywords	'John Thune' OR 'consumer privacy' OR privacy hearing OR google privacy OR apple privacy OR Twitter privacy OR amazon privacy OR 'data privacy' OR 'senate commerce hearing' OR 'senate commerce committee' OR #consumerprivacy OR #dataprivacy OR #consumerdata	'Senate Commerce, Science and Transportation Committee' OR 'consumer privacy' OR privacy hearing OR 'federal data privacy' OR federal data privacy OR google privacy OR apple privacy OR Twitter privacy OR amazon privacy OR facebook privacy OR 'data privacy' OR senate commerce hearing OR 'senate commerce committee' OR #consumerprivacy OR #dataprivacy OR #consumerdata OR privacy law OR federal privacy law OR US privacy law OR consumer privacy OR 'House Energy & Commerce Committee' OR E&C committee	'GDPR' OR 'General Data Protection Regulation' OR 'consumer privacy' OR 'data privacy' OR 'California Consumer Privacy Act' OR 'CCPA' OR #consumerprivacy OR #dataprivacy OR #consumerdata OR #CCPA OR #GDPR ↓ narrowed down with 'California' OR 'CCPA'