Privacy by debate:
A content analysis of post Cambridge Analytica congressional hearings

Dmitry Epstein and Rotem Medzini
The Hebrew University of Jerusalem

To be presented at GigaNet Annual Symposium
December, 2021

DRAFT – DO NOT CIRCULATE

Ever since data were pronounced as the new oil, questions of digital privacy became equivalent to those of climate change - the paramount, long-term importance of what is at stake, clashes with the seeming insignificance and intangibility of consequences of small, mundane actions. In their search after this "Cheshire cat of values" (Franzen, 2003, p. 42), researchers call for a multidimensional and contextual view of privacy as an object of study (Wu et al., 2019). On the one hand, such calls have advanced both conceptual and empirical understanding of how citizens think about privacy and enact privacy-related behaviors in networked environments (e.g. Bazarova & Masur, 2020; Bräunlich et al., 2020; Masur, 2018). On the other hand, scandals such as Cambridge Analytica (CA) reveal a gap in perceptions of privacy held by the users vs. those in positions of power, who design and regulate information networks. The 2018 revelations by the Guardian and The New York Times, followed by the outcry by civil activists and political actors, regarding the misuse of millions of Facebook users' data, resulted in parliamentary action. Politicians, sometimes repeatedly, sometimes unsuccessfully, invited the heads of Facebook, technological elites, to stand in front of congressional hearings and parliamentary investigations. In particular, the US Congressional hearings following the CA scandal offers a moment of explicit deliberation of privacy among policy and technological elites.

Even though CA has resulted in systemic effects for privacy and perhaps democracy, studies of privacy perceptions of elites remain scarce (e.g. Ribak, 2019). This is unfortunate as privacy perceptions of powerful elites can signal their plans to legislate or regulate the self-regulatory information processing practices of corporations and entire industries. Such

statements regarding privacy can remain theoretical on whether the threat for regulation will actually materialize. Elites' perceptions toward privacy can similarly educate on how their statements influence what scholars have termed "self-regulation in shadow of hierarchy," meaning the delegation of responsibilities from policymakers to private actors to formulate and impose regulations coupled with the continuous threat by policymakers for the private actors to comply (Héritier & Eckert, 2008; Medzini, forthcoming). Filling this theoretical gap, the current project offers an empirical insight into how policy and technological elites frame information privacy and how that framing may differ across elite stakeholder groups, such as commercial or government entities.

Literature Review

In this project, we build on two main bodies of literature. First, we survey privacy research to present the complexity and dynamic fluidity of privacy as a concept, which poses a challenge to both researchers and practitioners. Second, we survey literature on framing and public policy, as we discuss privacy as a rhetorical vessel carrying political meanings with practical repercussions. We leverage those two bodies of literature to base our research questions. Additionally, we touch on the scarce literature that did tackle specifically the challenge of privacy framing to explain the contribution of the current project to existing, specialized literature.

Privacy

Solove's (2006) reference to privacy as "a concept in disarray" seems to retain its currency to this day. Privacy remains an idea that is difficult to describe, it takes on a variety of functions within social order, and is both enacted and operationalized in research in a variety of ways. In this section we review those challenges, later linking them to framing as a mechanism linking this conceptual fluidity to policymaking as a field of discursive struggle. First, there is the challenge of describing what privacy is. Originally coined as the right to be let alone (Warren & Brandeis, 1890), in modern times, privacy has been increasingly perceived as a commodity that can be exchanged for digital services (Acquisti et al., 2015). Privacy can be viewed as a desire or a sense of control individuals have over when, how, and to what extent their personal information will be communicated to others (Westin, 1967), but it can also be viewed as a state of limited access to the self or to personal information (Smith et al., 2011). To add complexity, privacy can also be considered as a dialectic process between ideal and achieved states of interaction that include both desired and undesired levels of information sharing (Altman, 1975).

Second, adding to the conceptualization challenges, privacy can have different social roles. Privacy can be about the protection of one's personality, individuality, and dignity, yet it can also be about secrecy and concealment of information (Posner, 1981). Privacy can further be understood as an essential part of intimacy as it enables the formation of differential levels of self-revelation aimed at establishing and maintaining human relationships (Solove, 2006, p. 34). Finally, there is also the challenge of how privacy is enacted in social and technical systems. In public policy terms, privacy is often treated as "the group of policies designed to regulate the collection, storage, use, and transmittal of personal information" (Bennett, 1992, p. 13), thus focusing on what Europeans term as data protection. This policy-oriented understanding of privacy sometimes is too broad to the practice of "privacy on the ground" (Bamberger & Mulligan, 2015). For instance, engineers who design digital products often treat privacy through the lens of cybersecurity speaking of a privacy-by-design approach (Hadar et al., 2018; Ribak, 2019).

The richness and complexity in the perception and enactment of privacy have led scholars to think about privacy as a multidimensional, contextual, and political concept. The multidimensional approach treats individual privacy as harboring different dynamics of power asymmetries, hierarchies, and social stratification (Park, 2018; Wu et al., 2020). This approach pushes against a uniform treatment of privacy, both conceptually and empirically, pointing towards dynamics such as the privacy paradox and calling for acknowledgement that the way privacy is through about and enacted differ, depending on one's socioeconomic status and cultural identity (Marwick & boyd, 2018; Pearce et al., 2020). Second, in terms of contextuality, some scholars suggest that individuals' expectations and behaviors regarding privacy are guided by contextual integrity - perceived conformity of information flows to a set of norms typical to a particular context (e.g. medical visit vs. a job interview; Nissenbaum, 2010). Other scholars suggest that the ubiquitous use of digital social media and acceptance of personal information as digital currency have resulted in a privacy context collapse under which boundaries between imagined audiences and distinct contexts become blurry or altogether disappear (Marwick & boyd, 2011; Vitak, 2012). Finally, privacy is also political. From individual actors' perspective, they need privacy to control the exposure of their belief to and from others as a form of managing power relations (Park, 2018). From a more institutional perspective, political actors have been framing privacy in relation to such issues as security, freedom of expression, and human rights, as an attempt to set the agenda for decision makers and influence the prioritization of policy solutions (Epstein et al., 2014).

Taken together, the fuzziness of privacy as a social phenomenon and as a policy challenge, compound by complexity imposed by its multidimensionality, contextuality, and its political nature highlight the importance of understanding how stakeholder groups understand and enact privacy. A series of recent publications have called for investigating privacy in marginalized groups or more broadly, as it is argued that positions of relative (lack of) power substantively play into how privacy is perceived and enacted (Marwick & boyd, 2018; Epstein & Quinn, 2020). In this context technological and policy elites make a particularly intriguing group as privacy research tends to focus either on the mainstream or on the disempowered groups, taking both technological affordance and policy as given (Wu et al., 2020). But those are not given. Both technology and policy are developed by particularly powerful groups, thus embodying their worldviews, ideologies, and social practices (e.g. Friedman, 1997; Shilton, 2018). This project advances privacy research by interrogating how powerful margins think and talk about privacy, thus adding to literature that focuses on individual users' perspectives (Quinn et al., 2019).

Framing

Bacchi (2000) succinctly described policy as "meaning making" (p.46). With this idea in mind, privacy as a policy issue is a vessel used in a rhetorical struggle over resources, priorities, and political agenda (Fischer & Forester, 1993). One way to systematically unpack such discursive struggles is with the use of framing theory. Here, frames are "schemata of interpretation" (Goffman, 1974) that enable speakers to present a central organizing idea and make sense of relevant events (Gamson & Modigliani, 1989). Framing literature suggests a link between frames in communication and frames in thought, which allows leveraging analysis of discourse to gain understanding into the worldviews and heuristics employed by the speakers (Chong & Druckman, 2007b; Scheufele & Tewksbury, 2007). We use the link between frames in communications and frames in thoughts as a way to systematically unpack elite discourses as representing their perceptions of privacy (Druckman, 2001). Our focus is on frames in communication as reflective of systematic or macro level structures. Individuals use frames in communication when they engage in competitive behavior around establishing frames of reference, defining problems or mapping the realm of possible solutions. Arguably, we can leverage the analysis of frames in communication to draw inferences about frames in thought of the speakers, which reflect an individual's cognitive understanding of a given situation; what that individual considers the most salient aspect of an issue (Chong & Druckman, 2007a; Scheufele, 1999).

Within the broad area of framing research (see Amsalem & Zoizner, 2020; Scheufele & Tewksbury, 2007 for extensive reviews), we are particularly interested in the application of framing to problem definition in competitive environments .(e.g. Entman, 2004; Gamson & Modigliani, 1989; Rochefort & Cobb, 1994) including those dealing explicitly with the internet and related technologies (Osenga, 2013)**.** In this context individuals compete over ways to describe and define policy problems and in doing so, set priorities and resource allocation norms, delineate the space of possible solutions, place responsibility for causing the issue or take credit for resolving it (Barbehön et al., 2015; Genieys & Smyrl, 2008; Hoornbeek & Peters, 2017; Peters, 2005; Schon & Rein, 1995). Given the dynamic and evolving state of privacy as a policy issue, discursive battles over its definition are particularly important as they set to define both how we experience and study privacy moving forward.

Framing of privacy

Despite burgeoning empirical research of framing in policy discourse (e.g. Daviter, 2007; Eising et al., 2015; Koduah et al., 2016), framing studies of privacy remain relatively scarce. As is the case with media frame research, most projects seem to focus on the effects of framing on attitudes and behaviors in a rather instrumental fashion. This family of studies hosts primarily experimental research, often grounded in behavioral economics (e.g. Adjerid et al., 2019; Gluck et al., 2016; Rajivan & Camp, 2016). In doing so, scholars adopt an institutional take on privacy where individual's perceptions and behaviors relate to privacy relationships vis-a-vis institutions such as the government, commercial entities or platform providers. Additionally, research conducted in this vein brings in external conceptualizations of privacy (e.g. data protection) in order to design manipulations and test their effect (Wu et al., 2020). While fruitful and insightful, this research trajectory draws a partial picture of uses of privacy framing, as opposed to studying framing itself. As behaviors and attitudes of individuals tend to overlook institutional privacy relationships and focus on social privacy vis-a-vis their peers (Obar & Oeldorf-Hirsch, 2017; Quinn et al., 2019), it is increasingly important to consider privacy framing as an object of study in its own right.

A number of studies that examine privacy framing take a media-centric approach, focusing on frames in communication. Fornaciari (2014), for example, interrogated economic framing of privacy in New York Times editorials using critical discourse analysis. She points out a tendency to simplify privacy, focusing on the lack of control individuals have over the flow of their personal information, but at the same time placing the agency and the burden of privacy protection on the individuals themselves. In a later study, Fornaciari conducted a longitudinal

critical discourse analysis of privacy framing in the editorials of five major US newspapers showing how over the course of a century the framing of privacy shifted from normative to commercial, increasingly focusing on "the materialistic nature of personal information, often adopting on individualistic, interest-based approach to privacy through a focus on property, ownership, and control" (Fornaciari, 2018, p. 18). Other studies took a more privacy-issue-centric approach examining media framing of issues such as the right to be forgotten (Telesca, 2018). In a stark contrast to the inductive studies surveyed so far, Ashuri and Halperin employed a deductive approach demonstrating relative prominence of a variety of policy frames (e.g. conflict, morality) in privacy and self-disclosure coverage in Israeli newspapers in Hebrew.

A complementary thread in frame-focused research asks to understand privacy frames in thought. Some focus on users of digital technologies. Quinn et al. (2019), for example, conducted topic modeling and semantic network analysis of definitions of privacy among US social media users. Their findings highlight the relative dominance of horizontal (or social) privacy perceptions among social media users, as compared to institutional (or vertical) privacy. Minkkinen et al. (2017) analyzed metaphors collected through focus group discussions in Finland, Germany, and Israel to suggest two dominant themes of "individual control and trust in collective privacy protection" (p. 8). Similarly, Lapenta and Jørgensen (2015)in focus groups with Danish high school students identified control and concerns as major themes in their participants' attempt to manage their horizontal privacy relationships; at the same time they found little attention to vertical privacy relationships.

Finally, a few studies have focused on frames in thought amond technology designers or regulators. We reference the two groups together as "elites." Braman (2012) in her analysis of the Requests for Comments of the Internet Engineering Task Force demonstrates how internet pioneers imagined privacy threats to internet communication as stemming primarily from the governments and commercial players, how they framed privacy protection as an inherently technical issue, and designed internet protocols accordingly. Ribak (2019), one the other hand, in her interviews with developers identified a primarily security framing of privacy. With regards to policymakers, Mukherjee (2000), in her review of privacy framing in regulatory proceedings on caller ID regulation identified vertically-oriented frames capturing a tension between framing of privacy as control vs. access or a state. Similarly, Epstein et al (2014), in their analysis of the transcripts of the Internet Governance Forum described privacy framing by representatives of the governments as a tension between normative and security conceptualizations, while the civil society viewed it as a vulnerable state to be protected. Both frames referred to privacy

relationships between individuals and institutional actors. Similar dynamics were identified in privacy deliberations in the German parliament and in the EU around the adoption of passenger name records post 9/11 (Gein, 2018; Huijboom & Bodea, 2015).

The focus on elites is important. Unlike non-elites users, who have limited to no ability to make impact a structural change, elites are interesting subjects of policy research as they hold relative information power that they can utilize to influence or design privacy or technological policies (Braman, 2006). Policymakers, for example, can enhance the credibility of privacy policies by requiring that (European) organizations will appoint independent data protection officers, whose tasks are to guide and monitor self-regulatory decisions regarding privacy (Medzini, 2021b). Technology designers, similarly, can innovate in self-regulation by delegating responsibilities to different groups of actors and consequently redraw the boundaries between public and private interests (Medzini, 2021a). Hence, parliamentary and congressional hearings, where policymakers and technology designers directly interact on a particular policy issue offer an opportunity for researchers to study how elites frame privacy differently and which communicative and rhetorical strategies they use to direct attention to the policy issue of privacy and their assessment of possible solution vectors.

Current Study

Drawing on the literature described above, the current study asks two main questions. First, we ask how do elites frame privacy in policy-oriented discourse? Second, we ask whether there are differences in privacy framing across stakeholder groups within the elites? Particularly, we are interested in potential differences between commercial and government actors or along political affiliations. To answer those questions we focus on one of the pivotal events in policy deliberation of privacy in the US - the Senate hearing that followed the Cambridge Analytica scandal during the 2016 presidential election. This case is interesting, because it brings together, in a single deliberation, Facebook as a major technological power and US Senators as a major political power with clear ideological identities along the party lines. The two are the main groups of the relevant elites for the purposes of this study.

In our research, we adopt the deductive approach used by Ashuri and Halperin (2017) for the study of privacy framing. To operationalize the multidimensionality of privacy we leverage research that distinguishes between vertical and horizontal dimensions. Vertical privacy, sometimes also referred to as institutional privacy, addresses privacy relationships between an individual and an institution. Institutions can be either *public* institutions such as the government

or *private* institutions such as platform providers. Horizontal privacy, in turn, refers to privacy relationships between individuals and their peers (Bazarova & Masur, 2020)**.** Studies adopting this perspective suggest that lacking exogenous shocks information technology users - and especially users of social media platforms - prioritize horizontal thinking about privacy over institutional approaches to privacy (Afriat et al., 2021; Quinn et al., 2019).

In our analysis we further distinguish between primary and secondary privacy relationships (Bazarova & Masur, 2020). The earlier type of privacy relationships represents the *direct* recipients of the information that individuals disclose, such is the case with platform providers and intended users. Conversely, the latter represent *indirect or unintended* audiences, such as with other commercial actors, applications developers, governments, and extended communities (friends of friends).

Finally, given the context of the Cambridge Analytica hearing, we adopt the responsibility attribution and conflict frames as those are described in Ashuri and Halperin (2017; originally Semetko & Valkenburg, 2000)**.** The conflict frame is used to emphasize conflicts around a given issue and therefore should always reference, either explicitly or implicitly, two or more individuals, groups, or institutions. Traditionally. responsibility frame attributes responsibility for the cause or a solution to a policy issue to a specific individual, public institution, or a group (Entman, 1993). Given the importance of the responsibility frame to the policy discourse about privacy for our analysis we separated attribution of responsibility for harms and responsibility for offering solutions or protections.

Case: Cambridge Analytica

The 2018 Cambridge Analytica revelations have shaken the policy and polity debates around privacy. A whistleblower by the name of Christopher Wylie has revealed a major data breach that impacted both the 2016 US presidential elections and the Brexit referendum. According to the revelations, a Cambridge University academic Alexsandr Kogan had collaborated with Cambridge Analytica, a right-winged-affiliated firm, to develop an app called thisisyourdigitallife, which included a personality test. The app collected data on hundreds of thousands of users who answered the test, but unknowingly also their Facebook's friends. The app was able to gather the data as Facebook's policies permitted at the time to collect friends' data to improve user experience, yet prohibited selling the data or using it for advertising. Facebook, who received notice of the unprecedented harvesting of personal information in 2015, did not alert users of the data breach. It also did not take sufficient steps to recover or secure the private information of tens of million individuals. Cambridge Analytica has used the

data to profile voters, in order to predict and influence voters with personalized political advertisements.

The Cambridge Analytica revelations had provoked widespread international outrage. For example, in the UK, the Information Commissioner's Office, the British supervisory data protection authority, and the Electoral Commission initiated an inquiry into the matter of Cambridge Analytica's impact in the UK. Representatives of Facebook and Cambridge Analytica appeared before the House of Commons's Digital, Culture, Media and Sport Committee. In the US, meanwhile, the revelations about the unprecedented data breach, and how the data was put to use, came only weeks after special counsel Robert Mueller indicted 13 Russians for interfering in the 2016 presidential elections. The two events led policymakers to demand that Mark Zuckerberg (Facebook CEO) would testify before Congress, and specifically, under the premise of a Congressional hearing.

Methods

This project is based on quantitative content analysis of the transcribed joint session of the Senate Commerce, Science, and Transportation Committee and Senate the Committee on the Judiciary, which took place on April 10, 2018. The hearing, titled "Facebook, Social Media Privacy, and the Use and Abuse of Data," involved 44 Senators questioning a single witness - Mark Zuckerberg - for over four hours. The total length of the transcript exceeds 45 thousand words. We develop and validate a dedicated coding scheme for the analysis of privacy discourses, and apply this scheme to systematically analyze 92 distinct interventions in the hearing. The analysis was performed by two coders with 47.8% of the segments coded by both coders and disagreements resolved by consensus.

Sample, Unitization, and Inclusion Criteria

Our choice of units of observation and coding units is guided by the rigid structure of the hearing. In this case, upon brief introductory remarks and the opening statements of the committee chairs, the ranking members, and the witness, each committee member received a five-minutes slot during which they could question the witness at will on any relevant policy issue. Those five-minutes Q&A segments comprise the bulk of the corpus. The hearing resumed with closing remarks by the chairs. For the purposes of our analysis, we treat each speaking segment (formal statements or Q&A) as a unit of observation. Since a typical five-minutes Q&A segment included an exchange between a committee member and Mark

Zuckerberg, we separate the discourses of the committee members and the witness treating each as a separate coding unit (n=92).[1]

Given the relative freedom committee members have in their questioning of the witness, each opening statement or Q&A segment could include multiple thoughts, some of which are related to privacy and others are not. For example, beside privacy, Q&A segments have been on policy issues such as election interference, content moderation, and competition and antitrust policy. Building on the work of Stromer-Galley (2007) we treat a thought as "an utterance (from a single sentence to multiple sentences) that expresses an idea" (p.9) on the problem of privacy. Such utterances can include talk (including expressions of opinion, agreement, disagreement, facts, and questions) or metatalk about privacy, which may directly challenge the framing (see Stromer-Galley, 2007, p. 22 for a detailed discussion). Thus, coding units included in the study had to contain substantive thoughts about privacy (see Appendix A), which we, as coders, would focus on in subsequent coding. When Q&A segments were entirely on policy issues that are not related to privacy, we coded them accordingly as lacking any privacy thoughts.

We used a subset of the corpus for training purposes and revision of the inclusion criteria. The final application of the inclusion criteria was reliable (agreement = 95.35%, Krippendorff's α = 0.87) resulting in a final corpus of 69 coding units. Among those 53.6% (n = 37) of the segments were produced by the Senators (split almost equally between the Republicans and the Democrats) and 46.3% (n = 32) by Mark Zuckerberg as a witness.

Coding Procedures and Variables

The coding scheme used in this study was developed through synthesis of literature on privacy and framing as applied to policy, and particularly privacy. The process of developing the coding scheme was also informed through inductive reading of the transcripts in the spring of 2020. Building on privacy literature, we operationalize a series of privacy attributes such as privacy orientation, proximity of privacy interactions (e.g., Bazarova & Masur, 2020; Quinn et al., 2019). Further, building on framing literature we focus on responsibility framing, as it pertains to both infringement and protection of privacy, as well as conflict frames. In this project, we follow the lead of Semetko and Valkenburg (2000) and Ashuri and Halperin (2017) in unpacking each frame or attribute into a number of indicators that are coded dichotomously as either present or

[1] Few interventions, however, have been made without an exchange, such as with opening statements and stand-alone clarifications or brief notes.

absent. This deductive approach has been demonstrated as both more reliable and more amenable for comparison, as it allows assessing prominence of a frame as an accumulation of coded attributes.

As with inclusion, we used a subset of the corpus for training purposes and revision of the coding scheme. Units used in this pilot stage were later re-coded with the final coding scheme (Neuendorf, 2002). During the final coding phase almost half of the coding units (n=34) were coded by both authors to establish intercoder reliability (additional eight segments were coded by both authors, but excluded from analysis due to lack of privacy thoughts). Intercoder reliability was calculated using ReCal (Freelon, 2010). All disagreements were resolved by consensus through deliberation. Given the relatively small size of the reliability sample we used a combination of Kripendroff's alpha and percentage agreement as the basis for our decisions (Lombard et al., 2002), and we excluded from our analysis codes with alpha scores below 0.7 and percent agreement lower than 0.9 (See Table 1 for the description of included codes).

Each variable used in the analysis is based on values of at least two reliable codes. The analysis that follows uses two types of composite variables. On the one hand we created count variables that capture presence or absence of a particular framing condition in an intervention. Any intervention that had at least one positive code, would be counted as having that framing condition present. On the other hand, we ask to assess the relative strength of the frame used. We achieve that by aggregating the values of the codes comprising a framing condition. We consider a frame to be stronger if it has more indicators that comprise being coded as present.

Privacy Orientation and Proximity. In this project we operationalize the distinction between vertical and horizontal orientations of privacy, as well as proximity of privacy interactions vis-a-vis an individual actor. The former is drawing on the conceptual (Bazarova & Masur, 2020) and empirical survey work (Epstein & Quinn, 2020) asking to distinguish the orientation of privacy protecting attitudes and behaviors. The latter draws on the work that recognizes the complexity of online data flows and suggests that the distance of privacy-related activity from an individual actor both constrains control and may affect understanding actors have about their personal information flows (Baruh & Popescu, 2017; Bazarova & Masur, 2020; Masur, 2020).

Table 1: Codes and intercoder realibaility

Construct	Code	Example	percent agreement	Krippen-dorff's α
Vertical privacy, primary	[POVP3] In relation to privacy, does the intervention mention or imply **commercial or contractual relationships** between users and the platform provider?	GRASSLEY: It's not the first time that Facebook has mishandled its users' information. The FTC found that Facebook's privacy policies had deceived users in the past.	.86	.72
	[POVP5] In relation to privacy, does the intervention mention or imply **users' expectations** of platform provider behavior?	ZUCKERBERG: Senator, I think Facebook is safe. I use it, my family uses it, and all the people I love and care about use it all the time. These controls are not just to make people feel safe; it's actually what people want in the product. BOOKER: But there are a lot of communities of color worried that that data can be used to surveil groups like Black Lives Matter, like folks who are trying to organize against substantive issues of discrimination in this country.	.91	.78
	[POVP6] In relation to privacy, does the intervention mention or imply **platform provider's expectations** of its users' behavior?	ZUCKERBERG: Senator, I think that that's the right principle. And a hundred billion times a day in our services, when people go to share content, they choose who they want to share it with affirmatively. YOUNG: I would encourage you to, you know, survey that, get all the information you can with respect to that, and make sure that — make sure that user agreement is easy to understand and streamlined and so forth.	.95	.88

Construct	Code	Example	percent agreement	Krippen-dorff's α
Vertical privacy, secondary	[POVS1] In relation to privacy, does the intervention mention or imply **third institutional parties as major/dominant subjects** of the intervention?	ZUCKERBERG: Senator, you are referring I think to our developer platform, and it may be useful for me to give some background on how we set that up, if that's useful.	.95	.91
	[POVS2] In relation to privacy, does the intervention mention or imply **information flows between the platform provider and third party actors**?	FEINSTEIN: It appears the information collected included everything these individuals had on their Facebook pages and, according to some reports, even included private direct messages between users. HATCH: Some have professed themselves shocked — shocked that companies like Facebook and Google share user data with advertisers.	.95	.91
	[POVS3] In relation to privacy, does the intervention mention or imply **commercial** or **contractual relationships** between the platform provider and third party actors?	ZUCKERBERG: But, overall, the way we've enforced our platform policies in the past is we have looked at patterns of how apps have used our APIs and accessed information, as well as looked into reports that people have made to us about apps that might be doing sketchy things. HARRIS: Whether you knew whether Kogan's terms of service and whether you knew if that Kogan could sell or transfer data.	.91	.76
	[POVS4] In relation to privacy, does the intervention mention or imply a **power relationship** between the platform provider and third party actors?	ZUCKERBERG: Senator, we have kicked-off an investigation of every app that had access to a large amount of people's data before we locked down the platform in 2014 LEE: Do you have the technological means available, at your disposal, to make sure that that doesn't happen and to — to protect, say, an app developer from transferring Facebook data to a third party?	.95	.90

Construct	Code	Example	percent agreement	Krippen-dorff's α
Horizontal privacy, primary	[POHP1] In relation to privacy, does the intervention mention or imply users and their direct peers as major/dominant actors?	ZUCKERBERG That's why, every single time you go to share something on Facebook, whether it's a photo in Facebook, or a message — in Messenger or What's App, every single time, there's a control right there about who you're going to be sharing it with — whether it's your friends or public or a specific group — and you can — you can change that and control that in line.	.93	.73
	[POHP4] In relation to privacy, does the intervention mention or imply a **power relationship** between individuals and their immediate social circles?	ZUCKERBERG: if we could put those tools in people's hands, then that would empower people to do good things. FISCHER: And you wrote a Facebook post at the time on a public page on the Internet that it used to seem scary to people, but as long as they could make the page private, they felt safe sharing with their friends online; control was key.	.93	.37
Horizontal privacy, secondary	[POHS1] In relation to privacy, does the intervention mention or imply **individuals' extended social circles** as major/dominant actors?	ZUCKERBERG: whether it's your friends or public or a specific group — and you can — you can change that and control that in line.	.98	.66
	[POHS2] In relation to privacy, does the intervention mention or imply **information flows among members of the extended social circles** of a user?	ZUCKERBERG: Yes. And I think you raise a good point though, which is that it is — we will delete it from our systems but if you shared something to someone else then we can't guarantee that they don't have it somewhere else.	1.00	1.00

Construct	Code	Example	percent agreement	Krippen-dorff's α
Responsibility attribution - Infringement	[RAI1] In relation to privacy, does the intervention suggest that **an individual (or a group of people) *have the ability*** to inflict privacy harm/infringement?	WHITEHOUSE: On the subject of bans, I just wanted to explore a little bit what these bans mean. Obviously Facebook has been done considerable reputational damage by it's association with Aleksandr Kogan and with Cambridge Analytica, which is one of the reasons you're having this enjoyable afternoon with us. Your testimony says that Aleksandr Kogan's app has been banned. Has he also been banned? ZUCKERBERG: Yes, my understanding is he has. WHITEHOUSE: So if he were to open up another account under a name and you were able to find out that would be taken — that would be closed down? ZUCKERBERG: Senator, I believe we — we are preventing him from building any more apps. WHITEHOUSE: Does he have a Facebook account still? ZUCKERBERG: Senator, I believe the answer to that is no, but I can follow up with you afterwards.	1.00	1.00
	[RAI2] In relation to privacy, does the intervention suggest that the state (or the government), **platform provider or in/formal third party *has the ability*** to inflict privacy harm/infringement?	JOHNSON: But application developers do? Now, is that only through their own service agreement with their customers, or do they actually access data as they're developing applications?	.98	.95
	[RAI4] In relation to privacy, does the intervention suggest that the state (or the government), **platform provider or in/formal third party *are responsible***, even if partially, for the privacy harm/infringement?	THUNE: The recent revelation that malicious actors were able to utilize Facebook's default privacy settings to match email addresses and phone numbers found on the so-called Dark Web to public Facebook profiles potentially affecting all Facebook users only adds fuel to the fire.	.93	.86

Construct	Code	Example	percent agreement	Krippen-dorff's α
Responsibility attribution - protection	[RAP2] In relation to privacy, does the intervention suggest that the **state (or the government), platform provider or in/formal third party** *have the ability* to offer solutions against (or protection from) privacy harm/infringement?	TESTER: So you've been at this nearly five hours today. So besides taking reactive steps — and I want you to be as concise as you possibly can — what are you doing to make sure what Cambridge Analytica did, never happens again? ZUCKERBERG: Thank you, senator. There are three important steps that we're taking here. For Cambridge Analytica, first of all, we need to finish resolving this by doing a full audit of their systems to make sure that they delete all the data that they have and so we can fully understand what happened. There are two sets of steps that we're taking to make sure that this doesn't happen again. The most important is restricting the amount of accessed information that developers will have going forward. The good news here is that back in 2014, we actually had already made a large change to restrict access on the platform that would have prevented this issue with Cambridge Analytica from happening again today. Clearly we did not do that soon enough. If we'd done it a couple of years earlier, then we probably wouldn't be sitting here today. But this isn't a change that we had to take now in 2018, it's largely a change that we made back in 2014.	.86	.70

Construct	Code	Example	percent agreement	Krippen-dorff's α
Responsibility attribution - protection	[RAP4] In relation to privacy, does the intervention suggest that the **state (or the government), platform provider or in/formal third part**y *are responsible* for providing a solution against or protection from privacy harm/infringement?	HASSAN: Okay, but — and I understand the point that you're trying to make here, but here's what I'm concerned about. We have heard this point from you over the last decade-plus. Since you've founded Facebook — and I understand it — you've — you founded it pretty much as a solo entrepreneur with your roommate. But now, you know, you're sitting here at the head of a bazillion dollar company, and we've heard you apologize numerous times and promise to change, but here we are again, right? So I really firmly believe in free enterprise, but when private companies are unwilling or unable to do what's necessary, public officials have, historically, in every industry, stepped up to protect our constituents and consumers. You've supported targeted regulations, such as the Honest Ads Act, and that's an important step for election integrity, I'm proud to be a co-sponsor of that bill. But we need to address other, broader issues as well. And today you've said you'd be open to some regulation, but this has been a pretty general conversation. So will you commit to working with Congress to develop ways of protecting constituent privacy and well-being, even if it means that that results in some laws that will require you to adjust your business model? ZUCKERBERG: Senator, yes. We will commit to that. I think that that's an important conversation to have. Our position is not that regulation is bad. I think the Internet is so important in people's lives, and it's getting more important. HASSAN: Yes.	.95	.90

The main distinction we are asking to establish in the coding scheme is between the actors involved and the direction of information flows. The vertical orientation codes focused on the individual and institutional actors as the main agents referred to in the hearing intervention, while the horizontal orientation codes focused on individuals and their social networks. Related to that we coded for mentions of information flows, norms or behavioral expectation, contractual or social relationships. Concurrently, primary privacy codes focused on interactions between individual actors and the platform provider or their immediate social circles, while the secondary codes refer to privacy-related activities by institutional third parties (both government and commercial) and the extended social circles of the actors.

Hence, we define the following composite measures based on the reliability criteria described above. *Vertical primary privacy* is composed of three codes referring to commercial or contractual relationships between users and the platform provider, users' expectations of platform provider behavior, and platform provider's expectations of user behavior - all in the content of privacy. The count composite measure captured the presence of any of the indicators (N = 54), while the strength composite measure was an average of the three (M = .449, SD = .307) *Vertical secondary privacy* consists of four codes capturing references to institutional third parties as major actors, as well as information flows, commercial or contractual relationships, and power relationships between the platform providers and third parties. The count composite measure captured the presence of any of the indicators (N = 54), while the strength composite measure was an average of the four (M = .562, SD = .380). *Horizontal primary privacy* consists of two codes addressing references to users and their direct peers as major or dominant actors as well as power relationships between them. The count composite measure captured the presence of any of the indicators (N = 17), while the strength composite measure was an average of the two (M = .167, SD = .317). Finally, *horizontal secondary privacy* is composed of two codes capturing references to the extended social circles of an individual as the major actors as well as information flows between said extended social circles and individual actors. The count composite measure captured the presence of any of the indicators (N = 5), while the strength composite measure was an average of the two (M = .058, SD = .219).

We opted for averages in this battery of variables as the goal here is to capture the relative prominence of each frame, under the constraint of each variable being composed of a different number of components; given the dichotomous coding of individual indicators, the composite measures range between zero and one. Moreover, it is important to note, that given

the unique context of the hearing, our dataset has low rates of occurrences of reference to both primary and secondary horizontal privacy, which limits the analysis that follows. At the same time in addition to examining each one of the intersections of proximity and directionality, our variables allow aggregate examination of each one of the contracts separately.

Responsibility and conflict. Prior research on both policy and privacy framing has delved into questions of responsibility attribution and conflict (Ashuri & Halperin, 2017; Semetko and Valkenbur, 2000). Both aspects are important in unpacking policy discourse about an issue as those are critical factors in devising solutions. In this study, we adopt the conflict framing coding developed by Semetko and Valkenbur (2000). Based on reliability criteria outlined above, our measure of *conflict* captures references to two or more sides to a problem or to winners or losers. The count composite measure captured the presence of any of the indicators (N = 61), while the strength composite measure was an average of the two (M = .601, SD = .316).

Further, we adopt the established coding scheme for responsibility attribution to separate responsibilities for privacy infringement and privacy protection. Thus, based on reliability criteria outlined above we operationalize *responsibility attribution - infringement* as consisting of three codes capturing references to the ability of individuals and institutions to infringe one's privacy, as well as a direct assignment of responsibility for such infringement to institutions. The count composite measure captured the presence of any of the indicators (N = 57), while the strength composite measure was an average of the three (M = .502, SD = .272). Conversely, we operationalize *responsibility attribution - protection* as a composite measure capturing the ability and responsibility of institutional actors to protect privacy. The count composite measure captured the presence of any of the indicators (N = 65), while the strength composite measure was an average of the three (M = .862, SD = .283).

Meta Data. In addition to coding for privacy framing characteristics, we collected meta-data about the speakers, differentiating (a) between Senators and Mark Zuckerberg, and (b) distinguishing between the Republican and the Democratic members of the committees partaking in the hearing. Those variables were captured in the transcript and did not require coding. Finally, even though our coding units included interventions that contained privacy thoughts, given that a single intervention could include thoughts on other topics (e.g. content moderation or election interference), we coded for the dominance of privacy as a topic in a given intervention. Here, we distinguished between three levels: main, major, and minor (Krippendorff's $\alpha = 0.91$).

Findings

Table 2 summarizes the frequencies and percentages of aggregated occurrences of privacy frames analyzed in this study. A frame was counted towards an aggregative occurrence if one of the frame indicators was coded as present. It is important to note here that those codes are not mutually exclusive, i.e. a single intervention could include reference to a number of privacy frames and indeed most of them employed multiple frames. Percentages were calculated out of the total number of interventions made by each one of the groups involved in the hearing: Facebook as represented by Mark Zuckerberg, Democratic and Republican Senators. Privacy was the main topic in 65% of the segments in the corpus; in about 26% of the segments it was a major topic discussed at par with another issues such as content moderation or foreign intervention in the US election; only about 9% of the coding units included minor privacy thoughts, while most of the segment was dedicated to a different topic.

Privacy orientation and proximity. When considering the dimensionality of privacy regardless of its proximity, the hearing was dominated by the use of vertical framing. There was a significant difference ($p < .001$) in references to dimensions of privacy with over 83% of all references treating them in vertical terms and slightly less than 17% treating them in horizontal terms. This observation is further corroborated when we consider the relative strength of vertical and horizontal privacy frames as captured by our composite measures. The overall strength of vertical framing ($M = 1.011$) was higher when compared to the overall strength of horizontal framing ($M = 0.225$), $W = 2109$, $p < .001$.

Table 2: Frame frequencies

	Facebook		Democrats		Republicans		Total	
	N	%	N	%	N	%	N	%
Privacy orientation and proximity								
Vertical primary	23	0.72	14	0.78	17	0.89	54	0.78
Vertical secondary	23	0.72	17	0.94	14	0.74	54	0.78
Horizontal primary	11	0.34	2	0.11	4	0.21	17	0.25
Horizontal secondary	4	0.13	1	0.06	0	0.00	5	0.07
Responsibility								
Infringement	21	0.66	18	1.00	18	0.95	57	0.83
Protection	29	0.91	18	1.00	18	0.95	65	0.94
Conflict	25	0.78	18	1.00	18	0.95	61	0.88
Dominance								
Minor	3	0.09	2	0.11	1	0.05	6	0.09
Major	10	0.31	4	0.22	4	0.21	18	0.26
Main	19	0.59	12	0.67	14	0.74	45	0.65

However, when comparing the use of vertical and horizontal framing by Mr. Zuckerberg and the senators, we find that the vertical framing is more common among the senators (57%) and horizontal framing is more common in Mr. Zuckerberg's discourse (68%) (*p = .035, Fisher's exact test*). The comparison of relative strength of horizontal framing across institutional settings further reinforces this dynamic. The mean strength of horizontal framing in Mr. Zuckerberg's interventions (M = 0.359) is higher compared to those of the senators (M = 0.108), U = 457, p = .036. The relationship is reversed for vertical privacy. Vertical privacy was stronger pronounced among the senators (M = 1.09), compared to the CEO of Facebook (M = 0.919), but this relationship was not statistically significant in our corpus. When parsing the frequency or strength of orientation framing across party lines, we also find no significant associations or differences.

When we considered aggregate proximity frames, regardless of privacy orientation, there were no significant associations in the frequencies of their use across institutional or party lines. With that, there is an overall slightly higher proportion of segments with references to primary (55%) as opposed to secondary privacy relationships (45%). This trend was particularly pronounced among Republicans, who had 60% of segments with proximity framing referring to primary privacy relationships. At the same time, Democrats had more segments with proximity framing that referenced secondary relationships (53%) compared to primary (47%). This dynamic gains additional support when we consider the strength of proximity framing. The strength of primary privacy framing was higher among Republican senators (M = 0.693) compared to their Democratic counterparts (M = 0.426), U = 101, p = .03.

Frequency analysis does not reveal significant associations when we consider the combined presence of orientation and proximity framing. The analysis of strength, however, suggests that vertical secondary framing (M = 0.562) was the strongest overall frame, followed by vertical primary (M = 0.449), horizontal primary (M = 0.167), and horizontal secondary framing being the weakest (M = 0.058). A series of Wilcoxon rank paired tests indicated that those differences were statistically significant.

When examined across institutional boundaries, the trends remain consistent. Mr. Zuckerberg has a higher proportion of references to both primary horizontal (34% compared to 16% among senators) and secondary horizontal privacy (12% compared to 3% among senators). At the same time, senators, as a group, have a higher proportion of references to both vertical primary and vertical secondary privacy (84% compared to 72% in Facebook's interventions in both cases). Similarly, when we compare the strength of combined framing of

privacy orientation and proximity, we find no statistically significant differences, but the trend remains so that vertical framing is slightly stronger in both primary (M = 0.469 vs. M = 0.427) and secondary relationships (M = 0.622 vs. M = 0.492) when described by the senators and horizontal framing is stronger in both primary (M = 0.25 vs. M = 0.095) and secondary (M = 0.109 vs. M = 0.014) relationships when described by Mr. Zuckerberg. Despite lacking statistical significance, this is an interesting dynamic, given that witness' responses in a hearing are to a large extent directed by the questions of committee members.

Among the senators, Republicans have relatively higher rates of both primary vertical (89% compared to 78% among Democrats) and primary horizontal references to privacy (21% compared to 11% among Democrats). Democrats make a more frequent use of secondary framing both in relation to vertically (94% compared to 74% among Republicans) and horizontally oriented privacy relations (6% compared to 0% among Republicans). Comparison of strength of frames across political lines reveals trends that support those systematic differences. The Republicans use stronger primary frames for both horizontally (M = 0.132 vs. M = 0.056) and vertically (M = 0.561 vs. M = 0.37) oriented privacy, while the Democrats use stronger secondary farming for both horizontal (M = 0.028 vs. M = 0.0) and vertical orientations (M = 0.736 vs. M = 0.513). Among those trends, the difference in strength of vertical primary privacy framing is statistically significant based on Mann-Whitney test (W = 109, p = .047).

Responsibility and conflict. In this category we differentiated between responsibility attribution for privacy infringement and for privacy protection. Additionally, we looked at conflict framing of privacy discourse. All three frames were present in the corpus at significant rates (p < .001): 83% of all interventions included a reference to infringement responsibility, 94% included a reference to protection, and 88% included a conflict frame.

Responsibility attribution. There was no significant difference in the overall frequency of use of responsibility for infringement (47%) and responsibility for protection (53%) frames. When comparing across institutional boundaries senators had higher proportions of use of both infringement and protection responsibility framing as compared to Mr. Zuckerberg (63% vs. 37% and 55% vs. 45% respectively). Among the senators the use of both frames was split equally. In Mr. Zuckerberg's discourse there was a higher proportion of protection framing (58%) as opposed to infringement (42%), but not enough to amount to a statistically significant difference.

Considering the strength of responsibility attribution framing, responsibility for protection was more dominant (M = 0.942) compared to responsibility for infringement framing (0.826), W = 5.5, p = 0.13. Committee members employed stronger infringement responsibility attribution

framing (*M* = 0.604) compared to Mr. Zuckerberg (*M* = 0.385), *U* = 367, *p* = 0.002; and slightly stronger protection framing (*M* = 0.878 vs. *M* = 0.844), albeit this last difference was not statistically significant. Further, Democrats used stronger infringement responsibility framing (*M* = 0.685) compared to their Republican counterparts (*M* = 0.526), *U* = 102, *p* = 0.004. They did so also for the protection framing (*M* = 0.917 vs. *M* = 0.842), but that difference was not found to be statistically significant using Mann-Whitney test.

Conflict frame. The conflict frame was present in over 88% of all coding units in the corpus. Senators appeared to use this framing more frequently (59%), compared to Mr. Zuckerberg (41%), *p* = .021*, Fisher's exact test*. There was no difference in the frequency of use of conflict framing across political lines. When considering the strength of the framing used, conflict framing was more pronounced in the comments made by the senators (*M* = 0.73) compared to those made by Mr. Zuckerberg (*M* = 0.453), *U* = 326, *p* <0.001. Among the senators, Democrats relied on stronger conflict framing (*M* = 0.861), compared to their Republican counterparts (*M* = 0.605), *U* = 90, *p* = 0.005.

Discussion

In this study, we set out to explore how elites frame privacy as a policy issue and how that framing can vary across institutional or political lines. Our findings suggest two main contributions to the literature. First, our findings demonstrate the importance of treating privacy as a multidimensional construct in both policy and research. Second, our findings empirically demonstrate the political nature of privacy as a vessel for normative perspectives and ideological positions.

Dimensionality of Privacy

The dominance of vertical privacy framing in our corpus stands in stark contrast with earlier findings about the dominance of horizontal framing among the users of information technology. In some ways, this difference reinforces an intuition expressed in prior studies that the public, and technological and policy elites may hold orthogonal frames in thought about privacy (Quinn et al., 2019). The dominance of horizontal perspective among the users can be explained through a number of mechanisms ranging from perceived audience (Lutz & Strathoff, 2014), through lack of awareness about the covert data collection practices by public institutions or by the platform provider (Steinfeld, 2016), to inadequate privacy literacy levels (Büchi et al., 2017; Trepte et al., 2015). The dominance of vertical perspective among the elites could be a factor of their perceived audiences, an indication of more institutional thinking or deeper

understanding of the complexities of information flows, as well as an expression of a normative position regarding the state of privacy and its regulation. Future studies should interrogate the explanatory mechanism behind the vertical orientation of privacy framing among the elites.

The interplay between vertical and horizontal primary framing of privacy is potentially indicative of strategic use of framing. it is possible that Senators and Mr. Zuckerberg project from their own experiences or employ personal vignettes for the purpose of humanizing the policy issues by giving it a “human face” (Semetko & Valkenburg, 2000). Such a strategy would require references to primary privacy relationships, regardless of orientation. The use of personal vignettes and episodic framing is indeed a common persuasive tactic in policy appeals (Gross, 2008; Hart, 2011). Further research can investigate how elites use frames that humanize policy issues.

The interplay between vertical and horizontal framing can also suggest a more strategic and conscious use of frames. Although lacking statistical significance, our finding suggests a trend under which Mr. Zuckerberg provided horizontally-framed answers to vertically-framed questions. For example, consider the following exchange:

> MARKEY: No, *would you support legislation to back that general principle, that opt-in, that getting permission is the standard*. Would you support legislation to make that the American standard? Europeans have passed that as a law. Facebook's going to live with that law beginning on May 25th. Would you support that as the law in the United States?
>
> ZUCKERBERG: Senator, as a principle, yes, I would. I think the details matter a lot, and now that …
>
> MARKEY: Right. But assuming that we work out the details, you do support opt-in as the standard? Getting permission affirmatively as the standard for the United States? Is that correct?
>
> ZUCKERBERG: Senator, I think that that's the right principle. *And a hundred billion times a day in our services, when people go to share content, they choose who they want to share it with affirmatively.* [emphasis added]

Pivoting a vertical discussion from a vertical framing to horizontal, shifts the agency and the burden of privacy protection from Facebook to individual users. Potentially, such framing also aligns with the corporate narrative of Facebook as a tech company that creates tools, including tools for privacy management and protection (e.g. Weigel, 2018).

Politics of Privacy

Formally, the hearing was focused on CA, which represents a secondary, vertical privacy relationship. Yet, our findings suggest a difference between policymakers with regard to primary and secondary vertical relationships. Republicans reference primary relationships between Facebook and its users, while Democrats emphasize vertical secondary relationships that involve information flows between platforms and institutional third parties. One way to interpret this finding is as a reflection of differences in views on the role of state regulation in systematically impacting corporate or industry self-regulation. Vertical primary framing of privacy draws attention to the relationships between users and Facebook as a platform that benefits directly from personal information shared by its users. Vertical primary framing therefore is associated with the ability of companies to self-regulate their individualistic relationships with their consumers. Their failure to do so requires state intervention that would empower individuals as consumers. Conversely, vertical secondary framing focuses on information sharing between the platforms and other third-party institutions. Users are less aware of these types of information flows. Regulation of vertical secondary framing is more closely associated with the need to use state regulation to counter the shortcomings of firms setting and enforcing rules on one another (industry self-regulation; Medzini, 2021a, p. 4; Porter & Ronit, 2006).

Another indication of the political nature of privacy is the dominance of conflict framing in interventions of the Democratic lawmakers. This finding might be a result of a broader understanding of the boundaries of state intervention, and particularly, a willingness to regulate relationships between social media platforms and application developers. It is important to note that such relationships are characterized as being one degree removed from the user. Democartic lawmakers might have required an additional frame, such as presenting a conflict, in order to justify the need for state intervention in the name of consumer protection where consumers are not directly present in the relationship being regulated. Another reason for the existence of conflict frames with Democrats might be their role in the opposition. As an opposition party, their goal might be to use the debate strategically to attack a possible connection between the Trump Campaign, Cambridge Analytica, and foriegn interference. Interesting to note that, Repoblican lawmakers countered this practice by Democrats by mentioning similar practices by the Obama Campaign and the fact that Mr. Zuckerberg has mitigated the use of the conflict frames by using it less often than politicians.

Conclusions and Future Research:

Our study demonstrates how privacy dimensionality is both indicative of elite discourse and can be strategically used to drive a narrative consistent with institutional needs and aspirations. It also demonstrates that elite actors or ideological flavours into rhetorical vessel that is privacy. As such, our findings draw suggestions toward a better understanding of self-regulation in the shadow of hierarchy. Scholars across disciplines raise concerns regarding the ability of tech giants to self-regulate. They are particularly worried about the companies' regulatory and political power (Nahon, 2015), as well as their ability to predict and modify human behavior (Zuboff, 2019). Similar concerns are raised about the implications of corporate self-regulation on human rights, including but not limited to the right to privacy, as well as their increasing anti-competitive behavior (Khan, 2017). However, to understand the structural foundations that enable extensive corporate self-regulation requires deeper understanding of the manner in which those structures are produced. Policy discourse of political and technological elites are those rare instances where such structures are consciously constructed through discourse (Epstein, 2015), this is the space where the shade of the shadow of hierarchy is made through the framing. Future research should interrogate the links between elite framing to actual practices of self-regulation of commercial companies amid pressures for increased regulation (e.g., Medzini, 2021a).

The research, however, is not without limitations. Methodologically, our study is constrained to a single Congressional hearing, which yielded a relatively small sample. While the sample size was adequate for demonstrating both the dimensionality of privacy framing and its political nature, future studies should cover additional hearings that touched on privacy challenges facing the big tech. Mr. Zuckerberg is not the only technological elite that testified before Congress. In recent years, Facebook, Google, Amazon, and Twitter had to testify several times before Congress. The testimonies of corporate managers representing these companies offer additional opportunities to study the framing of privacy by policy and technological elites. Inclusion of additional hearings is needed to continue validating the coding scheme. Additionally, a larger sample is likely to increase the reliability of our measures, which in turn will allow more nuanced measures of the various framing conditions. Conceptually, as we indicated throughout the paper, future research should explore additional attributes of privacy framing (e.g. conceptual framing of privacy as a value-based or a cognate-based idea) as well as general framing attributes previously explored in the literature (e.g. gain vs. loss or thematic vs.

episodic framing). Adding those attributes will create a more rounded picture of privacy framing by elites and allow for deeper engagement with existing literature in the field.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Adjerid, I., Acquisti, A., & Loewenstein, G. (2019). Choice architecture, framing, and cascaded privacy choices. *Management Science*, *65*(5), 2267–2290. https://doi.org/10.1287/mnsc.2018.3028

Afriat, H., Dvir-Gvirsman, S., Tsuriel, K., & Ivan, L. (2021). "This is capitalism. It is not illegal": Users' attitudes toward institutional privacy following the Cambridge Analytica scandal. *The Information Society*, *37*(2), 115–127. https://doi.org/10.1080/01972243.2020.1870596

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Brooks/Cole Pub. Co.

Amsalem, E., & Zoizner, A. (2020). Real, but Limited: A Meta-Analytic Assessment of Framing Effects in the Political Domain. *British Journal of Political Science*, *First View*, 1–17. https://doi.org/10.1017/S0007123420000253

Ashuri, T., & Halperin, R. (2017). "Losers" and "Winners": Framing of online self-disclosure in online news media. *The Information Society*, *33*(5), 291–300. https://doi.org/10.1080/01972243.2017.1354111

Bamberger, K. A., & Mulligan, D. K. (2015). *Privacy on the ground: Driving corporate behavior in the United States and Europe*. The MIT Press.

Barbehön, M., Münch, S., & Lamping, W. (2015). Problem definition and agenda-setting in critical perspective. In F. Fischer, D. Torgerson, A. Durnová, & M. Orsini (Eds.), *Handbook of Critical Policy Studies* (pp. 241–258). Edward Elgar Publishing. https://www.elgaronline.com/view/edcoll/9781783472345/9781783472345.00021.xml

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

Bazarova, N. N., & Masur, P. K. (2020). Towards an integration of individualistic, networked, and institutional approaches to online disclosure and privacy in a networked ecology.

Current Opinion in Psychology, *36*, 118–123. https://doi.org/10.1016/j.copsyc.2020.05.004

Bennett, C. J. (1992). *Regulating privacy: Data protection and public policy in Europe and the United States*. Cornell Univ. Press.

Braman, S. (2006). *Change of state: Information, policy, and power*. MIT Press.

Braman, S. (2012). Privacy by design: Networked computing, 1969–1979. *New Media & Society*, *14*(5), 798–814. https://doi.org/10.1177/1461444811426741

Bräunlich, K., Dienlin, T., Eichenhofer, J., Helm, P., Trepte, S., Grimm, R., Seubert, S., & Gusy, C. (2020). Linking loose ends: An interdisciplinary privacy and communication model. *New Media & Society*, online first. https://doi.org/10.1177/1461444820905045

Chong, D., & Druckman, J. N. (2007a). A theory of framing and opinion formation in competitive elite environments. *Journal of Communication*, *57*(1), 99–118.

Chong, D., & Druckman, J. N. (2007b). Framing theory. *Annual Review of Political Science*, *10*, 103–126.

Daviter, F. (2007). Policy framing in the European Union. *Journal of European Public Policy*, *14*(4), 654–666. https://doi.org/10.1080/13501760701314474

Druckman, J. N. (2001). On the limits of framing effects: Who can frame? *Journal of Politics*, *63*(4), 1041–1066. https://doi.org/10.1111/0022-3816.00100

Eising, R., Rasch, D., & Rozbicka, P. (2015). Institutions, policies, and arguments: Context and strategy in EU policy framing. *Journal of European Public Policy*, *22*(4), 516–533. https://doi.org/10.1080/13501763.2015.1008552

Entman, R. M. (1993). Framing: Towards clarification of a fractured paradigm. *Journal of Communication*, *43*(4), 51–58. https://doi.org/10.1111/j.1460-2466.1993.tb01304.x

Entman, R. M. (2004). *Projections of power: Framing news, public opinion, and US foreign policy*. University of Chicago Press.

Epstein, D. (2015). Duality squared: On structuration of Internet governance. In R. A. Lind (Ed.), *Produsing Theory in a Digital World 2.0* (pp. 41–56). Peter Lang Publishing.

Epstein, D., & Quinn, K. (2020). Markers of online privacy marginalization: Empirical examination of socioeconomic disparities in social media privacy attitudes, literacy, and behavior. *Social Media + Society*, *6*(2). https://doi.org/10.1177/2056305120916853

Epstein, Roth, M. C., & Baumer, E. P. S. (2014). It's the Definition, Stupid! Framing of Online Privacy in the Internet Governance Forum Debates. *Journal of Information Policy*, *4*, 144. https://doi.org/10.5325/jinfopoli.4.2014.0144

Fischer, F., & Forester, J. (1993). Editors' introduction. In F. Fischer & J. Forester (Eds.), *The argumentative turn in policy analysis and planning* (pp. 1–20). Duke University Press.

Fornaciari, F. (2014). Pricey privacy: Framing the economy of information in the digital age. *First Monday*, *19*(12). http://uncommonculture.org/ojs/index.php/fm/article/view/5008

Fornaciari, F. (2018). What is privacy anyway? A longitudinal study of media frames of privacy. *Journal of Intellectual Freedom & Privacy*, *3*(1), 8–20. https://doi.org/10.5860/jifp.v3i1.6414

Franzen, J. (2003). *How to be alone: Essays*. Farrar, Straus and Giroux/Picador.

Freelon, D. G. (2010). ReCal: Intercoder reliability calclation as a web service. *International Journal of Internet Science*, *5*(1).

Gamson, W. A., & Modigliani, A. (1989). Media discourse and public opinion on nuclear power: A constructionist approach. *American Journal of Sociology*, *95*(1), 1–37. https://doi.org/10.1086/229213

Gein, I. (2018). Toward a surveillance society? Issues of privacy and surveillance in the Bundestag debates. *MaRBLe*, *4*. https://doi.org/10.26481/marble.2018.v4.639

Genieys, W., & Smyrl, M. (2008). *Elites, ideas, and the evolution of public policy*. Palgrave Macmillan.

Gluck, J., Schaub, F., Friedman, A., Habib, H., Sadeh, N., Cranor, L. F., & Agarwal, Y. (2016). *How short is too short? Implications of length and framing on the effectiveness of privacy notices*. 321–340. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/gluck

Goffman, E. (1974). *Frame analysis*. Harvard University Press.

Gross, K. (2008). Framing persuasive appeals: Episodic and thematic framing, emotional response, and policy opinion. *Political Psychology*, *29*(2), 169–192. https://doi.org/10.1111/j.1467-9221.2008.00622.x

Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S., & Balissa, A. (2018). Privacy by designers: Software developers' privacy mindset. *Empirical Software*

Engineering, *23*(1), 259–289. https://doi.org/10.1007/s10664-017-9517-1

Hart, P. S. (2011). One or many? The influence of episodic and thematic climate change frames on policy preferences and individual behavior change. *Science Communication*, *33*(1), 28–51. https://doi.org/10.1177/1075547010366400

Héritier, A., & Eckert, S. (2008). New Modes of Governance in the Shadow of Hierarchy: Self-regulation by Industry in Europe. *Journal of Public Policy*, *28*(1), 113–138. https://doi.org/10.1017/S0143814X08000809

Hoornbeek, J. A., & Peters, B. G. (2017). Understanding policy problems: A refinement of past work. *Policy and Society*, *36*(3), 365–384. https://doi.org/10.1080/14494035.2017.1361631

Huijboom, N., & Bodea, G. (2015). Understanding the political PNR debate in Europe: A discourse analytical perspective. *European Politics and Society*, *16*(2), 241–255. https://doi.org/10.1080/23745118.2014.997593

Khan, L. M. (2017). Amazon's Antitrust Paradox. *Yale Law Journal*, *123*(3), 564–907.

Koduah, A., Agyepong, I. A., & van Dijk, H. (2016). 'The one with the purse makes policy': Power, problem definition, framing and maternal health policies and programmes evolution in national level institutionalised policy making processes in Ghana. *Social Science & Medicine*, *167*, 79–87. https://doi.org/10.1016/j.socscimed.2016.08.051

Lapenta, G. H., & Jørgensen, R. F. (2015). Youth, privacy and online media: Framing the right to privacy in public policy-making. *First Monday*. https://doi.org/10.5210/fm.v20i3.5568

Lombard, M., Snyder-Duch, J., & Bracken, C. C. (2002). Content analysis in mass communication: Assessment and reporting of intercoder reliability. *Human Communication Research*, *28*(4), 587–604.

Lutz, C., & Strathoff, P. (2014). Privacy concerns and online behavior – not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses. In S. Brandini, A. Tamo, & R. Schister (Eds.), *Multinationale Unternehmen und Institutionen im Wandel—Herausforderungen für Wirtschaft, Recht und Gesellschaft* (pp. 81–102). Stämpfli Verlag Ag. https://doi.org/10.2139/ssrn.2425132

Marwick, A. E., & boyd, danah. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, *13*(1), 114–133. https://doi.org/10.1177/1461444810365313

Marwick, A. E., & boyd, danah. (2018). Understanding Privacy at the Margins: Introduction. *International Journal of Communication*, *12*(2018), 1157–1165.

Masur, P. (2018). *Situational privacy and self-disclosure: Communication processes in online environments*. Springer International Publishing. //www.springer.com/us/book/9783319788838

Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, *8*(2), 258–269. https://doi.org/10.17645/mac.v8i2.2855

Medzini, R. (2021a). Enhanced self-regulation: The case of Facebook's content governance. *New Media & Society*. https://doi.org/10.1177/1461444821989352

Medzini, R. (2021b). Credibility in enhanced self- regulation: The case of the European data protection regime. *Policy & Internet*, 1–19. https://doi.org/10.1002/poi3.251

Minkkinen, M., Auffermann, B., & Heinonen, S. (2017). Framing the future of privacy: Citizens' metaphors for privacy in the coming digital society. *European Journal of Futures Research*, *5*(1), 7. https://doi.org/10.1007/s40309-017-0115-7

Mukherjee, R. (2000). "Now you see it, now you don't": Naming privacy, framing policy. *Critical Studies in Media Communication*, *17*(4), 469–492. https://doi.org/10.1080/15295030009388414

Nahon, K. (2015). Where There Is Social Media There Is Politics. In A. Bruns, E. Gunn, S. Eli, O. L. Anders, & C. Christensen (Eds.), *The Routledge companion to social media and politics* (pp. 39–55). Routledge.

Neuendorf, K. A. (2002). *The content analysis guidebook*. Sage Publications.

Nissenbaum, H. F. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books.

Obar, J. A., & Oeldorf-Hirsch, A. (2017). Clickwrap impact: Quick-join options and ignoring privacy and terms of service policies of social networking services. *Proceedings of the 8th International Conference on Social Media & Society - #SMSociety17*, 1–5. https://doi.org/10.1145/3097286.3097336

Osenga, K. (2013). The Internet is not a super highway: Using metaphors to communicate information and communications policy. *Journal of Information Policy*, *3*, 30–54.

Park, Y. J. (2018). Social antecedents and consequences of political privacy. *New Media & Society*, *20*(7), 2352–2369. https://doi.org/10.1177/1461444817716677

Pearce, K. E., Gonzales, A., & Foucault Welles, B. (2020). Introduction: Marginality and Social Media. *Social Media + Society*, *6*(3), 1–9. https://doi.org/10.1177/2056305120930413

Peters, G. B. (2005). The problem of policy problems. *Journal of Comparative Policy Analysis: Research and Practice*, *7*(4), 349–370. https://doi.org/10.1080/13876980500319204

Porter, T., & Ronit, K. (2006). Self-Regulation as Policy Process: The Multiple and Criss-Crossing Stages of Private Rule-Making. *Policy Sciences*, *39*(1), 41–72. https://doi.org/10.1007/s11077-006-9008-5

Quinn, K., Epstein, D., & Moon, B. (2019a). We care about different things: Non-elite conceptualizations of social media privacy. *Social Media + Society*, *5*(3). https://doi.org/10.1177/2056305119866008

Rajivan, P., & Camp, J. (2016). *Influence of privacy attitude and privacy cue framing on Android app choices*. Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016). https://www.usenix.org/conference/soups2016/workshop-program/wpi/presentation/rajivan

Ribak, R. (2019). Translating privacy: Developer cultures in the global world of practice. *Information, Communication & Society*, *22*(6), 838–853. https://doi.org/10.1080/1369118X.2019.1577475

Rochefort, D. A., & Cobb, R. W. (1994). Problem definition: An emerging perspective. In D. A. Rochefort & R. W. Cobb (Eds.), *The politics of problem definition: Shaping the policy agenda* (pp. 1–31). University Press of Kansas.

Scheufele, D. A. (1999). Framing as a theory of media effects. *Journal of Communication*, *49*(1), 103–122.

Scheufele, D. A., & Tewksbury, D. (2007). Framing, agenda setting, and priming: The evolution of three media effects models. *Journal of Communication*, *57*(1), 9.

Schon, D. A., & Rein, M. (1995). *Frame reflection: Toward the resolution of intractrable policy controversies* (Reprint edition). Basic Books.

Semetko, H. A., & Valkenburg, P. M. V. (2000). Framing European politics: A Content Analysis of Press and Television News. *Journal of Communication*, *50*(2), 93–109. https://doi.org/10.1111/j.1460-2466.2000.tb02843.x

Smith, Dinev, & Xu. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989–1015. https://doi.org/10.2307/41409970

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477. https://doi.org/10.2307/40041279

Stromer-Galley, J. (2007). Measuring deliberation's content: A coding scheme. *Journal of Deliberative Democracy*, *3*(1), Article 12. https://doi.org/10.16997/jdd.50

Telesca, E. (2018). Framing the right to be forgotten: A transatlantic cultural clash? A comparative newspaper analysis. *MaRBLe*, *4*. https://doi.org/10.26481/marble.2018.v4.642

Vitak, J. (2012). The Impact of Context Collapse and Privacy on Social Network Site Disclosures. *Journal of Broadcasting & Electronic Media*, *56*(4), 451–470. https://doi.org/10.1080/08838151.2012.732140

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.

Weigel, M. (2018, April 11). Silicon valley's sixty-year love affair with the word "tool." *The New Yorker*. https://www.newyorker.com/tech/annals-of-technology/silicon-valleys-sixty-year-love-affair-with-the-word-tool

Westin, A. F. (1967). *Privacy and freedom*. Athenum.

Wu, P. F., Vitak, J., & Zimmer, M. T. (2020). A contextual approach to information privacy research. *Journal of the Association for Information Science and Technology*, *71*(4), 485–490. https://doi.org/10.1002/asi.24232

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (First edition). PublicAffairs.

Appendix A – Unitization and Inclusion Criteria

Congressional hearings have a rigid structure that enables committee members to collect information during legislative, investigative, or oversight processes. Hearings usually start with the committee chair making an opening statement to introduce the subject and the purpose of the session. The ranking minority member generally follows with his or her opening statement. After the opening statements, witnesses are allowed to present their oral testimonies. Once the witnesses gave their oral testimonies, the chairs would start recognizing members to question witnesses. While committees have the discretion to determine the order of questioning, a common procedure is to alternate between parties in order of seniority (starting with the chair and the ranking member). Several committees imposed time limitations (e.g. 5 minutes) until all members had the opportunity to ask questions. The chair would set the ground rules for questioning at the start of the hearing or after the oral testimonies and would summarize the hearing at the end of the Q&A period.

Units of observation and coding units

Given the formal structure of the hearings, we shall view a single intervention as a *unit of observation*. An intervention here may mean either opening remarks or an exchange between a member of the committee and the witnesses within the allocated time. These are units of observation dictated by the structure of the hearings. Within each intervention, we shall separate the discourses of the committee member and each witness. Those discourses are the *coding units*, i.e. the units to which the coding scheme should be applied. When the coding scheme refers to an "intervention," please note that this refers to the part of a particular speaker in the intervention. The spreadsheet is organized so that there is a row for each speaker in each intervention, while the content of each intervention is copied across the relevant rows.

Inclusion/exclusion criteria

To apply the inclusion/exclusion criteria we need to recognize that each intervention may include a number of thoughts, where "a thought is defined as an utterance (from a single sentence to multiple sentences) that expresses an idea on a topic" (Stromer-Galley, 2007, p.9). A major component of Stromer Galley's coding scheme is mapping out the process of deliberation (she distinguishes between talk about problem, metatalk, process, and social). Since we do not aspire to code the entire deliberation, we are solely interested in identifying whether the intervention includes thoughts about privacy.

In Stromer-Galley's terms we are looking for talk about the problem of privacy and metatalk about privacy discussions in the hearing. She defines talk about the *problem* as "talk that focuses on the issue under consideration in these deliberations: school consolidation [or privacy - DE]. Opinions, agreements, disagreements, facts, and questions all deal with the problem they are discussing" (p. 22). At the same time metatalk "attempts to step back and assess what has transpired or is transpiring in the interaction, either as a group, or between individuals or to clarify meaning—one's own or someone else's" (p.22). The latter is important as it directly engages in contesting the framing of privacy.

Adopting Stromer-Gally's approach to unitization requires a positive answer to both of the questions below in order for an intervention to be included in the analysis:

1. Does the intervention include thoughts about privacy? Those could be references to privacy or related concepts such as data protection, security, control over data flows, etc.?
2. Is the function of that though procedural or substantive? We want to focus on substantive thoughts, i.e. thoughts that can be categorized as either talk about the problem or metatalk .

Interventions we choose to code should include substantive thoughts about privacy. It is possible that not all speakers in the intervention will include those, and that is OK. In such cases we only code those participants, who had substantive thoughts about privacy in the intervention.

In using Stromer-Gally (2007), it is important to remember that the genre of conversation we are coding here is different from what she is analyzing. Just as she distinguishes between deliberation and dialogue or other forms of social conversation (p.2), here we are not analyzing a deliberation per se, but a questioning with a rigid, formal structure, and long-standing, established practices and customs (i.e. an epistemic community with its own language and rituals).