Powerful Privacy Norms in Social Network Discourse

NORA MCDONALD, University of Cincinnati, USA
ANDREA FORTE, Drexel University, USA

Social media companies wield power over their users through design, policy, and through their participation in public discourse. We set out to understand how companies leverage public relations to influence expectations of privacy and privacy-related norms. To interrogate the discourse productions of companies in relation to privacy, we examine the blogs associated with three major social media platforms: Facebook, Instagram (both owned by Facebook Inc.), and Snapchat. We analyze privacy-related posts using critical discourse analysis to demonstrate how these powerful entities construct narratives about users and their privacy expectations. We find that each of these platforms often make use of discourse about "vulnerable" identities to invoke relations of power, while at the same time, advancing interpretations and values that favor data capitalism. Finally, we discuss how these public narratives might influence the construction of users' own interpretations of appropriate privacy norms and conceptions of self. We contend that expectations of privacy and social norms are not simply artifacts of users' own needs and desires, but co-constructions that reflect the influence of social media companies themselves.

CCS Concepts: • Human-centered computing~Collaborative and social computing theory, concepts and paradigms~Social networks

KEYWORDS

Social networks, privacy, social norms, critical discourse analysis

ACM Reference format:

Nora McDonald, Andrea Forte. 2021. Powerful Privacy Norms in Social Network Discourse. *PACM on Human-Computer Interaction,* Vol. 5, No. 2 (October 2021), 25 pages. https://doi.org/10.1145/3479565

1 INTRODUCTION

The pervasive and powerful influence of social media on human activities has motivated many thousands of studies in CSCW and adjacent disciplines. Privacy-related practices have occupied a great deal of attention and resources. Scholars have examined how affordances of social media platform designs influence disclosures [93, 95, 97], the role of policies [48], and how researchers can holistically approach policy and design [57].

This work was supported by the National Science Foundation (award CNS-2031951).
Author's addresses: N. McDonald, University of Cincinnati, 2600 Clifton Ave, Cincinnati, OH 45221, USA; A. Forte, Drexel University, 3141 Chestnut St, Philadelphia, PA 19104, USA.

2573-0142/2021/10 - Art421 $15.00

https://doi.org/10.1145/3479565

The importance of "getting social media right," especially with respect to privacy, has grown apparent over the course of many scandals, ranging from revelations of voter manipulation [65], to attacks on millions of user accounts [71, 92], to bugs that exposed users' unposted photos [15]. Facebook in particular has faced scrutiny by the US Congress [84] and the US Federal Trade Commission for, among other thing, misinformation, election interference, and privacy violations regarding its data-sharing and privacy practices [86]. Facebook has, at various points, acknowledged that there is some "work to do to regain people's trust" [21], while simultaneously asserting that the company is "transparent" with users about data and privacy settings [86].

As social media companies' strategies for stabilizing meaning around privacy are called into question, scholars have the opportunity and obligation to examine the narrative about privacy that these companies promulgate. We take inspiration from Hoffmann, Proferes and Zimmer's examination of how the CEO of Facebook Mark Zuckerberg's public statements have contributed to the construction of the Facebook user [52]. In this paper, we describe and contrast contributions of social media companies to public discourse about their respective users' privacy concerns through analysis of their blogs.

Our novel contribution is an analytic assessment of the way these three sites, even while obliged to mimic key functionalities and themes (like sharing user data with advertisers through an API), continue to articulate privacy norms in different ways. These three social media platforms maintain distinct "brands" whose discourse can obscure critical similarities. While the revelation of Facebook's discursive use of "authentic" identity [48] as well as its antagonism towards anonymity [6] are not new in the literature, what is new is the contrast in discourse when compared with Instagram and Snapchat. Instagram allocates blame to bullies and makes appeals to community niceness to imply that its users are responsible for establishing and maintaining content-related standards and norms. Snapchat's claim to ephemerality in the service of "vulnerable" identities (those Instagram and Facebook evoke with the proxy semiotic of the "bullied" and "harassed") seeks to protect users under a seemingly new data regime but still operates under their implicit control over data flows and their API similar to Facebook and Instagram. Our research highlights the shared conceptual semiotics of identity and privacy on which these companies regularly riff, ostensibly articulating the premise of "safe haven" for "vulnerable" and "bullied" identities in their own specific ways, but always on terms set by data capitalism [100] or data colonialism [20].

Those who wish to maintain control over digital infrastructures have incentive to control the narrative around data-sharing and privacy protections [53]. This paper looks specifically at how social media companies use their public blogs to shape these narratives. Specifically, this research asks two questions: What narratives do social media companies construct about user behavior and identity in relationship to privacy? And how do these constructions relate to privacy features and infrastructures? To answer these questions, we apply critical discourse analysis (CDA) to examine how company-controlled narratives about technologies characterize the norms and laws which contribute to privacy definitions for their users, as well as how these discourses reflect or deflect from decisions about the design of social network platforms that serve data capitalism. That is, at the center of discourse and myth of identity and privacy are platform business goals. By examining the discourse strategies of these service providers in relationship to privacy features and infrastructures, we offer insight into the language used to describe what constitutes information privacy and user identity, and by extension, specify what privacy users can expect.

2 RELATED WORK

CSCW scholarship has a history of advancing expansive views of computing systems that encompass not only the digital tools used to support cooperation and communication, but also social features of use [1]. The invocation of concepts like norms, power relationships, policies, social roles, and functions of groups are examples of how CSCW researchers have enriched analyses of technologies to account for social features. Here we focus on the ways that privacy in social media platforms has been conceptualized in the CSCW literature and how discourse analysis provides a critical lens through which scholars might regard both the construction of social media users and the accompanying interpretation of their privacy needs.

2.1 Privacy-Related Behavior

In CSCW and other HCI venues, privacy and related behaviors in social computing contexts are frequently investigated in relation to technical features (e.g., affordances [3, 97], nudges [99], defaults [63]), social norms (e.g., expectations [83], breaches/breakdowns [37]), and the personal characteristics or preferences of users [77]. While these approaches often illuminate important design and policy implications, in this study, our aim is to regard studies of privacy-related behaviors within existing social media systems as inherently susceptible to reproducing biases and power relationships inherent in the systems themselves. For example, much of the privacy-related work in CSCW relies on some explication of social norms but takes for granted the techno-cultural constructs (e.g., algorithms, metadata, protocols, interface, and default settings that shape social acts) and socioeconomic constructs (e.g., business models, governance, ownership status, partnerships) [28] that influence those norms, including the discourse that helps to construct them and make them opaque and/or acceptable. These constructs all intersect with user privacy.

When used to investigate people's behaviors on social media, social norms are often depicted as spontaneous cultural adaptations. Social norms are fetishized as being illustrative of how communities are able to negotiate shared practices and beliefs, despite those communities being constrained by endemic structures and affordances that hamper their freedom to act [61]. In essence, users "make do." Socially normative frames draw on mechanisms for establishing power to study users who may in fact be powerless [70]. By implication, this means the observer is really seeing (only) what the system allows. Norm-based analyses can overlook how discourse and structures, sometimes hidden or implicit, constrain people's behavior, particularly for those who do not recognize these constraints [2] or whose concerns are not accounted for by collective norms [72]. Social norms are everywhere, but they are particularly constraining on platforms where social activity is computational.

2.2 Privacy and Identity

Popular notions of individual control over privacy have origins in Alan Westin's theory of privacy, which he defines as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [101]. Westin thus assumes that individuals can fully understand and exert control over their data flows. In today's information environment, where access requires constant surveillance, there is really no way to exert control over one's privacy, nor to fully understand the nature of it. Westin's work is frequently associated with the privacy paradox—the idea that while privacy is always valued in principle, in practice, people's behavior often does not appear to be aligned

with their beliefs [47]. Anticipating a world in which consumer data might have fungible value to secure other benefits, Westin segmented people into groups he called privacy pragmatists, fundamentalists, and unconcerned. The cynical argument has been made that Westin used a lens handed to him by business interests who might have preferred to understate how much people care about privacy. But scholars have used that lens ever since to examine people's approach to privacy in the social media context. Notably, Westin would argue for individual-driven determination about what data is shared about them, which would become the bases for notice and consent laws [12]. In a society where users are told conflicting things (you're in "control" but there's no privacy) and where users are given privacy management tools they find impractical or onerous to use, it's no surprise that we have a paradox. The question is: is the paradox somehow native to the way individuals think, or is it the consequence of norms and techno-cultural and socioeconomic conditions imposed on individuals which create paradox?

Many scholars have pushed back on the privacy paradox, challenging the notion that, for instance, young people's behavior is paradoxical at all. So while many accounts of users' privacy attitudes and practices depict them as ultimately uncaring [5, 60] that view has morphed into notions of self-censorship [70, 78], or limited ability to assert agency over privacy [7, 8]. Some scholars are tapping into the powerlessness that users might feel to investigate their practice. The concept of "privacy cynicism" builds on studies of privacy apathy [51], helplessness [70], and fatigue [13], and offers some additional perspective on the privacy paradox [67]. Privacy cynicism, "an attitude of uncertainty, powerlessness, and mistrust toward the handling of personal data by digital platforms" tends to lead to more protective behavior (e.g., limited disclosures), not less [67]. Despite these seemingly contradictory claims, it's simply not clear what people actually believe they are doing when they take steps to protect their privacy, who they are protecting themselves from and, perhaps most importantly, whether more holistic action is something they feel helpless to impact. Mulligan et al. argues, the privacy harms that arise from data analytics and machine learning algorithms are "not addressed by strategies centered on individual control over information" [74].

Scholars have also conceptualized privacy as being related to the articulation and preservation of self. Altman conceived of privacy as a dialectical process for maintaining control over access to the individual [2]. Studies of youth have demonstrated that privacy is bound up in self-expression (e.g., [7, 64]) and the need to manage identity across collapsing contexts (e.g., [69]), which becomes more challenging with identities that are traditionally marginalized (e.g., [36, 47, 48]). In each of these conceptualizations, however, is a presumption that users have the tools to control their own boundaries.

Normative frames such as contextual integrity which stipulate the contextual, collective control of information flows [76], fall short of producing guidance for less privileged members of a group. Contextual integrity presupposes that groups are easily delineated and empowered [72]. While contextual integrity may usefully describe how individuals think about privacy as dependent on context and membership, it overlooks those whose privacy concerns are less visible and whose voices are marginalized, including those who may not feel they are members of the dominant Western normative group. This is increasingly important as we considered these platforms' dominance in countries outside the US who are "already marginalized in normative Western technoculture" [56].

2.3 Platform Privacy

There are limited avenues for privacy self-determination in today's current ecosystem, even when users are aware of the mechanisms controlling their privacy—though they are often not. In a study of what Twitter users understand about privacy on the platform, Proferes proposes "informational solipsism" to describe the way in which users are unaware of van Dijck's concept of techno-cultural and socioeconomic logics of the platform, particularly when they fall outside of activities for which there are feedback mechanisms [80]. For example, a default privacy setting or a partnership with a third-party has no feedback mechanism (e.g., no notification or alerts) to allow the user to know about their existence. Yet, these policies and protocols can importantly dictate the way "the social" is arranged in the service of an economic model [18]. Proferes found that many Twitter users have misconceptions about what meta information is publicly available, the sale of data to third parties, or the fact that Twitter is publicly traded. Those items that users had the most misconceptions about tended to be those that they do not see or encounter in regular course of use.

Other research similarly suggests that users may be unaware of the algorithms that fuel economic models of popular social media sites. For example, Eslami et al., found that many users of Facebook were unaware that algorithms were used for news feed curation [38]. Rader and Gray found that the exact mechanisms of content filtering algorithms on Facebook newsfeed remains opaque to most users, but that (right or wrong) they still alter their behavior in various ways in order to affect what they see [82]. Users speculate about how others' privacy decisions affect what they themselves can see. In Bucher's study of the "algorithm imaginary," users who are aware of Facebook algorithms describe feelings of being profiled, tracked, and falling short of "human experience" (e.g., when a man is shown highlights from the year that include his dead daughter) [11]. Privacy decisions and algorithmic logic are entangled but their mechanisms seem to recede. Gillespie argues that "as they become more pervasive and trusted, [algorithms'] logics are self-affirming" [45]. How is a user to understand the relationship between their privacy and, for example, the tools they have to defend it, or the algorithms that arrange their social activities? These relationships are immensely complex, and the narratives these social media organizations provide emphasize user "control" and otherwise conceal the truth about techno-cultural and socioeconomic relations that fuel data capitalism. How much do users know or intuit about these arrangements?

2.4 Panoptic Platform Power

Data capitalism [67], surveillance capitalism [103], and data colonialism [20], are various terms used to characterize this system in which data are extracted, harvested, and bartered for service. Each of these economic models of online data requires that we consider two implications. The first is that we live in a panoptic environment, where the fact that (or knowledge that) someone is potentially always collecting data, and thus watching, might cause us to *behave* as if someone is always watching. Panopticism was introduced by French philosopher Michel Foucault as a disciplinary phenomena that relies on the idea that we don't know if we are watched but we behave as though we are. This is how panopticism exerts norm-abiding power [42]. Equations between social network and Foucault's notions of surveillance have been made before in describing how social network functions for users who habitually keep an eye on the digital traces of others [68]. Foucauldian discourse offers a paradigm that conceptualizes the process by which authorities garner power through access and subjectification.

Second, according to Braman, our online information state has traded in panopticism for electronic surveillance that is more far reaching and more controlling [9]. Surveillance/data capitalism, which is built around the laws and policies of privacy control, seems to reproduce normative constraints and, in a sense, manufacture contextual integrity in its own image or according to its own interests [43]. Braman conceptualizes several types of power: instrumental power exerted through manipulation of the material world; structural power manifest as societal rituals, rules, and institutions; symbolic power exerted through ideas and semantics; and informational power that exerts itself through state regulatory mechanisms of information providers (e.g., at present, networked media). While this study builds on Foucault's original formulation, it also considers an ever more expansive control, the power of discourse to shape privacy norms that serve data capitalism.

2.5 Discourse and Power on Social Media Blogs

Publishing a blog not only gives social network companies power to influence discourse [31]; it also gives them a platform from which to publicly define and potentially influence users' own self-conceptions. As Facebook blog posts regularly make it into mainstream media articles [14, 39] and tech blogs [66, 85], we must consider the possible ways in which they may impute (or stand in for) privacy norms—and how they may use a narrowly defined user concept to influence perceptions of (and distract from) potential privacy violations.

Social network companies use their blogs as a channel for influencing the public, through dissemination to platform users and, more broadly, through news and other media. In this way, social network companies have some degree of control over the narrative around user behavior and privacy. News media regularly draw on the same voices and influencers for their own narratives, amplifying those voices in unaltered presentation, and bestowing implicit benefit of the doubt, if not explicit endorsement [24].

We treat the blogs of these social media companies as attempts to directly influence the public perceptions about their platform and products, including their privacy policies, attitudes, and tools. When these blogs get picked up by the media (as do some of the texts analyzed for this study) they can play an important role in cultural discourse and beliefs about new technologies [87]. Although talking about advertisements, Stein argues that media produced by technology organizations about their products "form part of that public domain and thereby influence public perception of the desirability and efficacy of technological mediation of everyday social and economic interactions" [87]. When it comes to discourse about privacy, Popiel found that past media coverage of mobile privacy in the US privileged privacy tradeoffs over rights [79]. Looking at news media coverage of teens on social media, Stern and Odland concluded that the relationship between teens and social media is often depicted as dysfunctional [88]. Studies of media's direct influence on consumers are somewhat harder to find but some note a discordance [35, 73]. While we assume that social media organizations' blog discourse shapes wider media discourse and is directly read by some users of the platform, future research might look directly at how these messages affect perceptions.

We follow Gillespie's lead in considering that it is important to understand the "cultural vocabulary" and discursive practices of these organizations to capture how user and advertiser identity are constructed [44]. For instance, we might speculate that lack of awareness about how social media organizations govern their platforms, as well as their business model and partnerships, is, in part, a result of social media organizations' control over discourse and the discursive way in which they engage in their own self-definition. Gillespie describes how social

media organizations' use of the term "platform," while inherently misleading, is nevertheless useful for them because it gives the ability to serve multiple audiences [44]. Social media organizations provide a lofty "platform" that "unproblematically moves across all three registers" of user (advertisers, content creators, and audience) to deliver opportunity [44]. In our study, we will similarly show how discourse is used to elide the interests of advertisers and users. In our analysis of Facebook, for instance, users control over advertisers is made to seem like a right but is depicted as one that Facebook bestows on its users.

2.6 Identity, Norms, and Control on Facebook

Since the inception of Facebook's public blog—and in fact, since the inception of the company—Facebook has tended to emphasize "authentic" behavior (and its inverse, "inauthentic" behavior) to articulate a set of precepts about what is and is not permitted or considered productive on the site—and in so doing, to make a case for their brand of privacy protections while obscuring ways in which those protections might ultimately redound to the benefit of advertisers. This notion of using interactions to extract data is referred to by Couldry and Mejias as "data relations" [20].

Commentaries have tended to suggest or imply a definition of authenticity being evidence of belonging to the identity and/or group you claim—and there is always with Facebook the implication that you are the same self from one post to the next. This relates to the definition of privacy as one where the user is in "control" as a legitimate citizen of the network whose identity as a user conforms to network norms, leaving them with nothing to fear.

In an analysis of Mark Zuckerberg's public statements from 2004-2014, Hoffman et al. describe the Facebook user as connected with normalized "authenticity" consistent with Facebook's real-name policy and ideological emphasis [52]. Facebook pays a great deal of attention to how "bad actors" involved in "coordinated inauthentic behavior" affect life on Facebook.

3 STUDY DESIGN

To investigate the public discourse of social media companies and understand how they construct users and their privacy concerns, we used Critical Discourse Analysis (CDA) to investigate public blogs associated with three of the most used social media platforms: Facebook, Instagram (both owned by Facebook, Inc.) and Snapchat [4].

3.1 Critical Discourse Analysis (CDA)

CSCW scholars have used variants of discourse analysis to understand features of communication within about surrounding sociotechnical systems. Discourse analysis provides a mechanism by which researchers can address how narratives, not only within but also about these systems, might influence their function in society. For example, Su used a constellation of texts about the game Street Fighter IV to construct an understanding of game-related practices and identities [89]. Hardy and Lindtner similarly used discourse analysis to understand how news media contributes to the construction of users of Grindr and SCRUFF [49]; they found that popular discourse around these sites contributes to a conceptualization of a "desiring user" that fails to reflect the experiences of rural users.

Although many applications of discourse analysis yield critical examinations of the power inherent in narrative constructions, we borrow from van Dijck's characterization of CDA as a

method that explores the ways in which discourse reifies social and political inequalities and relations of power [33]. CDA takes an "attitude of opposition and dissent against those who abuse text and talk in order to establish, confirm or legitimate their abuse of power" [33]. According to Fairclough, CDA exposes how discursive practices produce or reinforce relations of power through construction of knowledge [40].

We also expand upon André Brock's meditation on "critical technocultural discourse analysis" to argue that norm-based frameworks (which constitute a great number of studies of social networks) are insufficient to interrogate systems that reinscribe the very inequalities on which they are built [10]. This is an important aspect of investigating social media in particular, a technology upon which interactions and community are themselves constructed. To acknowledge that Facebook is built by privileged elites is necessary but not sufficient. It is just as important to recognize that the very theories used to characterize them in analytic discourse are inherently flawed if those theories depend on, and affirm, the social norms that emerge from within these platforms. When scholars approach sociotechnical norms with norm-based theories, what they discover is that the normative behaviors social platforms construct reflect the technology of the environment and its data relations. According to Brock, frameworks "reduce the cultural aspects of ICT [information communications technology] use to a technologically limited 'social' aspect (e.g., 'user') while privileging ICT usage of elites as a 'norm,' leaving unspoken the environmental, social, or cultural ideologies shaping ICT design, expectations, or use" [10]. We draw on Brock's adaptation, treating blogs as artifacts that frame beliefs and practice. We treat the utterances of social media organizations on their blog platforms (authored by both unnamed and named spokespeople) as form of discourse that creates, articulates, and reinforces social norms.

For example, social media produces "algorithmically defined online configuration" to create data capital from unwitting users and calls this value creation "social" [20]. When Mark Zuckerberg describes Facebook as "a fabric that can make *any* experience online social" he is referring to its ability to broker identity in a way that both creates and exploits social currency for profit [18].

Our analysis (detailed in the next section) identified ways in which social media organizations talked about privacy (sometimes without using the word) and in relationship to identity and personal control. Once we had identified these posts, we further analyzed them for linguistic choices, semiotics, and other rhetorical practices that added up to a conceptualization or privacy in the service of their business model. We constantly subjected our analysis to a socioeconomic reading in which these organizations' rhetoric, while suggesting control for users, provided access and control for their governance and economic logic.

3.2 Data Selection and Collection

Prior to data collection, we read press related to each of these institutions for a period of several months using the top ten returns from Google Alerts for the names of each of these platforms ("Facebook," "Instagram," and "Snapchat"). This allowed us to become acquainted with issues that were coming up in the press, how the social media companies responsible for the platforms were influencing discussions, and what vehicles they use to contribute to public discourse. We ultimately chose the news media blogs associated with Facebook, Instagram, and Snapchat because these blogs are the primary medium through which they communicate their perspectives to their users and the press.

We first scraped data from the blogs of Facebook, Instagram, and Snapchat using the python script Scrapy to gather blog titles from the inception of the blogs to December 2018. We then created two sets of data detailed in Table 1. We collected a total of 1,220 news blogposts of Facebook (https://newsroom.fb.com/news/), Instagram (https://instagram-press.com/), and Snapchat (https://www.snap.com/en-US/news/).

3.2.1 Privacy dataset. The first author initially read through all posts and coded for inclusion those that had to do with privacy. Privacy posts might, for example, talk about privacy concerns, privacy violations, or new privacy-related features or tools. To these posts, we developed an initial set of descriptive codes based on how privacy was defined (i.e., "privacy as" or "privacy from"). This included codes such as "privacy as control," "privacy as protection from government inquiry," or "privacy from third-party apps." Notably, "privacy" is mentioned in only 20 out of 67 Facebook posts coded for privacy, three out of the 17 Snapchat posts coded for privacy, and none of the seven Instagram posts coded as having to do with privacy. This analysis would ultimately point to narratives around power with a focus on the privacy asymmetries these social media organizations chose to highlight and those they do not. For example, we focus on how economic models are obscured in favor of narratives of user control of data streams and bad actors who want to violate users, articulated in different ways by each of these three social media platforms. We thus build on van Dijk, looking at how social networks manipulate discourse and define privacy "as" or "from" to create an authentic "us" and an inauthentic "them," "emphasizing Our good things, and emphasizing Their bad things" [30]. The secondary dataset helped to further deepen the analysis of how vulnerable users are enlisted in manipulative discourse about power and agency in relationship to privacy as we discussed below.

3.2.2 *Secondary dataset.* Another set of posts dealt with issues potentially having to do with platforms' perspectives on privacy-related norm articulation (often through exposition of counter-normative behaviors) expressed in themes like "bullying," "harassment," "inauthentic behavior," "hate speech," etc. We coded these as part of a secondary dataset. This dataset was included in our analysis of the privacy norms articulated by these social media platforms. These secondary coded data were important to make connections between discourse about privacy (in the primary analysis) and discourse about "vulnerable" identities (those suffering "bullying" and "harassment" described in our secondary data set), who are the targets of online vitriol. These datasets were merged for the final analysis. The first author developed codes and met regularly with the second author to discuss edge cases and code coherence.

Table 1: Data Collection

Platform	**Total blogposts (date)**	**Included in privacy dataset (wordcount)**	**Secondary analysis (wordcount)**
Facebook	957 (Apr. 19, 2006 to Dec. 13, 2018)	67 (36,096)	55 (44,770)
Instagram	173 (Oct. 6, 2010 to Dec. 11, 2018)	7 (3,205)	5 (1,641)
Snapchat	90 (May 9, 2012 to Nov 13, 2018)	17 (6,759)	2 (864)
Total	**1,220**	**91 (46,060)**	**62 (47,275)**

As we read the texts, we used the same first-author led approach to inductively develop an additional set of descriptive codes to guide exploration of the data such as "topics" (e.g., advertisers, API restrictions, new products etc.) and "solutions to privacy issues" (e.g., new tools, tutorials, changes to privacy policy, etc.). These codes were applied to the blog posts rather than to individual statements within them.

3.2.3 Critical Discourse Analysis (CDA) methods. We used CDA methods to augment our interpretation of these descriptive codes, looking at stated privacy definitions in relationship to rhetoric about privacy and reporting tools, topics, user identity, vulnerability, and behavioral norms. This allowed us to consider how language is tied to relationships of power and privilege in the design of tools, affordances, and policies to be used by dominant groups. To do this, the first author again read through each of these posts and coded segments of text based on their use of grammar, vocabulary, syntax, and rhetorical and semantic strategies, including the use of syllogism. The result is an analysis that used descriptive codes to guide thematic grouping of salient discourse strategies that illuminate how these concepts were constructed. For instance, we looked at how these organizations use semantics and vocabulary to undermine those victims they are purporting to protect.

It is important to note that Facebook Inc. bought Instagram in April 2012, an acquisition that led to some organizational tension based on differing visions, and may ultimately have led to some change in tonality at Instagram [54]. This offers an interesting perspective on the strategic ways that companies position a variety of platforms. Whatever intramural differences there may be, the two entities both differ from Snapchat in that their default platform is one-to-many, whereas for some users, Snapchat may be primarily a one-to-one platform. Snapchat users can post "stories" to followers in a way that is nearly identical to Facebook and Instagram, while (in a sign of regression toward common functionality) Facebook appropriated Snapchat's stories format—first, for Instagram in 2016, and for Facebook and Facebook Messenger in 2017. There are suggestions made in the media and by company insiders that Instagram sees Snapchat, with its default non-real name policy, as its norm-bearer [55]. This makes Instagram perhaps more like Snapchat, in some ways, than Facebook.

4. FINDINGS

We organize our first set of findings (Part 1) by summarizing how service providers talk about identity and behavior norms, often discussed in the context of discourse about the bad things that people do to perpetuate a myth about privacy control. In our second set of findings (Part 2), we go into more detail about the ways in which privacy is defined and how norms of behavior are used to support those definitions. Unifying our CDA analysis is the way each of these platforms often make use of discourse about "vulnerable" identities to invoke relations of power, while at the same time, advancing interpretations and values that give the user the illusion of power and favor data capitalism ("annexing" and selling user data) [20]. Our analysis primarily uses CDA, focusing on grammar, language, and rhetorical and semantic strategies used by these platforms, including the use of syllogism. We do this at the word and sentence level but also sometimes quote large bodies of text similar to van Dijk [32].

4.1. Part 1. Identity, Behavior, and Norm Articulation

4.1.1. Facebook: bullying and harassment. Bullying and harassment are challenging to manage because they cannot simply be "removed" by managerial oversight, but rather require (at the time of publication) victims to report them. These victims are "vulnerable" but for unclear reasons.

Facebook does not represent these bad behaviors as the consequence of privacy policies but rather, as a natural outcome of social interaction requiring social tools to remediate. Their discourse treats bullying as inevitable. As a result, Facebook relies on community policing, calling on friends and family to "protect people from bullying and harassment."

> "Being the target of unwanted attention can be stressful and some people may not feel comfortable reporting a bully or harasser … If you see a friend or family member being bullied or harassed, now you can report someone on their behalf ..." [23]

This is Facebook's rhetorical strategy: stating what users who are vulnerable to bullying and harassment "feel"—that is, "[not] comfortable reporting a bully or harasser"—thus necessitating intervention by dominant users. We adopt the notion of *implications* by van Dijk [29], arguing that the obligations of community defense on behalf of vulnerable individuals work to legitimate a loss of control and an increase in powerless. All its claims to the contrary, Facebook's discourse implies that they insist on retaining the right to be arbiters of bad behaviors reported by normative identities within the community. This is a clever semantic move: *informing* good Samaritans that they "now can report [to Facebook]" on behalf of others [23]. In this way discourse *about* affordances have semiotic value in shaping power relations.

What is also notable about this specific text is that the semantic construction renders the person who is "the target" an as-yet unproven victim. They are the focus of *unwanted attention*, which is not how you describe targets of "a bully or harasser." A bully, by definition, is a noun that packs the actor with so much negativity that there can be no grateful object; there is no *wanted* attention from a bully or harasser. This is not like a suitor from whom there may be either wanted *or* unwanted attention. "[A] bully or harasser" "targets" with violence and abuse, *not* "unwanted attention." (Notably, the use of the word *target* limits the interpretation of "unwanted attention" as coming from the bully or harasser and not from those whom one is reporting to, for example, authorities or the platform itself.)

Targets are possibly "uncomfortable" reporting "a bully or harasser" because Facebook is implying that the attention of a bully *needs* interpretation (i.e., is it wanted or unwanted). It's no longer clear what the actor is (bully or something else entirely?) since they must be explained by the recipient (or target) in order for there to be an acknowledged problem. The victim must tell Facebook (or their friend who is reporting to Facebook) if they want to be bullied or not, shifting the burden to the victim to prove that they didn't encourage it, that they didn't *want* it. Who then is in control? It would seem the arbiters of "attention," which is to say, Facebook.

4.1.2. Instagram: safety and kindness. Instagram has at times portrayed itself as a "safe place," whose goal is spreading "kindness" and promulgating productive interaction with brands. The word "privacy" is literally never mentioned. By contrast, "safety" and "kindness" are called out frequently; "safety" is used in titles eight times (all in the last three years) and "kindness," six times (all in 2017). For instance, Instagram offers "tips for staying safe" in which they suggest users make use of two-factor authentication or restrict visibility with a private account. They also attempt on several occasions to nurture a "safer, kinder community" with the introduction

of tools that block sensitive photos and videos, turn off comments, and remove followers (i.e., protect users from the unkindness and indecency of others). They attempt to elicit kinder behavior with the suggestion, for instance, that users "spread kindness by leaving an encouraging comment, giving an inspiring person a like, or sharing a message of support with a friend" [96].

A blog titled "New Tools to Help Keep Instagram Safe" published in August 2018, is used by Instagram as an opportunity to largely repeat these themes, calling out the relevance of "authenticity," which it defines as:

> "…an important way for you to know that the account you are interacting with is the authentic presence of a notable public figure, celebrity, global brand or entity." [75]

Instagram equates "safety" and "kindness" with "control" and "authenticity" and in so doing avoids responsibility for enforcing privacy and protection. In the Instagram lexicon, "kindness" and "safety" speak, respectively, to ways of being and acting (tools to use) that protect privacy without invoking the word.

4.1.3 Snapchat: liquid self. Snapchat is built on the very different premise that data-sharing should be ephemeral (without data traces or logs) and indeed, that the concept of identity is a false premise. Snapchat presumably grants users control over their information flows by not producing any for advertisers to use [102]. One of the rhetorical moves that Snapchat pulls is to describe the "self" in this privacy regime as "liquid" or "ephemeral." This creates a false sense that one's data is evaporating into thin air. Of course, that data vapor is being sucked into the Snapchat API; this is the business model.

In a 2013 Snapchat blog titled "The Liquid Self" Snapchat researcher Nathan Jurgenson promotes the view that users' identities are, in fact, "fluid" and "ever changing" [91]. A "liquid self," according to Jurgenson, is "more verb than noun." The "liquid self" is best served by a social network that doesn't impose a profile with a set of containers for age, race, gender, etc. that doesn't "bundl[e]" "self-expression" and potentially limit the kind of playful revision that we enjoy as we grow. According to Jurgenson, this is particularly true of Snapchat's most "socially vulnerable" users, for whom having a "single, stable, true" or "authentic" identity (borrowing language often used by Facebook in support of measures taken to ban users) can be problematic. Ultimately, Jurgenson offers up Snapchat as a "corrective," an antidote to the "authentic" web where there is room for identity exploration through impermanence and anonymity. Jurgenson writes in a footnote to the post:

> "The idea that a person should have a single, stable, true or authentic identity is most difficult for those who are more socially vulnerable. Having only one, unchanging identity may not seem all that problematic if who you are is not often stigmatized and penalized. However, there needs to be far more recognition that many people justifiably enjoy and need some social-closets where identity can be played with and not put on bright display because the potential consequences are greater. Race, class, sex, sexuality, ability, age, and all the other various intersections of power and vulnerability need to be part of the discussions around how social media is built, used, and improved." [91]

Here Snapchat is campaigning on behalf of the marginalized other, whom "you" may take for granted because "who you are" is an "unchanging identity." The "you" here is arguably white and privileged; the marginalized is othered. This privileged user is being campaigned to, as if they are in some position to further this regime of ephemerality. The privileged user is

seemingly the stand-in for the real culprit of identity free expression, which is the data that is being stored and sold.

The implications for privacy are not only that storing data is harmful to users, but that doing so disproportionally affects those with the most to lose, those for whom reality of the web is already challenging. For Jurgenson the "social-closets" of the web are the boundary-regulating settings that Snapchat provides through erasure. Snapchat evokes the data-less existence. They seem to be making Couldry and Mejias' argument about how data colonialism is "*annexing* human life directly to the economy" [20]. The language, at least, moves us away from the idea of erecting privacy protections for the self to a more fundamental *dismantling* of that self for the purposes of preventing encroachment. The cynical view, however, is that use of an API to which advertisers can connect directly with consumers of their platform [98], even if more private than Facebook [16], belies this insistence that data and identity are distinct and that advertising profiles built from data are not personhood. In this discourse, Jurgenson calls for identity vulnerabilities ("race, class") and "intersections of power and vulnerability" to be "part of the discussion" only to relegate them metaphorically to the "social-closet." The rhetorical strategy is to suggest that there is no need to debate or question power.

4.2 Part 2: Defining Privacy

In this section, we discuss in greater depth how each of these platforms implicitly define privacy (whether they invoke the term or rely on language proxies) and we reflect critically on how those definitions (and omissions or proxies) relate to each platform's articulated norms of identity and behavior. The language of control over data takes on many guises across these platforms but ultimately all are invested in sanctioning identity for the purposes of maintaining power over user data. We explore these definitions in relationship to infrastructural and socio-economic constructs.

4.2.1 Facebook: privacy as exercise of "control." None of these sites provides an explicit dictionary of terms like "privacy." Our CDA points to a functional definition of privacy on Facebook as user "control over data," in relation to advertisers, app abusers, or other users, through an arsenal of privacy controls and features. We coded 16 posts under the heading "privacy as control" spanning 2006 to 2017—the most frequent of any other theme. These posts often coincide with the rollout of a new tool and/or tutorial. For example, with the introduction of Privacy Checkup, a Facebook feature released in September of 2014, Facebook emphasizes the importance of "control" over data shared with what sounds like friends, but which actually also includes advertisers. It is as if the two (users and advertisers) are part of the same social ecosystem with the same terms of engagement.

The following post from 2014 begins by invoking the salience of personal engagement in the "about-you, not-us" space around which Facebook is ostensibly built; then, with a simple "but," it slips quickly and deftly into a different realm with discourse structured around the economy of personal data.

> "We know you come to Facebook to connect with friends, not with us. But we also know how important it is to be in control of what you share and who you share with." [95]

The use of "but" as opposed to "and" is a syntactical signal that the second half of the sentence, which ostensibly affirms personal control, is actually an implicit contradiction of the first: the assertion of users' own power to connect directly with friends. The word "but" concedes that

coming together on Facebook for purposes of connection is to surrender a certain important control over social relations, a control that Facebook, in acknowledging users might be troubled by its loss, implies it is prepared to restore or lend back.

On more than one occasion, Facebook has asserted that they don't sell users' information, but rather rely on that information to fund the delivery of "better service," employing an economic vocabulary which distinguishes selling data from requiring companies to pay for the privilege of using data [46]. They position the data access and permissions extended to advertisers as a benefit of using the platform since it allows the delivery of "stuff" users might want to see. In this same post, Facebook assured users that user activities supply advertisers with generalized information that brings users closer to friends ("issues that matter most to you") and helps Facebook recommend new groups. These "everyone wins" pronouncements are an illustration of how dominant norms are conditioned by economic relations [62] in which success depends on the continual commodification of their data [100]. Users' control over whom they share with (a particular vulnerability for non-normative users) is shaped by the economy of data flows.

In an April 2018 post, Facebook sought to reassure its users that they are not the product. The statement depicts a benign relationship with advertisers, and it aims to refute or ignore a commonly invoked economic premise that whatever is purchased by someone must be deemed a product. It is also refuting a more nuanced view: that if you receive something valuable without paying then you must be giving up something of value in exchange. In other words, it is representing the social network as a gift.

> "If I'm not paying for Facebook, am I the product?
> No. Our product is social network – the ability to connect with the people that matter to you, wherever they are in the world. It's the same with a free search engine, website or newspaper. The core product is reading the news or finding information – and the ads exist to fund that experience." [46]

The use of a "borrowed" rhetorical question, phrased as if the user is posing it, implies Facebook knows what you are thinking and, in fact, is deputized to raise concerns on your behalf by *borrowing your own perspective.* The flat "no," implies this question is a simple one with a clear and simple answer. It reads almost as a rebuke to the person who has presumed to pose the question, or on whose behalf Facebook presumes to pose the question. The use of gerunds like *reading* or *finding to describe the social network* casts the product in terms of user consumption, both informalizing and personalizing those activities so that they sound both quotidian and indispensable. The absence of an article ("the product is social network") serves to not particularize social network, elevating it to the status of universal nouns. Like love and kindness, "social network" is fundamental to existence. The word *fund,* which is frequently associated with a benefactor rather than a buyer, reinforces the notion that something is given as a gift by others in this triangle, with no user obligation in return. It is reminiscent of patronage: someone funding the arts in order for the audience to experience a free performance. The entire premise of this post conflates a purchase economy with a barter economy. The fact that consumers do not "pay" with dollars for their service means that they are offering something of value in exchange for the reading and the finding, which means that they are, indeed, a "good" or a "service" in a complex transactional equation.

In this same post, Facebook assured users that user activities supply advertisers with generalized information that brings users closer to friends ("issues that matter most to you") and helps Facebook recommend new groups:

> "If you're not selling advertisers my data, what are you giving them?
> We sell advertisers space on Facebook – much like TV or radio or newspapers do. We don't sell your information. When an advertiser runs a campaign on Facebook, we share reports about the performance of their ad campaign. We could, for example, tell an advertiser that more men than women responded to their ad, and that most people clicked on the ad from their phone. [...] As people use Facebook, they share information and content – whether it's liking a post, sharing a photo or updating their profile. We use this information to give you a better service. For example, we can show you photos from your closest friends at the top of your News Feed, or show you articles about issues that matter most to you, or suggest groups that you might want to join." [46]

When Facebook disclaims selling (as opposed to merely using) data, there is a false equivalence being drawn. The Facebook construction of events assumes that the user and the advertiser are networking under the same rules, with the same privacy controls. Because of revelations in late 2018, the public now knows that advertisers see much more than was previously acknowledged, and that violations of the social contract on this platform were, in fact, enabled by Facebook [21]. Now that the veil has been lifted, users are also confronting the realization that Facebook redefined privacy as a service, in which personal data are used to provide a satisfying experience by customizing offerings.

This manipulation of the truth serves their bottom line in two ways. First it allows Facebook to grant advertisers access couched in the language of user settings, the same or similar settings relied on by users to negotiate their identity on the platform. Second it allows users to prevent unwanted disclosures by relying on those same tools. It is a circular conception of identity and privacy control, which ties decisions about who can access them (advertiser or friend) to identity performance. False equivalence (between advertiser and friend) puts users' own power on the same plane with that of advertisers, whose own "authenticity" is defined (collaboratively with Facebook) in terms that don't align with definitions of user authenticity. In Facebook discourse, the equation of social and commercial occurs behind a veil of terms that cannot possibly mean the same thing when applied to social users and advertisers.

4.2.2 Facebook: privacy is protection from abusers. The second most common and related type of privacy post focuses on protecting users' privacy from advertisers or application abusers. In these instances, Facebook typically describes defending users against apps that have overstepped by imposing restrictions and investigations (e.g., Cambridge Analytica, which is mentioned in five out of 12 privacy posts in the last year of data collection).

Facebook tackled the Cambridge Analytica violation of the user-advertiser pact, depicting the problem as an abuse of privileges bestowed on companies by a community that extended trust. The implication is that bad actors, lacking self-restraint, violated "policies" in a community built on trust and controlled only through self-policing.

> "[W]e know that this flow of information has the potential for abuse [...] as we saw with the Cambridge Analytica situation, bad actors are more than willing to ignore these policies in pursuit of their own objectives." [22]

There is nothing in this paragraph which assumes structural responsibility for an environment in which bad actors are free to behave badly, much less any nod to the ways in which data flows could prove to be particular liabilities for vulnerable users. Indeed, the phrasing "flow of information" makes it seem natural and by extension, any intervention by Facebook; they

cannot intercede on nature. In this respect, at least, Snapchat's discourse reflects greater sense of responsibility for the problem.

4.2.3 Instagram: privacy is about "staying safe" by living in a "safe community." As noted, Instagram does not use the word "privacy" in any of its privacy-related posts. The semiotic proxy is "safety:" six out of the seven posts that relate to the concept of privacy on Instagram have the word "safe(r)" in the title. The concept of "safety" is interesting, semantically and critically. While Instagram most commonly refers to keeping "Instagram safe," they also, on two separate occasions, talk about a "safer" community. One of these two posts deal specifically with a new feature in partnership with Facebook which allows users to report harassment or bullying. Responsibility for keeping Instagram safer is therefore left in the hands of the entire community, who are ostensibly given tools and responsibility to act protectively on behalf of the most vulnerable.

These tools are situated in a context of norm propagation, as illustrated by a post from 2016 introducing new tools or reinforcing old ones, underscoring the responsibility of users to keep Instagram safe and welcoming.

> "Since the beginning of Instagram, we have focused on making it a welcoming place for everyone … I'd like to tell you about a few more tools we're launching to keep people safe." [59]

This post represents the apogee of Instagram's privacy norm articulation. It does little more than make safety a collaboration between community and platform based on Samaritanship rather than empowerment.

4.2.4 Snapchat: privacy is "the right to be forgotten." The precept of users' data as ephemeral, and therefore not available to be mined or used, is advanced by Snapchat as a "corrective" to real-name social network sites like Facebook. In a post on the company blog titled "Temporary Social Media," Jurgenson aligns Snapchat with propelling a movement to seriously constrain digital traces, thus making digital communities more closely approximate life in the physical world.

> "It's easy to underestimate the significance of injecting more ephemerality into social media … It alters the functioning of social stigma, shame, and identity itself. Beyond the 'right to forget', what about the possible erosion of the obligation to remember?" [90]

Snapchat's rhetorical strategy is a warning shot: it's easy to "underestimate" the logic of "ephemerality" at the cost of experiencing "stigma" and "shame." What Jurgenson is advocating is not a return to the old offline world, but rather a data-free online existence where the desire to retreat or "be forgotten" is the unnaturalness of the medium itself and its misalignment with our more ephemeral real/authentic/physical world. In this same post, Jurgenson considers that Snapchat has norm-busting potential. The admonishment described earlier about the "harm" caused by "permanent media" is singled out as being particularly harmful to non-normative identities. In this same post, Jurgenson observes that when privacy mistakes are made, it is the "not straight, white, and male who pay the biggest price."

> "It is deeply important to recognize the harm that permanent media can bring–and that this harm is not evenly distributed. Those with non-normative identities or who are otherwise socially vulnerable have much more at stake being more likely to encounter the potential damages past data can cause by way of shaming and stigma. When social

> media companies make privacy mistakes it is often folks who are not straight, white, and male who pay the biggest price. This is why movements like the right to be forgotten are so crucial." [90]

Here, Jurgenson is ultimately rejecting the normative precept of "flawlessly consistent" identity required of social networking in favor of ever-changing identity, not pitting ephemeral media against authenticity so much as questioning whether authentic identity ever existed in the first place. If you agree that visibility is bad (and it's "deeply important" that you do) then by implication, you should be motivated to embrace Snapchat's ideology of ephemerality. By devoting attention in this discourse to a concept of ephemeral real-life identity, this discourse successfully diverts attention away from a more durable, ineluctable reality. Users' profiles can still be matched against advertiser's data, meaning that threats to safety are not eliminated but merely displaced, lodged in the reams of "permanent media" recreated elsewhere. This conversation forces us to consider whether privacy is not the right of the white, privilege male and/or the right to choose with whom we share information, but the right not to store it in the first place. The concept of erasable data doesn't just facilitate the right to be forgotten; it safeguards it. From Snapchat's perspective, data permanence (or identity permanence) should never be a requirement or a norm of interaction.

4.2.5 Privacy is erasable data. The right to be forgotten clearly overlaps with the notion of privacy as erasable data. As already noted, Snapchat configures an identity that is best served by a privacy policy of zero or little data and limited record-keeping. This is particularly true with respect to the "vulnerable" individual for whom Snapchat expresses concern in the design of privacy policy.

In an update to their privacy policy, Snapchat reiterates what ephemeral media is *not*: an attempt to warehouse user data and user interactions for the benefit of advertisers or business partners.

> "[W]e continue to delete [your snaps] from our servers as soon as they're read, we could not—and do not—share them with advertisers or business partners." [81]

This phrase "continue to delete [your snaps] from our servers as soon as they're read" functions to make Snapchat not just the platform in control of user data, but also the friend who reads your "Snap" and then deletes it. There is, in fact, some controversy about users taking screenshots of Snaps to override Snapchat's ephemerality. Here Snapchat provides misleading assurance that Snaps are deleted "as soon as they're read," as if they are also the friend (or maybe even watching the friend and thus in the position to assure you) who read them and then deleted them.

Snapchat's notion of identity as a series of fleeting impressions fits nearly perfectly with their explicit data policy of storing data only to be seen by other users and then deleted when read. Notably, this policy is bolstered by concern for those whose identity leaves them more vulnerable, more susceptible to the drudging up of identity stigma unless they subscribe to a data-less exchange.

5 DISCUSSION

This analysis of social network blog discourse highlights the ways in which information privacy discourse is inextricably linked to user identity and norm articulation. Facebook's focus on "authentic" behaviors belies what is, in fact, an infinitely extensible and intrusive information

privacy policy that obligates users to be "in control" of all their data without giving them true latitude to do that. Facebook is very much grounded in the language and theory of Westin and Altman's individualistic privacy "control," talking incessantly about giving user's "control" over what information is shared about them to advertisers, who are, of course, part of "social network," the neutral *funders* of the experience. Facebook and Instagram evoke a normative community-based model of privacy that borrows from contextual integrity the notion that *where* and *why* data flows is regulated by community members who want to make the community safe and trusted.

Facebook also makes normative users responsible for defending others whose non-normative identities presumably render them more vulnerable to bullying and harassment. In recent years, Instagram seems to have adopted this concept as well, couching it in morally prescriptive terms like "safety" and "kindness"—as if these concepts were handy affordances, as readily available to users as privacy settings might be. The easy transposition of terminology suggests that the rhetoric of either of these two sites can be used to interpret the other.

Snapchat, in no uncertain terms, presents itself as a corrective to both, with its very different approach to data management and retention—policies which serve to mitigate security risks on one hand, and to facilitate fluid identity on the other. Each sites' philosophy of identity and self-presentation is aligned with their respective privacy and security setting options and the rhetoric that surrounds them.

Through articulation of behavioral and identity norms and values in their blog posts, these companies provide maps which depict their information privacy practices and expectations. Facebook's notion of privacy is utilitarian, justifying privacy encroachments on the basis of their ostensible value to users, conflating the clear benefits to advertisers with the not-so-clear benefits to users of advertising customization. This service model does not offer or acknowledge an independent notion of privacy separate and apart from user satisfaction with advertising customization. It does not offer a notion of privacy that is even separate and apart from a somewhat lower standard: passive acceptance of whatever passes through the advertising filter constructed with users' own data. By contrast, Snapchat's foundational premise is that the user should have the right to evolve, and with that evolution comes ostensible protections against encroachment. That is, if by protection what is meant is the right to reinscribe yourself; and the platform's own technology would seem to instantiate that notion by precluding permanent user self-documentation. Instagram is more ambiguous in language and ideology, although they seem increasingly to be speaking the dialect of Facebook. It is not clear, in this dynamic, post-acquisition scenario, how site norms are evolving in relationship to the public articulation of privacy norms.

Our analysis also shows how dominant social network providers insert themselves into characterizations of users and user privacy needs/goals. Our analysis shows how these social networks use vulnerability as the conceit of their discursive style. Indeed, the spokespeople of these organizations assume so broad a mandate on the subject of privacy that they define social values even in offline environments, claiming the moral authority to speak for the way users construct privacy wherever they are [97]. This seems to be particularly the case for Snapchat, which advances a fiction that they successfully emulate an offline standard and experience of privacy, where an individual's data are not easily captured (or even remembered). In doing so, they overlook or ignore transactional privacy concerns that remain in this digital simulacrum of social reality, based on the way data are stored and encrypted. The values they project on users are unconstrained by the boundaries of online spaces because, by implication, those values

insist on authenticity and connection with real-world contacts. Our most important selves may live online, and those who govern our identity and our data online assert a broader power.

While Snapchat's argument for the "liquid self" might easily be read as validation, embrace, and defense of non-normative identities, they may effectively create, through the process of erasure, a paradoxical or unintended consequence, in which such individuals are relegated to an invisible, sanctioned safe space [62]. It is reminiscent of the spaces in which bullied Facebook users reside: on site but out of sight, without agency (e.g., because they don't "feel comfortable," or may not legitimately be victims as Facebook implies) to report bad behaviors.

All three platforms position their own policies about privacy and data flows as the final word on *how to be* in networked spaces. In that sense, these sites are defining privacy for platform users rather than channeling or reflecting existing norms of privacy—norms which the members of any society may struggle to define for themselves. Because these platforms are self-appointed arbiters of privacy, claiming to know and respect the wants and desires of users, their articulation of privacy norms and values requires continual scrutiny. They may propagate a set of priorities that better suit the commercial needs of social media sites than the true desires of their user communities. Social media prophesies regarding what users want (i.e., to connect with friends and advertisers) becomes self-fulfilling. The implications from this work are that norms surrounding privacy articulated by social network services are not necessarily resident or endemic throughout their user communities. But no matter their source, these norms are ultimately tools of control used by social network service providers to dictate terms of identity which support their economic model. Social networks are not a safe space for identity exploration. They are not even a natural environment for our true selves, at least not on terms that any service providers are capable of offering. In each of these spaces, the power to harvest data and control data flows resides with the companies. Variations in the language used by each may signal different levels of protection or different priorities, but all operate based on the syllogism that identity must be sanctioned to be safe; that the privacy tools provided by the site give users the appropriate identity control (potentially even replicating the controls available outside the digital world); and therefore, these platforms are necessary, and also effective for safekeeping identity.

If we accept the premise that discourse of social media networks sustains production of data capitalism [94, 104], the critical question is not *whether* users' needs and wants are reflected by these platforms. Rather, it is how discrepant, or at odds, they may be, and what are the consequences when users are socialized to embrace privacy norms that may violate their own self-interest? The challenge in an environment where social media platforms control the discourse and the terms of data protection is whether we can withdraw their claim to normative legitimacy and start anew [34].

5.1 The Economic and The Social, and Radical Literacy

We applied CDA as a method for interrogating text and talk to see how social power manipulation, control, and inequality are (re)produced on social media blogs. Our insights about how discourse is used to obscure power and economic relations as they pertain to privacy has implications for how we do research in CSCW going forward, which we discuss in this section. Arguably, the myth of existence on these platforms may be so engrained that they require radical approaches to literacy that incorporate framing around and education about data capitalism. We start with looking at how other researchers have explored data capitalism and privacy and then conclude with recommendations for future research.

West's recent analysis of the rise of data capitalism is instructive here in that it shows how big tech has long been creating narratives that "mask information asymmetries resulting from the commoditization of data by foregrounding the social and political benefits of networked technologies," creating an illusion of personalization and consumer power [100]. Mark Zuckerberg is particularly masterful at deploying this "double bind" in which users are "caught between desires for privacy and the ability to form meaningful communities with other users online without opting out of these services" [100]. In this model, the myth of user "control" over the social contributes to the endlessly recursive construction of the self from data that arguably fuels data/surveillance capitalism. How then are we to study social networks "as if the social mattered" [18], if what we are watching is a heavily manipulated social reality?

Some work has begun to explore what users believe about the algorithmic mechanisms that support data capitalism [26, 38, 50, 82]. In 2014, van Dijck argued that users are being conditioned to regard "algorithmic relations" as mere social interactions [27]. To study privacy behaviors and expectations as if they are unmediated by algorithms that support platform economics is becoming, nearly ten years later, increasingly problematic. To van Dijck's point: "Promoting the idea of metadata as traces of human behavior and of platforms as neutral facilitators seems squarely at odds with the well-known practices of data filtering and algorithmic manipulation for commercial or other reasons" [27]. In other words, it would be disingenuous to study what people do as a result of purely social activity uninfluenced by some larger techno-cultural and socioeconomic fix.

The apathy and helplessness that some CSCW and communication scholars have convincingly posited (e.g., [51, 70]) seems to suggest that data capitalism renders individuals helpless to conceptualize or defend their privacy. Fisher argues that "capitalist realism" operates as an all-consuming atmosphere that regulates culture to the extent that it is not possible to imagine another future [41]. Have we become so accustomed to (data) capitalism that we can't imagine anything else? Dencik and Cable argue that it's impossible to resist the pull towards "social" established mechanism of citizenship like the ones we find on Facebook [25]. Those who dare engage in abstinence from the commodification of their data suffer consequences. Social media, operating in late-stage capitalism enforces a social order of the market. In his discussion about datafication, Couldry quotes Marx saying that "individuals are now ruled by abstractions" and these abstractions nevertheless change our subjectivity and our norms [17].

The confessions of ex-Facebook and other technology company employees who argue that social media platforms have monetized attention at the expense of social and democratic institutions may be a staggering (and hopeful) disavowal of Silicon Valley utopianism and economic logics, but they do not provide a clear path forward [58]. The social forces that are catapulting us towards what Couldry and Mejias darkly describe as data colonialism require a radical, critical accounting for power and subjectivity [19, 20] that includes users.

How we transition to new forms of radical literacy about the ways that we are instruments of data capitalism would seem to be the next step for CSCW scholars. Radical literacy focuses not just on the "how to" of privacy but also on understanding the data capitalism infrastructures that influence what is being done to users *and how*. We should also be investigating how users think about algorithms in relationship not to other people's behaviors but social networks' business models and bottom line. More research is needed to explore how people think about what constitutes "social" interaction on these platforms and about data capitalism, and how knowledge of theses mechanics (can) change behavior and expectations about privacy. CSCW studies should continue to grapple with how perceptions of privacy and privacy preserving activities relate to data capitalism [67]. What do people know about data capitalism and how

can they be educated about it in ways that empower them? CSCW researchers are particularly well suited to traverse a research landscape in which we may find that there is little opportunity for literacy to address privacy deficits, but unlimited potential for reimagined sociotechnical spaces.

6 CONCLUSIONS

This study looks at how rhetoric propagates identity norms and spins them into myth; and considers how those norms fit within a framework of organizational policies whose goal is ultimately to advance the commercial objectives of social media platforms. Each of these social networks talks about privacy but almost always obliquely. They use rhetoric and constructs that invoke proxy ideas like safety, personal authenticity, and data impermanence, without taking care to expose potential misalignment between data and economic policies and whatever privacy norms might already be present in the community. Propagation of these proxy concepts has the effect of removing the word privacy from social media discourse and creating for users a set of standards that have more to do with functionality, satisfaction, and comfort than user agency or privacy self-awareness. Differences in the language may reflect differences in the protections available to community members but language may also serve to cloud rather than expose these policies. The language also cultivates a view of the self that may include or condone non-normative, fluid, or fragmented identities but does not necessarily give users full protection. Because online identity construction is intrinsically related to how data is managed and maintained, protections also correspond to degrees of identity consistency versus impermanence.

The three platforms we studied created three distinct identity myths to support their business goals. These identity myths don't necessarily reflect the realities of their users but they do support definitions of data and power which are inscribed in the system and which their users ultimately embrace (or, at least, concede to) through use of the system, even if that imposes normative constraints [78]. Motivating this work is concern for who is left out of norm articulation when dominant social network companies control discourse and the consequences for those who are left out. It is also becoming clear, however, that these norms may not be appropriate for any users, that there is, perhaps, nothing resembling social activity worth fighting for. This critical approach shows the way that media companies conceptualize (pragmatically) both normative users and non-normative (the "vulnerable," the "bullied") users and the tools and other solutions they offer—and the behaviors and identities they attach to use of those tools.

6.1 Limitations

We chose these three social media platforms because they did and still do dominate the market and are highly visible in setting the tone and agenda for data capitalism and privacy. These data were gathered in 2018 and, while a lot has happened since then with regard to social media platform privacy and governance, much of the rhetoric around privacy remains the same. We also capture the years before and after the Cambridge Analytica events, when discourse was likely to change in significant ways. We focused interpretation of our results through the lens of US-based users but encourage further analysis from the perspective of non-US users for whom privacy practices and policies are different.

Future work might look at a variety of network platforms and/or examine text from these blogs that have made their way into mainstream media—investing more in how power is

networked in more pervasive ways. For instance, research should empirically study how these communications impact user's perceptions of privacy, and how knowledge of the mechanics of data capitalism shapes behavior and expectations about privacy. Future work should also look at how to reimagine these spaces informed by a critical lens on power.

REFERENCES

[1] Ackerman, M.S. 2000. The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility. *Hum.-Comput. Interact.* 15, 2 (Sep. 2000), 179–203. DOI:https://doi.org/10.1207/S15327051HCI1523_5.

[2] Altman, I. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Brooks/Cole.

[3] Andalibi, N. 2020. Disclosure, Privacy, and Stigma on Social Media: Examining Non-Disclosure of Distressing Experiences. *ACM Transactions on Computer-Human Interaction (TOCHI).* 27, 3 (2020), 1–43.

[4] Andrew Perrin and Anderson, M. Share of U.S. adults using social media, including Facebook, is mostly unchanged since 2018. *Pew Research Center Report.*

[5] Barnes, S.B. 2006. A privacy paradox: Social networking in the United States. *First Monday.* 11, 9 (Sep. 2006).

[6] Bodle, R. 2013. The ethics of online anonymity or Zuckerberg vs. "Moot." *ACM SIGCAS Computers and Society.* 43, 1 (2013), 22–35.

[7] boyd, danah 2014. *It's Complicated: The Social Lives of Networked Teens*. Yale University Press.

[8] boyd, danah and Marwick, A.E. 2011. *Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies*. Technical Report #ID 1925128. Social Science Research Network.

[9] Braman, S. 2009. *Change of State: Information, Policy, and Power*. The MIT Press.

[10] Brock, A. 2018. Critical technocultural discourse analysis. *New Media & Society.* 20, 3 (Mar. 2018), 1012–1030. DOI:https://doi.org/10.1177/1461444816677532.

[11] Bucher, T. 2017. The algorithmic imaginary: exploring the ordinary affects of Facebook algorithms. *Information, Communication & Society.* 20, 1 (Jan. 2017), 30–44. DOI:https://doi.org/10.1080/1369118X.2016.1154086.

[12] Cate, F.H. 2010. The Limits of Notice and Choice. *IEEE Security Privacy.* 8, 2 (Mar. 2010), 59–62. DOI:https://doi.org/10.1109/MSP.2010.84.

[13] Choi, H., Park, J. and Jung, Y. 2018. The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior.* 81, (Apr. 2018), 42–51. DOI:https://doi.org/10.1016/j.chb.2017.12.001.

[14] Conger, K., Dance, G.J.X. and Isaac, M. 2019. Facebook's Suspension of 'Tens of Thousands' of Apps Reveals Wider Privacy Issues. *The New York Times.*

[15] Constine, J. 2018. Facebook bug exposed up to 6.8M users' unposted photos to apps. *TechCrunch.*

[16] Constine, J. 2018. Snapchat launches privacy-safe Snap Kit, the un-Facebook platform. *TechCrunch.*

[17] Couldry, N. 2020. Recovering critique in an age of datafication. *NEW MEDIA & SOCIETY.* 22, 7 (2020), 1135–1151. DOI:https://doi.org/10.1177/1461444820912536.

[18] Couldry, N. and van Dijck, J. 2015. Researching Social Media as if the Social Mattered. *Social Media + Society.* 1, 2 (Jul. 2015), 2056305115604174. DOI:https://doi.org/10.1177/2056305115604174.

[19] Couldry, N. and Mejias, U.A. 2019. Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television & New Media.* 20, 4 (May 2019), 336–349. DOI:https://doi.org/10.1177/1527476418796632.

[20] Couldry, N. and Mejias, U.A. 2019. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press.

[21] Dance, G.J.X., LaForgia, M. and Confessore, N. 2018. As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants. *The New York Times.*

[22] David, B. 2018. Hard Questions: Should People Be Able to Share Their Facebook Information with Other Apps? *About Facebook.*

[23] Davis, A. 2018. Protecting People from Bullying and Harassment. *Facebook.*

[24] Davis, H. 2011. Discourse and Media Influence. *Discourse and Communication: New Approaches to the Analysis of Mass Media Discourse and Communication*. De Gruyter, Inc. 44–59.

[25] Dencik, L. and Cable, J. 2017. The advent of surveillance realism: public opinion and activist responses to the Snowden leaks. *International Journal of Communication.* 11, (Feb. 2017), 763–781.

[26] DeVito, M.A., Birnholtz, J., Hancock, J.T., French, M. and Liu, S. 2018. How People Form Folk Theories of Social Media Feeds and What it Means for How We Study Self-Presentation. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, Apr. 2018), 1–12.

[27] van Dijck, J. 2014. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society.* 12, 2 (May 2014), 197–208. DOI:https://doi.org/10.24908/ss.v12i2.4776.

[28] Dijck, J. van 2013. *The Culture of Connectivity: A Critical History of Social Media*. Oxford University Press.

[29] van Dijk, T.A. 1993. Analyzing racism through discourse analysis: Some methodological reflections. *Race and ethnicity in research methods*. Sage Publications, Inc. 92–134.

[30] van Dijk, T.A. 2006. Discourse and manipulation. *Discourse & Society*. 17, 3 (May 2006), 359–383. DOI:https://doi.org/10.1177/0957926506060250.
[31] van Dijk, T.A. 2008. *Discourse and Power*. Palgrave.
[32] van Dijk, T.A. 2010. Discourse, knowledge, power and politics. *Critical Discourse Studies in Context and Cognition*. John Benjamins.
[33] van Dijk, T.A. 2001. Multidisciplinary CDA: A Plea for Diversity. *Methods of Critical Discourse Analysis*. Sage. 95–120.
[34] Dourish, P. 2019. User experience as legitimacy trap. *Interactions*. XXV1.6 (2019), 46.
[35] Draper, N.R.A. 2012. Is Your Teen at Risk? Discourses of adolescent sexting in United States television news. *Journal of Children and Media*. 6, 2 (May 2012), 221–236. DOI:https://doi.org/10.1080/17482798.2011.587147.
[36] Duguay, S. 2016. "He has a way gayer Facebook than I do": Investigating sexual identity disclosure and context collapse on a social networking site. *New Media & Society*. 18, 6 (Jun. 2016), 891–907. DOI:https://doi.org/10.1177/1461444814549930.
[37] Dym, B. and Fiesler, C. 2018. Vulnerable and Online: Fandom's Case for Stronger Privacy Norms and Tools. *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing* (New York, NY, USA, 2018), 329–332.
[38] Eslami, M., Rickman, A., Vaccaro, K., Aleyasen, A., Vuong, A., Karahalios, K., Hamilton, K. and Sandvig, C. 2015. "I always assumed that I wasn't really that close to [her]": Reasoning about Invisible Algorithms in News Feeds. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (New York, NY, USA, Apr. 2015), 153–162.
[39] Facebook wants to help you do a privacy checkup: 2014. *https://money.cnn.com/2014/09/05/technology/social/facebook-privacy/index.html*. Accessed: 2020-07-24.
[40] Fairclough, N. 1995. *Critical Discourse Analysis*. Longman.
[41] Fisher, M. 2009. *Capitalist Realism: Is There No Alternative?*. Zero Books.
[42] Foucault, M. 1977. *Discipline & Punish: The Birth of the Prison*. Vintage Books.
[43] Gandy, O.H. 2017. Surveillance and the Formation of Public Policy. *Surveillance & Society Biennial Conference* (2017).
[44] Gillespie, T. 2010. The politics of 'platforms.' *New Media & Society*. 12, 3 (May 2010), 347–364. DOI:https://doi.org/10.1177/1461444809342738.
[45] Gillespie, T. 2014. The Relevance of Algorithms. *Media Technologies: Essays on Communication, Materiality, and Society*. MIT Press.
[46] Goldman, R. 2018. Hard Questions: What Information Do Facebook Advertisers Know About Me? *Facebook*.
[47] Haimson, O.L., Buss, J., Weinger, Z., Starks, D.L., Gorrell, D. and Baron, B.S. 2020. Trans Time: Safety, Privacy, and Content Warnings on a Transgender-Specific Social Media Site. *Proceedings of the ACM on Human-Computer Interaction*. 4, CSCW2 (Oct. 2020), 124:1-124:27. DOI:https://doi.org/10.1145/3415195.
[48] Haimson, O.L. and Hoffmann, A.L. 2016. Constructing and enforcing "authentic" identity online: Facebook, real names, and non-normative identities. *First Monday*. 21, 6 (Jun. 2016). DOI:https://doi.org/10.5210/fm.v21i6.6791.
[49] Hardy, J. and Lindtner, S. 2017. Constructing a Desiring User: Discourse, Rurality, and Design in Location-Based Social Networks. *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (New York, NY, USA, 2017), 13–25.
[50] Hargittai, E., Gruber, J., Djukaric, T., Fuchs, J. and Brombach, L. 2020. Black box measures? How to study people's algorithm skills. *Information, Communication & Society*. 23, 5 (Apr. 2020), 764–775. DOI:https://doi.org/10.1080/1369118X.2020.1713846.
[51] Hargittai, E. and Marwick, A. 2016. "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication*. 10, (2016), 3737–3757.
[52] Hoffmann, A.L., Proferes, N. and Zimmer, M. 2018. "Making the world more open and connected": Mark Zuckerberg and the discursive construction of Facebook and its users. *New Media & Society*. 20, 1 (Jan. 2018), 199–218. DOI:https://doi.org/10.1177/1461444816660784.
[53] Hull, G. 2015. Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data. *Ethics and Information Technology*. 17, 2 (2015), 89–101.
[54] Instagram founders fought with Zuck over Facebook integrations, says report: 2019. *https://www.theverge.com/2019/4/16/18410309/instagram-mike-krieger-kevin-systrom-cofounders-leave-facebook-mark-zuckerberg*. Accessed: 2020-07-23.
[55] Instagram's co-founder ignored suggestions to copy Snapchat's best feature before finally relenting: 2020. *https://www.cnbc.com/2020/04/08/instagrams-kevin-systrom-ignored-suggestions-to-copy-snapchat-stories.html*. Accessed: 2020-07-24.
[56] Jack, M.C., Sovannaroth, P. and Dell, N. 2019. "Privacy is not a concept, but a way of dealing with life": Localization of Transnational Technology Platforms and Liminal Privacy Practices in Cambodia. *Proceedings of*

the ACM on Human-Computer Interaction. 3, CSCW (Nov. 2019), 128:1-128:19. DOI:https://doi.org/10.1145/3359230.

[57] Jackson, S.J., Gillespie, T. and Payette, S. 2014. The Policy Knot: Re-integrating Policy, Practice and Design in CSCW Studies of Social Computing. *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing* (New York, NY, USA, 2014), 588–602.

[58] Karppi, T. and Nieborg, D.B. 2020. Facebook confessions: Corporate abdication and Silicon Valley dystopianism. *New Media & Society*. (Jun. 2020), 1461444820933549. DOI:https://doi.org/10.1177/1461444820933549.

[59] Keeping Instagram Safe: More Tools and Control: 2016. *https://about.instagram.com/blog/announcements/keeping-instagram-safe-with-more-tools-and-control*. Accessed: 2020-07-25.

[60] Kokolakis, S. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*. 64, (Jan. 2017), 122–134. DOI:https://doi.org/10.1016/j.cose.2015.07.002.

[61] Lampinen, A., Tamminen, S. and Oulasvirta, A. 2009. All My People Right Here, Right Now: Management of Group Co-presence on a Social Networking Site. *Proceedings of the ACM 2009 International Conference on Supporting Group Work* (New York, NY, USA, 2009), 281–290.

[62] Lewis, H. 2016. *The Politics of Everybody: Feminism, Queer Theory and Marxism at the Intersection*. Zed Books.

[63] Liu, Y., Gummadi, K.P., Krishnamurthy, B. and Mislove, A. 2011. Analyzing Facebook Privacy Settings: User Expectations vs. Reality. *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference* (New York, NY, USA, 2011), 61–70.

[64] Livingstone, S. 2008. Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New media & society*. 10, 3 (2008), 393–411.

[65] Lomas, N. 2020. Facebook data misuse and voter manipulation back in the frame with latest Cambridge Analytica leaks. *TechCrunch*.

[66] Lomas, N. 2019. Facebook denies making contradictory claims on Cambridge Analytica and other 'sketchy' apps. *TechCrunch*.

[67] Lutz, C., Hoffmann, C.P. and Ranzini, G. 2020. Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society*. 22, 7 (Jul. 2020), 1168–1187. DOI:https://doi.org/10.1177/1461444820912544.

[68] Marwick, A. 2012. The Public Domain: Surveillance in Everyday Life. *Surveillance & Society*. 9, 4 (Jun. 2012), 378–393.

[69] Marwick, A. and boyd, danah 2010. I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience. *New Media & Society*. (2010). DOI:https://doi.org/10.1177/1461444810365313.

[70] Marwick, A., Fontaine, C. and boyd, danah 2017. "Nobody Sees It, Nobody Gets Mad": Social Media, Privacy, and Personal Responsibility Among Low-SES Youth. *Social Media + Society*. 3, 2 (Apr. 2017).

[71] Matsakis, L. and Lapowsky, I. 2018. Everything We Know About Facebook's Massive Security Breach. *Wired*.

[72] McDonald, N. and Forte, A. 2020. The Politics of Privacy Theories: Moving from Norms to Vulnerabilities. *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems. CHI 2020* (2020).

[73] McGovern, A., Crofts, T., Lee, M. and Milivojevic, S. 2016. Media, legal and young people's discourses around sexting. *Global Studies of Childhood*. 6, 4 (Dec. 2016), 428–441. DOI:https://doi.org/10.1177/2043610616676028.

[74] Mulligan, D.K., Koopman, C. and Doty, N. 2016. Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*. 374, 2083 (Dec. 2016), 20160118. DOI:https://doi.org/10.1098/rsta.2016.0118.

[75] New: Updates to Verification and Authentication Tools | Instagram Blog: 2018. *https://about.instagram.com/blog/announcements/instagram-verification-and-authentication-tool-updates*. Accessed: 2020-07-24.

[76] Nissenbaum, H. 2009. *Privacy in context: technology, policy, and the integrity of social life*. Stanford Law Books.

[77] Page, X., Ghaiumy Anaraky, R., Knijnenburg, B.P. and Wisniewski, P.J. 2019. Pragmatic Tool vs. Relational Hindrance: Exploring Why Some Social Media Users Avoid Privacy Features. *Proceedings of the ACM on Human-Computer Interaction*. 3, CSCW (2019), 1–23.

[78] Pitcan, M., Marwick, A.E. and Boyd, D. 2018. Performing a Vanilla Self: Respectability Politics, Social Class, and the Digital World. *Journal of Computer-Mediated Communication*. 23, 3 (May 2018), 163–179. DOI:https://doi.org/10.1093/jcmc/zmy008.

[79] Popiel, P. 2019. Terms of public service: Framing mobile privacy discourses. *First Monday*. (Nov. 2019). DOI:https://doi.org/10.5210/fm.v24i11.10005.

[80] Proferes, N. 2017. Information Flow Solipsism in an Exploratory Study of Beliefs About Twitter. *Social Media + Society*. 3, 1 (Jan. 2017), 2056305117698493. DOI:https://doi.org/10.1177/2056305117698493.

[81] Protecting your Privacy: 2015. *https://www.snap.com/en-US/news/post/protecting-your-privacy*. Accessed: 2020-07-25.

[82] Rader, E. and Gray, R. 2015. Understanding User Beliefs About Algorithmic Curation in the Facebook News Feed. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (New York, NY, USA, Apr. 2015), 173–182.
[83] Rashidi, Y., Kapadia, A., Nippert-Eng, C. and Su, N.M. 2020. " It's easier than causing confrontation": Sanctioning Strategies to Maintain Social Norms and Privacy on Social Media. *Proceedings of the ACM on Human-Computer Interaction*. 4, CSCW1 (2020), 1–25.
[84] Schroeder, P. 2019. Facebook's Zuckerberg grilled in U.S. Congress on digital currency, privacy, elections. *Reuters*.
[85] Shaikh, R. 2018. Facebook Argues Why Users Should Continue Sharing Their Data. *Wccftech*.
[86] Singer, N. 2018. Why the F.T.C. Is Taking a New Look at Facebook Privacy. *The New York Times*.
[87] Stein, S.R. 2002. The "1984" Macintosh Ad: Cinematic Icons and Constitutive Rhetoric in the Launch of a New Machine. *Quarterly Journal of Speech*. 88, 2 (May 2002), 169–192. DOI:https://doi.org/10.1080/00335630209384369.
[88] Stern, S.R. and Odland, S.B. 2017. Constructing Dysfunction: News Coverage of Teenagers and Social Media. *Mass Communication and Society*. 20, 4 (Jul. 2017), 505–525. DOI:https://doi.org/10.1080/15205436.2016.1274765.
[89] Su, N.M. 2010. Street fighter IV: braggadocio off and on-line. (2010), 361–370.
[90] Temporary Social Media: 2013. *https://www.snap.com/en-US/news/post/temporary-social-media*. Accessed: 2020-07-25.
[91] The Liquid Self: 2013. *https://www.snap.com/en-US/news/post/the-liquid-self*. Accessed: 2020-07-24.
[92] Thompson, N. and Barrett, B. How Twitter Survived Its Biggest Hack--and Plans to Stop the Next One. *Wired*.
[93] Trepte, S. 2015. Social media, privacy, and self-disclosure: The turbulence caused by social media's affordances. *Social Media+ Society*. 1, 1 (2015), 2056305115578681.
[94] Tufekci, Z. 2014. Engineering the public: Big data, surveillance and computational politics. *First Monday*. 19, 7 (2014).
[95] Underwood, P. 2014. Privacy Checkup Is Now Rolling Out. *Facebook*.
[96] Updates That Foster a Safer, Kinder Community | Instagram Blog: 2017. *https://about.instagram.com/blog/announcements/updates-that-foster-a-safer-kinder-community*. Accessed: 2020-07-27.
[97] Vitak, J. and Kim, J. 2014. You can't block people offline: examining how Facebook's affordances shape the disclosure process. (2014), 461–474.
[98] Wagner, K. 2018. Snapchat is building the same kind of data-sharing API that just got Facebook into trouble. *Vox*.
[99] Wang, Y., Leon, P.G., Acquisti, A., Cranor, L.F., Forget, A. and Sadeh, N. 2014. A field trial of privacy nudges for facebook. (2014), 2367–2376.
[100] West, S.M. 2019. Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*. 58, 1 (Jan. 2019), 20–41. DOI:https://doi.org/10.1177/0007650317718185.
[101] Westin, A.F. 1967. *Privacy and Freedom*. Atheneum.
[102] Xu, B., Chang, P., Welker, C.L., Bazarova, N.N. and Cosley, D. 2016. Automatic Archiving Versus Default Deletion: What Snapchat Tells Us About Ephemerality in Design. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (New York, NY, USA, 2016), 1662–1675.
[103] Zuboff, S. 2015. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*. 30, 1 (Mar. 2015), 75–89.
[104] Zuboff, S. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

Received January 2021; revised April 2021; accepted July 2021.