Journal of Public Interest Communications

ISSN (online): 2573-4342

Is Privacy Dead? Does it Matter? How Facebook Frames its Data Policy Through Public Communication

Brandon C. Boatwright, Candace White

Clemson University, University of Tennessee

Article Information

Received: June 10, 2019

Accepted: January 13, 2020

Published online: May 22, 2020

Keywords

Data privacy
Framing
Public policy
Corporate social responsibility
Public communication

Abstract

Facebook is the largest social media company in the world. The corporation holds vast amounts of data that provide artificial intelligence about attitudes and behaviors of 1.6 billon users throughout the world. The current study analyzes Facebook's public communication regarding data collection and privacy to better understand how the company frames its message strategy, which affects user understanding. As calls for oversight and legislation of data privacy continue to surface, this study explores how Facebook defines *data* and how it frames its data policy through public communication. Results show Facebook addresses *what* data the company collects but fails to provide sufficient clarity explaining how data is stored or used. It frames its privacy policy in terms that benefit users without explanation of its business model.

Introduction

As the CEO of Facebook, Mark Zuckerberg has said that "privacy is no longer a 'social norm'" (Osnos, 2018, para. 50). Today, consumer data are continuously collected by social media and other Internet companies in ways that differ dramatically from the ways data from individuals have been traditionally collected, often without the knowledge, understanding, or agreement on the part of the people from whom the data are collected. Furthermore, such data collection is not subject to any substantive regulatory oversight in the United States. Super computers owned by private-sector companies allow for the collection, storage, and analysis of vast quantities of

**Please send correspondences about this article to Brandon Boatwright, Department of Communication, Clemson University. E-mail: boatwrightbc10@gmail.com.*

https://doi.org/10.32473/jpic.v4.i1.p78

information, known as big data, that are harvested and analyzed to develop predictive algorithms that are used for a variety of purposes that include psychological manipulation and social engineering (c.f., Ward, 2018). In the past, the right to privacy was associated with government as the invader of privacy. However, today people accept continuous corporate surveillance down to a person's physical location, even though they would never accept this level of surveillance from a government. Why do we reject mass government surveillance but agree to corporate surveillance?

The indifference of users who are willing to give up details of their private life and their rights to privacy in exchange for a platform to communicate with their friends, acquaintances, and bots is somewhat of a paradox in democratic countries where individual freedom and constitutional rights to privacy have been traditional values. The continuous surveillance that an average Internet user is subjected to daily has become an accepted cost of doing business. However, social media users may *not* be completely indifferent to privacy as a social norm, but rather may be unaware of how their privacy is invaded and at what costs.

Facebook's privacy policy offers users very little privacy, but most users have never actually read the policy. Lilley et al. (2012) surveyed more than 500 Facebook users and found most participants in their study were ignorant of the company's data sharing and selling practices. However, when they were told how Facebook uses their data, the majority of participants opposed such practices. According to a 2018 survey by the Pew Research Center, 74 percent of Facebook users did not know that Facebook collects information about them and maintains a list of their interests and traits to sell to advertisers. When directed to their list of interests and traits, 51 percent said they were not comfortable with Facebook maintaining this kind of list (as cited in Smith, 2019).

Most Facebook users have not read the privacy policy because it is difficult to find. Facebook users are instead presented with simplified bullets of the most benign parts of the policy along with a clickwrap for them to agree. Clickwraps are digital prompts that allow users to agree to privacy policies without seeing them. Obar and Oeldorf-Hirsch (2018) found that clickwraps facilitated circumvention of consent policies, allowing social media companies to manufacture consent by making it possible to consent to a privacy policy without seeing a single word of it on screen. However, from a legal standpoint clicking Agree means users opt in to Facebook's data policy and provides proof that they have read and understood the policy in its entirety. Zeadally and Winkler (2016) found Facebook's full privacy policy is not only difficult to access, but also difficult to understand. Their analysis of readability concluded that over half the population of users cannot understand what they are agreeing to when they sign up for an account (assuming they actually read it). The site changes its terms and conditions regularly, usually in response to complaints or controversy, often making the terms and conditions more complex and harder to access so most users do not understand how their personal information can be used.

Concerns over Facebook's policies and use of personal data are increasing. A national NBC News/*Wall Street Journal* poll found that 60 percent of Americans do not trust Facebook with their personal information (as cited in Grothaus, 2019). Consequently, social media users have taken steps to curtail the types and amount of data they share with the platform (e.g., clearing cookies and limiting the amount of information they share), but nearly one-third of U.S. Internet users are still willing to sacrifice privacy for the sake of convenience (Droesch, 2019). Despite attempts to clarify its advertising transparency on the platform, Facebook's "ad explanations are often incomplete and sometimes misleading while data explanations are often incomplete and vague" (Andreou et al., 2018, p. 1). The lack of transparency has significant implications for public interest communications as users, advertisers, and policy makers are left to blindly navigate an ethical minefield. This study examines how Facebook frames its messages about privacy to the general public and looks critically at the consequences—intended and unintended—of Facebook's corporate business model and data collection practices.

The environment of unregulated social media surveillance

Facebook's business model is the extraction of data to sell, harvested through vast data surveillance, the results of which fuel an opaque system of microtargeting for the purpose of social engineering to affect behaviors and attitudes (Tufekci, 2018). A 2017 article in *The Economist* made a compelling argument that data has superseded oil as the world's most valuable commodity. Alphabet (Google's parent company), Amazon, Apple, Facebook, and Microsoft "collectively racked up over $25 billion in the first quarter of 2017" (*The Economist*, 2017, para. 1, emphasis added). Advances in technology, complex data-scraping algorithms, and loose privacy restrictions have created a data economy through which companies like Facebook have derived entire profit models. In its most basic form, the data economy is a marketplace in which users' personal information is first translated into an array of data points that then are brokered by third parties for targeted advertisements in exchange for vast sums of money (Wood, 2018). Constantiou and Kallinikos (2014) noted that "such data are acquired, abstracted, aggregated, analyzed, packaged, sold, further analyzed and sold again" (p. 85) for large profits for those who collect it. Facebook monetizes data by profiling users and selling their attention based on algorithms that can infer personality traits, sexual orientation, political views, mental health status, substance abuse history, and more, just from Facebook likes (Tufekci, 2018). From its inception, the process through which data are created, collected, and shared in the data economy has proven difficult to understand.

In 2014, the U.S. Federal Trade Commission (FTC) issued a report calling for congressional legislation requiring greater transparency and accountability of data brokers. The report found:

> Data brokers collect and store billions of data elements covering nearly every U.S. consumer. Just one of the data brokers studied held information on more than 1.4 billion consumer transactions and 700 billion data elements and another adds more than 3 billion new data points to its database each month. (FTC, para. 4, 2014)

It is important to note that data collection does not begin and end on social media. For example, McFarland (2017) reported that by 2020, car manufacturers will make more money off the sale of a driver's data than from the sale of the actual vehicle. Nevertheless, social media platforms remain the focus of this study because of the sheer volume of information the average user provides to platforms like Facebook.

Zuboff (2015) referred to the collecting and selling of personal data as "surveillance capitalism," which she defined as a "new form of information capitalism that aims to predict and modify human behavior as a means to produce revenue and market control" (p. 75). She noted that surveillance capitalism is immune to the traditional reciprocities between customers and capitalists. Facebook customers, advertisers, and third-party data brokers are the entities to which Facebook sells data. Facebook users are the company's product since they are the targets of data extraction and collection.

Multiple reports suggest that Facebook has the capacity to both (1) collect greater swaths of personal information that users do not directly provide themselves and (2) distribute that information to various buyers. A 2018 report in *The Wall Street Journal* found that Facebook had struck customized data-sharing deals that gave select companies (e.g., Nissan and RBC Capital Markets) "special access to user records well after the point in 2015 that the social network has said it walled off that information" (Seetharaman & Grind, 2018, para. 1). Additional reports released in February 2019 suggested that Facebook partnered with various smartphone applications to collect sensitive personal data. These included Flo Period and Ovulation Tracker, "which reportedly shared with Facebook when users were having their periods or when they were trying to become pregnant" (Doward & Soni, 2018, para. 6). According to *Financial Times'* personal data calculator, knowing whether or not a user is expecting a child roughly equates to nine cents of the user's personal data value (Steel et al., 2013). Importantly, a separate *Wall Street Journal* report found that Facebook can receive information from numerous apps even if the user does not have a Facebook account (as cited in Schechner, 2019).

Beyond partnering with and sharing content among various third parties, Facebook has demonstrated an unrivaled capacity to collect data on its own. To its credit, the platform has enabled a Download Your Data feature that allows users the ability to download and review information they have posted to Facebook. However, a *Wired* report found that the feature hardly tells users everything Facebook knows about them. Among the information not included is:

> information Facebook collects about your browsing history, information Facebook collects about the apps you visit and your activity within those apps, the advertisers who uploaded your contact information to Facebook more than two months earlier, and ads that you interacted with more than two months prior. (as cited in Tiku, 2018, para. 4)

Corporate surveillance, algorithms, and microtargeting

In his book *Zucked: Waking up to the Facebook Catastrophe*, Roger McNamee, a former Facebook investor and mentor to Zuckerberg, posited that "the value is not really in the photos and links posted by users. The real value resides in metadata—data about data—which is what we call the data that describes where the user was when he or she posted, what they were doing, with whom they were doing it…and more" (McNamee, 2019, p. 68). An investigation by ProPublica identified more than 52,000 unique attributes that Facebook has to classify users (Agnwin et al., 2016). Further demonstrating the extent to which Facebook seeks to obtain user information, the company filed patents in 2014 and 2015 for a technique that employs smartphone data to figure out if two people might know each other through metadata attached to the phone's camera including, for example, "if lens scratches or dust were detectable in the same spots on photos, revealing the photos were taken by the same camera" (Hill & Mattu, 2018, para. 6).

Every Facebook like, search, video, purchase, page view, etc., including the location of the user at the time, are captured from Facebook users even when they are not logged on to Facebook and aggregated to constitute big data. Since small data points are inconsequential and seemingly insignificant in their everydayness (Constantiou & Kallinikos, 2014), most social media users are unconcerned with and unaware of the purpose of the data collection. However, when small data are aggregated, predictive patterns are revealed that can be used to micro-target identifiable individual users with granular precision. It becomes possible to construct detailed individual psychological profiles and predictive algorithms that can produce patterns-of-life analysis and observation of behavior that was previously unobservable (Constantiou & Kallinikos, 2014).

Buhmann et al. (2020) noted that algorithms have repeatedly had intentional and unintentional negative consequences. Algorithms are used intentionally as organizational intelligence for strategy development and managerial decision making by many corporations (Markus, 2015). Although big data benefit corporations, big data can have negative consequences at the individual level based on the way the data are used for profits. Grocery store chains, for example, collect data when shoppers use customer cards, but the data are used primarily to target customers with coupons or as intelligence to determine which items to stock since profits come from the sale of food. Facebook, on the other hand, makes all of its profits by selling data to external third-party data brokers and companies, which can include political parties or quasi-governmental organizations in other countries. Such data can be used for purposes of social engineering and behavioral modification by affecting attitudes and behaviors (Frontline, 2018). For example, data sold to insurance companies can be used to produce algorithms to predict the likelihood of contracting diseases or having accidents (to decide who not to insure) or by employers to predict absenteeism, propensity for addiction problems, or to determine religious beliefs, political leanings, sexual orientation, or ethnicity (questions that companies cannot legally ask otherwise) (Silverman & Waller, 2015). Algorithmic microtargeting also has been used to affect election outcomes, in what Osnos (2018) refers to as a threat to democracy.

Perhaps the most widely publicized instance of data collected through Facebook stems from the Cambridge Analytica breach. Cambridge Analytica, a political data firm hired by Donald Trump’s 2016 election campaign, “gained access to private information on more than 50 million Facebook users” (Granville, 2018, para. 2) in order to provide the campaign with micro-targeted advertisements based on users’ personality traits (Ward, 2018). In response, Zuckerberg posted an update on the platform several days after news of the breach broke, writing in part: “We have a responsibility to protect your data, and if we can’t then we don’t deserve to serve you” (Zuckerberg, 2018, para. 2). These comments, however, not only call into question the definition of the word *data* as Zuckerberg describes it, but also of the word *breach*. On the surface, it appears that Zuckerberg’s definition of data refers to the information that users voluntarily post on Facebook (i.e., demographic information, job titles, relationships status, photographs, etc.), but does not account for information that Facebook collects based on metadata including users’ network connections, online behavior, or psychographic profiles, for example. Facebook would have *sold* the data to Cambridge Analytica, which describes itself as a global election management agency, just as it sold data directly to the Trump campaign for the same purpose. Such a disconnect is problematic in that it distorts public perceptions about what actually constitutes personal information and, consequently, data privacy. It is likely that, having never read Facebook’s policies in their entirety, many users believe Facebook’s misleading claims that the corporation protects personal information.

The right to privacy

In the United States, the legal definition of personal information is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context (Schwartz & Solove, 2014). It is generally assumed that individuals have the right to control the use of their personal data, and a number of U.S. laws protect the personal information of citizens. However, when a person agrees to Facebook’s policy, he or she is agreeing to accept a different definition of personal information as defined by Facebook, relinquishing other legal protection. What little privacy the Facebook policy affords is in regard to what other Facebook users can see. Facebook sees, owns, and stores all of it. Social media companies obscure their operations in complex legalese, including how they use personal information, to whom it can be transferred, and how it is used by other companies. Schwartz and Solove (2014) purported that such policies have been allowed to stand because they, and the technological advances behind them, have moved at such a high velocity that few people outside a small number of experts understand their meaning. Privacy laws threaten surveillance capitalism.

There are no overarching privacy laws in the United States that apply to corporate data (Schwartz & Solove, 2014). Corporate super computers allow personal information to be stored indefinitely and used for purposes not yet discovered. Millions of data points are collected without a specific purpose and warehoused in case they become useful later (Zuboff, 2015). Facebook stores this information for "as long as it is necessary to provide products and services to you and others" (11, para. 29, Facebook policy). Tufekci (2018) noted that Facebook can store information indefinitely since the company decides how long it is necessary to keep the data. New technologies, such as facial recognition algorithms, and applications for data are discovered and implemented every day. Facebook users cannot control what is done with their data now or in perpetuity. Facebook has publicly defended its data policy and procedures, citing the fact that users opt in to the platform's terms and conditions, which will be discussed in later sections of this paper.

Facebook has faced public scrutiny over its data collection and privacy policies. In April 2018, the U.S. Congress called Zuckerberg to testify before the Senate Commerce and Judiciary committees on topics including privacy, data mining, and regulation. After fielding questions during the hearing, Zuckerberg and Facebook's newsroom were quick to articulate new privacy initiatives that purported to give users greater control over their data and assured increased transparency in its data collection processes. However, the new initiatives only gave users control over what other users see. In February 2019, Senator Elizabeth Warren called Facebook, Google, and Amazon monopolies for abusing their dominant position in the marketplace and suggested in a political advertisement posted on Facebook they be broken up. Consequently, Facebook removed the series of advertisements from its platform but later reversed its decision saying the company wanted to allow robust debate (Lima, 2019).

There is some indication that the public is becoming aware of some of the pitfalls of social media use and that policy makers may be becoming aware of the need for a regulatory response in the United States, as has already happened in Europe with the introduction of the GDPR.[1] Burrell (2016) noted that the word algorithm has shifted from an obscure technical term used by computer scientists to one used increasingly in mainstream media, often attached to a polarized discourse. In a joint letter from the Electronic Privacy Information Center and the Center for Digital Democracy to the FTC, they said, "Neither Facebook's Data Use Policy nor its Statement of Rights and Responsibilities adequately explains the specific types of information Facebook discloses, the manner in which the disclosure occurs, or the identities of the third parties receiving the information" (Lee, 2012, para. 3). Politicians have begun to call for the break-up of social media monopolies, particularly Facebook. The Pew Research Center's latest report on public perceptions of privacy indicates that 91 percent of U.S. adults agree or strongly agree that consumers have lost control over their personal data (Madden, 2014).

[1] The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU) that went into effect May 25, 2018.

However, the same Pew survey found that 55 percent of the participants agree or strongly agree that they are willing to share some information about themselves with companies in order to use online services for free (as cited in Madden, 2014). People want to use social media and until recently, most people have viewed social media companies positively without questioning their policies. As Zuboff (2015) observed:

> Individuals quickly came to depend upon the new information and communication tools as necessary resources in the increasingly stressful, competitive, and stratified struggle for effective life. The new tools, networks, apps, platforms, and media thus became requirements for social participation. (p. 85)

It is difficult for social media users to see past the advantages of quick and easy communication and look behind the curtain at how billions of dollars in revenue are derived from data mining and data brokerage and how these practices affect their lives.

Rationale for the study

Facebook is the largest social media company, valued at more than $560 billion (MacroTrends.net). The corporation holds vast amounts of data that provide artificial intelligence about attitudes and behaviors of 1.6 billon users throughout the world. Zuckerberg himself has explained that “there’s no question that we collect some information for ads—but that information is generally important for security and operating our services as well” (Zuckerberg, 2019, para. 12). To be clear, although Facebook “primarily makes money by selling advertising space on its various social-media platforms” (Johnston, 2019, para. 1), its ability to sell advertising space in the first place is predicated on the accumulation and analysis of data about people (Amnesty International, 2019). In other words, advertising space on Facebook would be worth far less without the amount of information it has on users in order to assure buyers that messages would definitively reach their intended audience. So, although it is technically true that Facebook earns revenue by selling advertising space, we argue that the public is not provided with sufficient information with regard to how its personal data are used in the process.

This is problematic when positioned within the context of corporate public interest. Holland et al. (2018), in writing about the use of clarity, disclosure, and accuracy in organizational messages, noted that communication can be technically truthful but present incomplete or otherwise poorly framed information resulting in harm to an organization’s credibility and transparency. The authors noted that message transparency includes clarity, avoiding jargon or legal definitions, as well as easy access, and that technically correct, truthful information has the potential to be undermined by the omission of key information. “Taken together, clarity, disclosure, and accuracy can be used to determine the level of transparency within a given organizational message through the inclusion of precise, truthful information that message receivers need to make informed decisions or form unbiased perceptions” (Holland et al., 2018, p. 258).

Extant literature in the area of corporate public interest suggests that openness and transparency are integral attributes to corporate social responsibility (Hoertz Badracco, 1998; Rawlins, 2008; Schnackenberg & Tomlinson, 2016). Lerbinger (2006) argued that openness is a critical component of corporate public affairs. He wrote:

> An open organization is permeable; it interacts with its environment at many points along its boundary with society. It is ready to listen to stakeholders, include their concerns in decision making, and sometimes involve them in coalitions and collaborative decision making. In contrast, a closed system is like a fortress, recognizing its interactions with society only through the economic marketplaces for necessary inputs (e.g., factors of production) and outputs (of its products and services). (pp. 15-16)

The current study analyzes Facebook's public communication regarding data collection and privacy to better understand how the company frames its message strategy, which affects user understanding and, thus, the public interest. As calls for oversight and legislation on the topic of data privacy continue to surface, this study poses two research questions in an effort to comprehend how Facebook defines data and how it frames its data policy through public communication:

RQ1: How does Facebook define data through its public newsroom?

RQ2: How does Facebook frame its data policy through its public newsroom?

Method

Sample

In total, 44 topically relevant posts from Facebook's online newsroom (www.newsroom.fb.com) were selected and downloaded for analysis. Newsroom posts were chosen for analysis because they are the organization's primary means to provide strategic, controlled messaging directly to the public without the influence of external pressures such as pointed questions during Congressional hearings or televised interviews. As such, newsroom posts were considered to be more measured accounts of Facebook's organizational framing.

Data collection began with a post on March 16, 2018, explaining Facebook's decision to suspend Cambridge Analytica and Strategic Communication Laboratories (SCL) from the platform and continued through March 6, 2019, when Zuckerberg outlined a vision for privacy focused social networking. These beginning and end dates were chosen in order to capture an entire year's worth of public communication efforts on behalf of Facebook during the height of its data privacy scandal. During that span, the authors' sampling strategy was guided by identifying topically relevant posts that contained clear, in-text references to "data use," "personal information," "transparency," and "privacy."

Data analysis

Thematic analysis was used to examine Facebook's public communication efforts through the company's newsroom. Braun and Clarke (2012) define thematic analysis as "a method for systematically identifying, organizing, and offering insight into patterns of meaning (themes) across a dataset" (p. 57). This method of analysis allowed for an in-depth description of patterns within the data to be identified. Thematic analysis was conducted in six phases summarized below in Table 1, adapted from Braun and Clark (2006).

Table 1

Phases of thematic analysis, adapted from Braun and Clark (2006)

Phase	Description of the Process
1. Familiarization with the data	Once collected, authors read and re-read the releases from Facebook, noting initial ideas for coding.
2. Generating initial codes	Authors coded interesting features of the releases in a systematic fashion across the entire dataset, collating data relevant to each code.
3. Searching for themes	Using the list of codes developed in Phase 2, authors re-focused the analysis to a broader level of themes of organized codes.
4. Reviewing themes	Authors refined themes to ensure data within themes cohered together meaningfully, and that there were clear and identifiable distinctions between themes.
5. Defining and naming themes	Authors clarified the 'essence' of each theme, and finalized versions were developed based around author agreement on what the themes were and what they were not.
6. Producing the report	Analysis was written to provide a concise, coherent, logical, and interesting account of the story the data tell.

An essentialist/realist framework (Braun & Clarke, 2006) for a data-driven thematic analysis was used. Under an essentialist/realist framework, thematic analysis can be used as a tool to explore how "events, realities, meanings, experiences, and so on are the effects of a range of discourses operating within society" (Braun & Clarke, 2006, p. 81). Operating under this framework, themes could be directly derived from the original data, and a unique coding framework in relation to Facebook's definition of data and its framing of the company's data policy could be developed. Van den Bogaert et al. (2018) adopted a similar framework in examining press releases of the four largest pharmaceutical companies in Belgium and the industry's trade association. Posts to Facebook's newsroom were read several times by both authors to ensure thorough comprehension. Patterns within the data were coded by the researchers and extracts from the original data were assembled into non-overlapping themes. They were compared to the original posts and further refined to ensure that data within the themes cohered together meaningfully, and that there were clear and identifiable distinctions among themes.

Results

In identifying themes present in the company's online news releases, a three-part framework was adopted from Ward's (2018) position that there are three aspects of information privacy: (1) data collection, (2) storage, and (3) use. In its releases, Facebook primarily addresses *what* data the company collects but ultimately seems to fail to provide sufficient clarity explaining how data are stored or used. Facebook frames its privacy policy in terms that benefit users without any explanation of its business model.

How does Facebook define data?

In a published transcript of a media interview with Zuckerberg, CBS News correspondent Nancy Cortez posed a question seeking greater clarity on Facebook's data collection process: "Your critics say, look, Facebook's model, Facebook's business model, depends on harvesting personal data. How can you ever personally assure users that their data won't be used in ways they don't expect?" Zuckerberg responded using what appears to be a consistent message in Facebook's definition of data—that the platform collects information that users voluntarily provide on the platform:

> I think we can certainly do a better job of explaining what we actually do. There are many misconceptions around what we do that I think we haven't succeeded in clearing up for years. So, first, the vast majority of data that Facebook knows about you is because you chose to share it. Right? There are other Internet companies or data brokers or folks that might try to track and sell data, but we don't buy and sell. In terms of the ad activity, I mean that's a relatively smaller part of what we're doing. The majority of the activity is people actually sharing information on Facebook, which is why people understand how much content is there, because people put all the photos and information there themselves.

This portion of Zuckerberg's response is emblematic of Facebook's double speak in defining data collection in a way that does not really explain it and ultimately places the burden of privacy on the user. His response does not paint a complete picture describing the process Facebook uses to extract data about more substantive data points such as users' behavior on the platform and metadata, nor does his answer provide any substantive explanation for what Facebook actually collects.

In a separate release on April 23, 2018, Rob Goldman (VP of Ads at Facebook) suggested that the company collects information from things the user *chooses* to share like age, gender, hometown, and friends. Goldman also pointed out that Facebook gathers information based on what users click, and the posts, pages, or articles they like. Consequently, newsroom releases suggest that Facebook is only collecting that which its users *voluntarily* share thereby absolving itself while placing the burden of privacy on the user.

Zuckerberg's second half of his response to Cortez's question framed the company's *use* of data as a way to benefit the user:

> The second point, which I touched on briefly there: for some reason we haven't been able to kick this notion for years that people think we sell data to advertisers. We don't. That's not been a thing that we do. Actually, it just goes counter to our own incentives. Even if we wanted to do that, it just wouldn't make sense to do that. So, I think we can certainly do a better job of explaining this and making it understandable, but the reality is the way we run the service is: people share information, we use that to help people connect and to make the services better, and we run ads to make it a free service that everyone in the world can afford.

Facebook does not sell the inconsequential, everyday points of data, which are worthless without aggregation and analysis. The concept of data use here is positioned as a benefit to Facebook users. This notion is repeated consistently throughout several of the newsroom releases selected for this study.

In an April 17, 2018 release, Erin Egan (VP & Chief Privacy Officer) and Ashlie Beringer (VP & Deputy General Counsel) suggested, "Ads on Facebook are more relevant" (para. 3) to the consumer based on data Facebook uses and that the platform's facial recognition software features "help protect your privacy and improve your experiences, like detecting when others might be attempting to use your image as their profile picture and allowing us to suggest friends you may want to tag in photos or videos" (para. 5). In the same April 23 post by Goldman, he suggested, "We use this information to give you a better service…Data also helps us show you better and more relevant ads" (para. 12). Moreover, Goldman suggested that these data uses benefit small businesses that otherwise may not be able to compete with larger organizations: "Data lets a coffee shop survive and grow amid larger competitors by showing ads to customers in its area. And it lets a non-profit promote a diabetes fundraiser to those interested in the cause" (para. 14). Of course, Facebook algorithms can predict which users have diabetes. Goldman evades the issue of what the company sells, which is the artificial intelligence that is developed *from* the data.

With regard to storage, few releases address how long Facebook keeps data but several outline ways for users to exert greater control over the company's storage of data. In a March 28, 2018, release on making Facebook's privacy tools easier to find, Egan and Beringer asserted, "It's one thing to have a policy explaining what data we collect and use, but it's even more useful when people see and manage their own information" (para. 8). This announcement introduced Facebook's Access Your Information tool that purportedly offered users a secure way to access and manage information, such as posts, reactions, comments, and searches. But the company provided minimal clarity with regard to how long data are actually stored. In a March 6, 2019, release, Zuckerberg raised the idea of reducing data permanence but does so under ambiguous terms:

> People should be comfortable being themselves and should not have to worry about what they share coming back to hurt them later. So, we won't keep messages or stories around for longer than necessary to deliver the service or longer than people want them. (para. 10)

However, Zuckerberg offered no clarification for what *longer than necessary* means.

In sum, releases from Facebook's online newsroom offer a narrow definition of data that provides limited clarity with regard to the company's data collection procedures and little to no information about storage and use. The contextual definition of data in the releases is the everyday posts, likes, etc., that have no value to the company. The overall tone is one of reassurance, and the overall message is that users have nothing to worry about.

Framing Facebook's data policy

Three themes emerged in the analysis that illustrate how Facebook frames its data policy: (1) Facebook establishes privacy and data collection as a salient issue facing the company; (2) it places user experience at the center of its rationale for data collection; and (3) the online news releases are strategically ambiguous with regard to how data are collected, stored, and used.

Establishing issue salience

In the March 16, 2018, release in which Facebook announces that it banned Cambridge Analytica and SCL Group from the platform, the company contended that "protecting people's information is at the heart of everything we do, and we require the same from people who operate apps on Facebook" (para. 1). Throughout the study period, news releases on Facebook's online newsroom make data privacy a salient issue facing the company. Several posts affirm the company's responsibility and accountability with regard to protecting user data and providing greater transparency in its operations. In a post on March 21, 2018, Zuckerberg wrote:

> We have a responsibility to protect your data, and if we can't then we don't deserve to serve you…I started Facebook, and at the end of the day I'm responsible for what happens on our platform. I'm serious about doing what it takes to protect our community. While the specific issue involving Cambridge Analytica should no longer happen with new apps today, that doesn't change what happened in the past. We will learn from this experience to secure our platform further and make our community safer for everyone going forward.

The fallout from Cambridge Analytica prompted Facebook to post about updates to its data policy several times over the course of the year. On April 4, 2018, Egan and Beringer authored a release, "We're Making Our Terms and Data Policy Clearer, Without New Rights to Use Your Data on Facebook." In it, they outlined updates following Cambridge Analytica that were intended to provide greater clarity on the platform's privacy standards including new features and tools, information about what the company shares, advertising, and device information, among others.

Subsequent releases included references to data privacy as the most important topic at Facebook. The company announced plans to crack down on platform abuse, launched a new initiative to help scholars assess social media's impact on elections, created a data abuse bounty program, and published a series of transparency reports to further establish the idea that the company was taking this topic seriously.

Several releases addressed Facebook's preparation for and compliance with the European Union's GDPR. An April 17, 2018 release, for example, said:

> As soon as GDPR was finalized, we realized it was an opportunity to invest even more heavily in privacy. We not only want to comply with the law, but also go beyond our obligations to build new and improved privacy experiences for everyone on Facebook. We've brought together hundreds of employees across product, engineering, legal, policy, design and research teams. We've also sought input from people outside Facebook with different perspectives on privacy, including people who use our services, regulators and government officials, privacy experts, and designers. (para. 2)

Four outside opinions came in the form of a series of guest posts by thought leaders in the industry and in the academy. Former FTC Chairman Terrell McSweeny, for example, wrote: "Privacy is a crucial aspect of consumer rights in the digital age—and openness is another. The right balance will be found in policies that give users meaningful control over their digital identities but that also foster competition and innovation." In sharing each of the guest posts, Facebook demonstrated its commitment to bringing outside voices into the decision-making process.

Moreover, many of the releases selected during this span concluded with the author of the release asserting that Facebook is committed to doing more to ensure public trust in the organization's efforts. By establishing data privacy as a salient issue with the organization, Facebook positioned its data policy as a sincere, thoughtful effort to address its shortfalls. The company turned the Cambridge Analytica breach, through which the company lost potential revenue, into an opportunity to reassure users without explaining what the company was really protecting.

User experience

While maintaining that data privacy is a salient issue that requires significant improvement, Facebook's online news releases simultaneously worked to establish data collection, use, and storage as integral to the user experience and advertiser success. In a July 26, 2018 post, David Baser (Director of Product Management) defended the process of information sharing across platforms that Facebook relies upon:

> Some of the world's most popular apps have been built on the Facebook Platform—it's helped great ideas get off the ground and simplified and streamlined people's digital lives. But we know that this flow of information has the potential for abuse. Bad actors can gather information from people and use it in ways that they aren't aware of and didn't agree to. Facebook has clear policies against this, but as we saw with the Cambridge Analytica situation, bad actors are more than willing to ignore these policies in pursuit of their own objectives. Some argue that the best response to Cambridge Analytica would be to lock Facebook down completely so apps can't get access to this kind of information. But limiting people's ability to share information would erase the conveniences we enjoy. (paras. 3-4)

This post suggests two things. First, Facebook's data policy has clear benefits to its users. By collecting and harvesting data about interests, political affiliation, religion, sexual orientation, relationship status and the like, Facebook is better suited to provide users with tailored content. What the company does not explain is that much of the tailored content is sponsored advertisements. In response to a reporter from Buzzfeed during the April 4 Q&A session with the media, Zuckerberg stated,

> People tell us that if they're going to see ads, they want the ads to be good. And the way to make the ads good, is by making it so that when someone tells us they have an interest, they like technology or they like skiing or whatever it is they like, that the ads are actually tailored to what they care about.

Overall, the tone of the message appears to imply a balance between giving users control over data sharing and preventing abuse without hampering the Facebook experience.

Second, Baser's post suggests that data misuse happens because bad actors ignore Facebook policies and breach the platform's trust. As such, Facebook is not the guilty party. Rather, these bad actors (i.e. Cambridge Analytica, SCL, Six4Three) abuse the system making Facebook just as much a victim as its users. The implication here is that if everyone plays by the rules, Facebook can provide countless benefits through its data policy.

Benefits do not extend only to users, however. Several releases emphasize the utility of data collection, use, and storage to advertisers and designers. A June 28, 2018, release, for example, suggested, "The vast majority of ads on Facebook are run by legitimate organizations—whether it's a small business looking for new customers, an advocacy group raising money for their cause, or a politician running for office" (para. 5). Similarly, a July 31, 2018, release suggested that changes in Facebook's data policy "ensure that we better protect people's Facebook information while also enabling developers to build great social experiences—like managing a group, planning a trip, or getting concert tickets for your favorite band" (para. 4). These releases function to make the role of advertisers on Facebook more palatable to the company's users. The logic appears to be that if advertisers and developers can make the user's experience better, continued data collection, use, and storage are warranted.

Strategic ambiguity

Although establishing the salience of data privacy as an issue and bolstering the user experience appear to be noble efforts on the company's part, the language used in the releases appears to be strategically ambiguous so as to allow greater discrepancy and legal wiggle room for Facebook to operate.

In Baser's April 16 release, he wrote: "Whether it's information from apps and websites, or information you share with other people on Facebook, we want to put you in control—and be transparent about what information Facebook has and how it is used" (para. 26). But although Facebook continues to suggest that the company is affirming its commitment to transparency, many of the releases contain language that appears to intentionally withhold or manipulate information that may be necessary to fully understand the subject of the post. For instance, several releases refer to the platform's strict restrictions on how its partners can use and disclose data. Nowhere, however, does the company explain what those restrictions entail. A May 14, 2018, release by Ime Archibong on Facebook's application audit suggested, "To date thousands of apps have been investigated and around 200 have been suspended—pending a thorough investigation into whether they did in fact misuse any data" (para. 4). Again, a description of what constitutes the misuse of data is conspicuously absent.

Perhaps the most obvious example of this theme emerged through the company's ardent defense that it does not sell data to advertisers. In several cases, the author(s) of the releases suggest that Facebook *never* sells data to advertisers. Zuckerberg staunchly defended this position in the aforementioned media conference call. His response to a question posed by Carlos Hernandez, a reporter for Expansión (a Spanish economic and business newspaper), reinforces this notion. Hernandez asked:

> You mentioned one of the main important things about Facebook is people…and users' understanding of the platform. Do you have any plans to let users know how their data is being used? Not just on Facebook but also on Instagram and other platforms that you are responsible for?

Zuckerberg responded:

> I think we need to do a better job of explaining principles that the service operates under, but the main principles are, you have control over everything you put on the service, and most of the content Facebook knows about you is because you chose to share that content with your friends and put it on your profile. And we're going to use data to make those services better, whether that's ranking News Feed, or ads, or search, or helping you connect with people through people you may know, but we're never going to sell your information. And I think if we can get to a place where we can communicate that in a way that people can understand it, then I think we have a shot of

> distilling this down to something, to a simpler thing, but that's certainly not something we have succeeded at doing historically.

Zuckerberg readily admits that the company has failed to offer an acceptable degree of clarity with regard to how its process for data collection, use, and storage works. He acknowledges that there is a need for this, and yet offers no substantive response to the question. Rather than taking an opportunity to directly address the issue, Zuckerberg doubles down on benign platitudes such as users having control of information because they chose to share it in the first place.

This notion of user control is reaffirmed in an April 23, 2018, release by Goldman that attempts to explain what information Facebook advertisers have about users. The release is structured as a Q&A format, and the following is an excerpt from the release:

> If I'm not paying for Facebook, am I the product?
>
> No. Our product is social media—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 the experience.
>
> 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.

The distinction between selling data and selling space, however, is not made apparent through this explanation. Rather, the release strategically positions Facebook with more common variations of advertisements for TV, radio, and newspapers. It does not provide a clear description of how data is used *for* these advertising campaigns to be successful. There is a logical disconnect between how Facebook sells advertisers space, and how Facebook knows what space to sell. What Facebook sells to advertisers is space on the News Feeds of individuals who will be the most psychologically susceptible to the advertisement, determination of which is made based on personal data.

Discussion

Thematic analysis of the releases examined in this study show that Facebook provides little information about its data collection, use, and storage practices. Our analysis cannot offer a comprehensive understanding of what Facebook considers to be user data, which is precisely the heart of the issue. The bottom line is that Facebook offers no clear definition of data to its users, and that makes it difficult for the company to articulate a cohesive privacy policy to the public. This overall lack of transparency yields significant consequences with regard to the public interest.

This is in large part a byproduct of minimal oversight and regulation on data privacy; the company simply is not required to be fully transparent in its data collection practices. From its inception, the process by which data are created, collected, and shared in the data economy has been difficult to understand. Seemingly inconsequential small data from individuals' likes, searches, videos, clicks, location, purchases, page views, etc., are aggregated to constitute big data, which can be analyzed to produce algorithms that reveal predictive patterns of behaviors, values, and attitudes (Zuboff, 2015). Facebook does not sell the small data points, which users see as personal data, but rather the small data are the raw material from which psychological profiles of individual users are derived, producing a form of artificial intelligence. Facebook monetizes data by profiling users and selling their attention based on algorithms that can infer personality traits that are useful to advertisers. For example, if the algorithm determines that a woman is trying to get pregnant, advertisers will pay to put messages in front of her.

The term Facebook advertisement is a misnomer since Facebook does not sell space to advertisers in the traditional sense but sells algorithms to micro-target individuals who will be the most psychologically susceptible (c.f. Ward, 2018) to the messages. Moreover, McNamee (2019) contended that "all that data goes into Facebook's artificial intelligence and can be used by advertisers to exploit the emotions of users in ways that increase the likelihood that they purchase a specific model of car or vote in a certain way" (p. 69). Facebook's advertisers include not only legitimate organizations, but also political entities—foreign and domestic, special interest groups, app developers, fake organizations, and real grassroots organizations that seek to polarize and radicalize.

Unlike traditional advertising messages that are regulated by the FTC, algorithmic micro-targeting is completely unregulated. Facebook also sells data to third-party brokers who use bulk data to create their own algorithms and who operate, in the United States at least, in secrecy—outside of statutory consumer protections and without consumers' knowledge, consent, or rights of privacy and due process (U.S. Committee on Commerce, Science, and Transportation, 2013, as cited in Zuboff, 2015, p. 78). In other words, third-party brokers can decide how the data are used, and Facebook policies do not apply, giving Facebook a legal loophole to escape liability for any misuse. However, according to Ward (2018), most individuals are unaware of how data are collected, stored, and used and have little understanding of what, exactly, is taken from them, and the current study found that Facebook does little to contribute to a better understanding.

Zuckerberg purports that Facebook uses data to provide better service. According to McNamee (2019), Facebook's algorithms give users what they want, which is good for Facebook's bottom line since happy users share more data, which are the raw materials from which profits are derived. He suggested that one might assume that Facebook's users would be outraged by the way the platform has been used to undermine not only privacy, but also democracy, human rights, public health, and innovation: “Some are, but most users love what they get from Facebook. They love to stay in touch with distant relatives and friends. They like to share their photos and their thoughts. They do not want to believe that the same platform that has become a powerful habit is also responsible for so much harm” (p. 242). Debatin et al. (2019) found empirical evidence in support of these assertions, suggesting that Facebook users’ lax attitude may be based on a combination of high gratification, use patterns, and a psychological mechanism similar to third-person effect. Debatin et al. (2019) claimed that safer use of social network services would thus require changes in user attitude. Their findings are consistent with extant literature about social media platform use and behavior.

The current study represents a point of departure from placing the burden of behavioral change on the individual user, but rather makes a case that social media companies like Facebook need to be held responsible for creating, maintaining, and communicating clearer policies regarding data collection, use, and storage. Although legislative action like GDPR in the European Union and California’s Consumer Privacy Act have attempted to resolve some of the issues such as clearly defining personal data, using plain language, obtaining informed consent, data accessibility and portability, and the right to be forgotten, among others, technology companies such as Facebook, Twitter, and Google persist in collecting personal information under the guise of providing better service to the user. What is surprising is the lengths that these companies will go to in order to maintain their competitive advantage. A report in *The Guardian* on unearthed internal documents at Facebook, for example, found that the company “targeted politicians around the world—including former UK chancellor, George Osborne—promising investments and incentives while seeking to pressure them into lobbying on Facebook’s behalf against data privacy legislation” (Cadwalladr & Campbell, 2019, para. 1). In 2017, Facebook spent $11.5 million on lobbying, making it among the top spenders in Washington (Osnos, 2018). Stories such as this one lend additional support to the argument that Facebook’s public communication efforts are misleading in regard to its data policy and are emblematic of the company’s clandestine nature.

The releases selected for analysis in this research suggest that Facebook may not necessarily be keeping its processes secret in order to protect its competitive advantage, but rather, as Buhmann et al. (2020) suggested, “The fluidity of these systems makes it excessively difficult, and in some cases even impossible, to detect problems and identify causes even if organisations [*sic*] grant access” (p. 81). These opacity concerns affect not only Facebook, but any entity (i.e., political, corporate, etc.) that chooses to advertise on the platform.

That Facebook’s public communication is unclear only scratches the surface of potential legal, ethical, and policy implications associated with data gathering, storage, and use. Isaak and Hanna (2018) considered these issues to be disruptive forces that “have a tangible influence on citizens’ rights such as statutory rights—due process, equal representation before the law, the right to appeal, and trial by jury—and constitutional rights like freedom of expression, voting, and non-discrimination” (p. 57). Ward (2018) argued, “Regardless of how data is used, the very collection of it in bulk results in power imbalances that threaten the autonomy of individuals who have little say in whether data is hoarded and scant knowledge of what, exactly, is taken" (p. 137). At the very least, companies such as Facebook should be fully transparent in their practices to ensure that users are completely aware of what they do, in fact, opt in to.

Conclusion

Concerns about Facebook's policies and use of personal data are increasing. This study examined how Facebook frames its messages about privacy to its users and took a critical look at the consequences of Facebook's corporate business model and business practices. The primary contribution from the study is the light it sheds on Facebook's message strategy regarding its privacy policies and algorithmic applications. In keeping with Fessmann's (2017) conceptual foundations of public interest communications, we believe that by illuminating Facebook's strategic framing of its privacy policy, results from the current study might yield valuable insight into the organizational structures that need to be challenged in order for scholars and practitioners alike to effectively and ethically address public interest concerns associated with corporate surveillance and obscure data collection practices. Tufekci (2015) warned of the potential consequences of allowing such structures to go unchecked: "In essence, our machines, armed with our data, can increasingly figure things out about us beyond any previous level, and completely unaccounted for in law, policy, or even basic awareness among the general public" (p. 211).

Big data and algorithms are not inherently bad. Prior research has "exposed both the potential harm in the use of Big Data, as well as its potential for improving society and bringing about social justice" (Holtzhausen, 2016, p. 21). But in order to stem the negative consequences associated with data collection on such a massive scale, public policy is needed to better protect social media users as well as to require more transparency about how data are used. Given how rapidly the social media landscape can change, it is critical to note that data collection, if left unregulated, will only expand, casting more doubt on its effects on our cultural institutions.

References

Amnesty International. (2019). Surveillance giants: How the business model of Google and Facebook threatens human rights. https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF

Andreou, A., Venkatadri, G., Goga, O., Gummadi, K., Loiseau, P., & Mislove, A. (2018, February 18-21). *Investigating ad transparency mechanisms in social media: A case study of Facebook's explanations* [Paper presentation]. Network and Distributed Systems Security Symposium, San Diego, CA, United States. http://dx.doi.org/10.14722/ndss.2018.23191

Angwin, J., Mattu, S., & Parris Jr., T. (2016, December 27). Facebook doesn't tell users everything it really knows about them. *ProPublica.* https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them

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

Braun, V., & Clarke, V. (2012). Thematic analysis. In H. Cooper (Ed.), *APA Handbook of Research Methods in Psychology: Vol. 2. Research Designs* (pp. 57-71). American Psychological Association.

Buhmann, A., Passmann, J., & Fieseler, C. (2020). Managing algorithmic accountability: Balancing reputational concerns, engagement strategies and the potential of rational discourse. *Journal of Business Ethics*, *163*, 265-280. http://dx.doi.org/10.1007/s10551-019-04226-4

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, *3*(1), 1-12. http://dx.doi.org/10.1177/2053951715622512

Cadwalladr, C., & Campbell, D. (2019, March 2). Revealed: Facebook's global lobbying against data privacy laws. *The Guardian.* https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment

Constantiou, I. D., & Kallinikos, J. (2015). New games, new rules: Big data and the changing context of strategy. *Journal of Information Technology*, *30*, 44-57. http://dx.doi.org/10.1057/jit.2014.17

Debatin, B., Lovejoy, J. P., Horn, A., & Hughes, B. N. (2019). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer Mediated Communication*, *15*, 83-108. http://dx.doi.org/10.1111/j.1083-6101.2009.01494.x

Doward, J., & Soni, R. (2019, February 23). Facebook attacked over app that reveals period dates of its users. *The Guardian.* https://www.theguardian.com/technology/2019/feb/23/facebook-app-data-leaks

Droesch, B. (2019, April 29). How social media users have—and have not—responded to privacy concerns. *eMarketer*. https://www.emarketer.com/content/how-social-media-users-have-and-have-not-responded-to-privacy-concerns

The Economist. (2017, May 6). The world's most valuable resource is no longer oil, but data. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

Fessmann, J. (2017). Conceptual foundations of public interest communications. *The Journal of Public Interest Communications*, *1*(1), 16-30. http://dx.doi.org/10.32473/jpic.v1.i1.p16

FTC. (2014, May 27). FTC recommends Congress require the data broker industry to be more transparent and give consumers greater control over their personal information. https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more

Gramlich, J. (2019). Ten facts about Americans and Facebook. *Pew Research Center*. http://www.pewresearch.org/fact-tank/2019/02/01/facts-about-americans-and-facebook/

Granville, K. (2018, March 19). Facebook and Cambridge Analytica: What you need to know as fallout widens. *The New York Times*. https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

Grothaus, M. (2019, April 8). More than 60% of Americans don't trust Facebook with their personal information. *Fast Company*. https://www.fastcompany.com/90331377/more-than-60-of-americans-dont-trust-facebook-with-their-personal-information

Holland, D., Krause, A., Provencher, J., & Seltzer, T. (2018). Transparency tested: The influence of message features on public perceptions of organizational transparency. *Public Relations Review*, *44*, 256-264. http://dx.doi.org/10.1016/j.pubrev.2017.12.002

Holtzhausen, D. (2016). Datafication: Threat or opportunity for communication in the public sphere? *Journal of Communication Management*, *20*(1), 21-36. http://dx.doi.org/10.1108/JCOM-12-2014-0082

Hill, K., & Mattu, S. (2018, January 11). Facebook knows how to track you using the dust on your camera lens. *Gizmodo*. https://gizmodo.com/facebook-knows-how-to-track-you-using-the-dust-on-your-1821030620

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *IEEE Computer Society*. https://www.computer.org/csdl/magazine/co/2018/08/mco2018080056/13rRUxbCbmn

Johnston, M. (2019, December 12). How Facebook makes money. *Investopedia*. https://www.investopedia.com/ask/answers/120114/how-does-facebook-fb-make-money.asp

Lilley, S., Grodzinsky, F. S., & Gumbus, A. (2012). Revealing the commercialized and compliant Facebook user". *Journal of Information, Communication and Ethics in Society*, *10*(2), 82-92. http://dx.doi.org/10.1108/14779961211226994

Lee, T. B. (2012, September 27). Privacy groups seek investigation of Facebook's retail data sharing. *Ars Technica*. https://arstechnica.com/tech-policy/2012/09/privacy-groups-seek-investigation-of-facebooks-retail-data-sharing/

Lerbinger, O. (2006). *Corporate public affairs: Interacting with interest groups, media, and government*. Routledge.

Lima, C. (2019, March 11). Facebook backtracks after removing Warren ads calling for Facebook breakup. *Politico*. https://www.politico.com/story/2019/03/11/facebook-removes-elizabeth-warren-ads-1216757

Markus, M. L. (2015). New games, new rules, new scoreboards: The potential consequences of big data. *Journal of Information Technology*, *30*, 58-59. http://dx.doi.org/10.1057/jit.2014.28

McFarland, M. (2017, February 7). Your car's data may soon be more valuable than the car itself. *CNN*. https://money.cnn.com/2017/02/07/technology/car-data-value/index.html

McNamee, R. (2019, January 17). Zucked: Waking up to the Facebook catastrophe. *TIME*. https://time.com/5505441/mark-zuckerberg-mentor-facebook-downfall/

Obar, J. A., & Oeldorf-Hirsch, A. (2018). The clickwrap: A political economic mechanism for manufacturing consent on social media. *Social Media & Society*, *4*(3), 1-14. http://dx.doi.org/10.1177/2056305118784770

Osnos, E. (2018, September 17). Can Mark Zuckerberg fix Facebook before it breaks democracy? *The New Yorker*. https://www.newyorker.com/magazine/2018/09/17/can-mark-zuckerberg-fix-facebook-before-it-breaks-democracy

Rawlins, B. (2008). Give the emperor a mirror: Toward developing a stakeholder measurement of organizational transparency. *Journal of Public Relations Research*, *21*(1), 71-99. http://dx.doi.org/10.1080/10627260802153421

Schechner, S. (2019, February 24). Popular apps cease sharing data with Facebook. *The Wall Street Journal*. https://www.wsj.com/articles/popular-apps-cease-sharing-data-with-facebook-11551044791

Schnackenberg, A. K., & Tomlinson, E. C. (2016). Organizational transparency: A new perspective on managing trust in organization-stakeholder relationships. *Journal of Management*, *42*(7), 1784-1810. http://dx.doi.org/10.1177/0149206314525202

Schwartz, P. M., & Solove, D. J. (2014). *Reconciling personal Information in the United States and European Union, California Law Review, 102*, 877.

Seetharaman, D., & Grind, K. (2018, June 8). Facebook gave some companies special access to additional data about users' friends. *The Wall Street Journal*. https://www.wsj.com/articles/facebook-gave-some-companies-access-to-additional-data-about-users-friends-1528490406

Silverman, R. E., & Waller, N. (2015). The algorithm that tells the boss who might quit. *Wall Street Journal*. http://www.wsj.com/articles/the-algorithm-that-tells-the-boss-who-might-quit-1426287935

Steel, E., Callum, L., Cadman, E., & Freese, B. (2013, June 12). How much is your personal data worth? *Financial Times*. https://ig.ft.com/how-much-is-your-personal-data-worth/

Tiku, N. (2018, April 23). What's not included in Facebook's 'Download Your Data.' *Wired*. https://www.wired.com/story/whats-not-included-in-facebooks-download-your-data/

Tufekci, Z. (2014, December 18). The year we get creeped out by the algorithms. *Nieman*. https://www.niemanlab.org/2014/12/the-year-we-get-creeped-out-by-algorithms/

Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colo. Tech. LJ*, *13*, 203.

Tufekci, Z. (2018, March 19). Facebook's surveillance machine. *The New York Times*. https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html

Van den Bogaert, S., Declercq, J., Christiaens, T., Jacobs, G., & Bracke, P. (2018). In the land of pharma: A qualitative analysis of the reputational discourse of the pharmaceutical industry. *Public Relations Inquiry*, *7*(2), 127-147. http://dx.doi.org/10.1177/2046147X18774588

Ward, K. (2018). Social networks, the 2016 presidential election, and Kantian ethics: Applying the categorical imperative to Cambridge Analytica's behavioral microtargeting. *Journal of Business Ethics*, *33*(3), 133-148. http://dx.doi.org/10.1080/23736992.2018.1477047

Wood, M. (2018, March 19). Cambridge Analytica, Facebook and the new data war. *Marketplace*. https://www.marketplace.org/2018/03/19/tech/cambridge-analytica-facebook-and-new-data-war

Zeadally, S., & Winkler, S. (2016). Privacy policy analysis of popular web platforms. *IEEE Technology and Society Magazine*, *35*(2), 75-85. http://dx.doi.org/10.1109/MTS.2016.2554419

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization, *Journal of Information Technology*, *30*, 75-89. http://dx.doi.org/10.1057/jit.2015.5