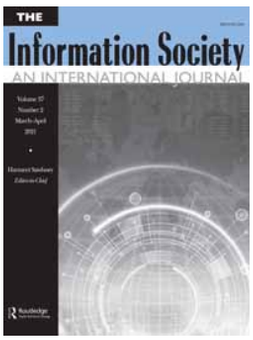

The Information Society
An International Journal

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/utis20

"This is capitalism. It is not illegal": Users' attitudes toward institutional privacy following the Cambridge Analytica scandal

Hagar Afriat, Shira Dvir-Gvirsman, Keren Tsuriel & Lidor Ivan

To cite this article: Hagar Afriat, Shira Dvir-Gvirsman, Keren Tsuriel & Lidor Ivan (2021) "This is capitalism. It is not illegal": Users' attitudes toward institutional privacy following the Cambridge Analytica scandal, The Information Society, 37:2, 115-127, DOI: 10.1080/01972243.2020.1870596

To link to this article: https://doi.org/10.1080/01972243.2020.1870596

Published online: 11 Mar 2021.

THE INFORMATION SOCIETY
2021, VOL. 37, NO. 2, 115–127
https://doi.org/10.1080/01972243.2020.1870596

Routledge
Taylor & Francis Group

"This is capitalism. It is not illegal": Users' attitudes toward institutional privacy following the Cambridge Analytica scandal

Hagar Afriat, Shira Dvir-Gvirsman, Keren Tsuriel, and Lidor Ivan

Department of Communication, Tel Aviv University, Tel Aviv, Israel

ABSTRACT

In this study, we seek to understand the considerations of young adults who chose to continue their active engagement with Facebook even after Cambridge Analytica scandal laid bare the mechanics of economic surveillance. We base our analysis on two sets of in-depth face-to-face interviews we conducted with young adults in Israel—26 before the Cambridge Analytica scandal, which we had already conducted for a study on privacy, and 24 after the scandal erupted. To analyze our respondent's rationales, we employ Boltanski and Thévenot's regimes of justification framework. Before the scandal, our respondents largely saw privacy as a commodity, a tradeoff made by the individual—information disclosure in exchange for free personalized digital services. However, there were some respondents who rejected the notion of privacy as a commodity and advanced an alternative perspective that considers it to be a human right. After the Cambridge Analytica scandal, there was a marked shift away from understanding of privacy as a right, which our respondents neither saw an unconditional right nor something enforceable by regulators. Instead, they largely saw economic surveillance as something inherent to the digital world, which one needs to accept if one wants to participate in it.

ARTICLE HISTORY
Received 22 June 2019
Accepted 22 November 2020

KEYWORDS
Cambridge Analytica; economic surveillance; Facebook; legitimacy; privacy; social media

Introduction

In March 2018, the *Guardian* and the *New York Times* jointly published a news story entitled "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach." This news story unveiled what subsequently came to be known as the Cambridge Analytica (CA) scandal, often referred to as a watershed moment in public discourse on companies' use of personal data (Golbeck and Aral 2018; Griggs 2018).

The scandal centered on massive collection of data of 87 million Facebook users made possible by a Facebook app *This Is Your Digital Life*, developed by the Global Science Research (GSR) in partnership with CA. In what began as an academic research project, CA and GSR paid users to take a personality test within the app if they allowed the data so collected to be used for research. At that time, Facebook's default terms allowed their Facebook friends' data to be collected as well, unless the users changed their privacy setting (Such access is no longer available). CA and GSR used this data to identify users' political beliefs and personality characteristics and determine which users to target and how to influence their actions and thoughts (Ur Rehman 2019). The 270,000 Facebook users who took the personality test as participants in an academic research project ended up also providing access to their Facebook friends' information. Since none of these users, or their Facebook friends, agreed to give their data to a third-party company for use in marketing, various concerned parties accused CA and GSR of violating Facebook's terms of service[1] (Cadwalladr and Graham-Harrison 2018).

As a result of this crisis, Facebook was fined, and its founder and CEO Mark Zuckerberg was summoned to testify before the US Senate (Brewster 2018). Worldwide media coverage of this story was massive. Journalists wrote of the "beginning of the end" of Facebook (Bogle 2018) and reported surveys suggesting decline in users' trust in Facebook and use of its platform after the eruption of the scandal (Beck 2018; Insider Intelligence 2020; Kahn and Ingram

CONTACT Hagar Afriat hagar.afriat@gmail.com Department of Communication, 710 Naftali Building, Tel Aviv University, Ramat Aviv, Tel Aviv 69978, Israel.

2018; Weisbaum 2018). This uproar led journalists and academics to ask whether it was a watershed moment that would result in disconnections by its users (Griggs 2018; Golbeck and Aral 2018).

While some news stories reported (Hern 2019; Statt 2018) that the scandal was followed by user disconnection from the platform, actual number of Facebook users increased the year the CA scandal broke out. In December 2018 Facebook had over 1.52 billion people using its platform every day—a 9% increase over the previous year (Gartenberg 2019). Pew data (Perrin 2018) also shows little evidence of user disengagement—only 9% of users took advantage of the new post-CA scandal privacy setting Facebook put in place, allowing them to download all information it had collected about them.[2]

In this study, we seek to understand the considerations of young adults who chose to continue their active engagement with Facebook even after confronting evidence of economic surveillance. We base our analysis on two sets of in-depth face-to-face interviews we conducted in Israel[3]—26 before the CA scandal, which we had already conducted for a study on privacy, and 24 after the scandal erupted. To analyze their rationales, we employ Boltanski and Thévenot's (2006) *regimes of justification* framework.

In-depth interviews suggest that users perceive privacy not as an integral component of one's civil rights but as a negotiable commodity traded according to societal norms. This perception became even more prevalent after the outbreak of CA scandal. At that critical moment, users reestablished in their minds Facebook's legitimacy and right to harvest data by reframing it according to a neo-liberal ideology. In this view, it is the users' responsibility to manage their privacy, as it is Facebook and other social media companies' right to profit from activities on their platforms. After all, as one participant remarked: "This is capitalism. It is not illegal."

Social and institutional privacy

Harvesting of personal information posted on social media for advertising purposes, referred to as economic surveillance, is of major scholarly concern (Marwick and Hargittai 2019; Turow, Hennessy, and Draper 2015). Users, however, appear to be indifferent to the issue (Sujon 2018; Young and Quan-Haase 2013)—due to lack of awareness (Stutzman, Gross, and Acquisti 2013), or resigned pragmatism, i.e., a sense of helplessness (Hargittai and Marwick 2016; Hoffmann, Lutz, and Ranzini 2016; Turow, Hennessy, and Draper 2015).

When people are concerned about online privacy, they tend to focus on *social privacy*—"the control of information flow about how and when personal information is shared with other people" (Raynes-Goldie 2010). In other words, they tend to be concerned about their social visibility—privacy from peers, family, employers, and others (Sujon 2018). But sharing information with family, friends, and others on social media also allows companies providing the service to access their data (Andrejevic 2013; Fisher 2018; Fuchs 2012; Jansson 2012; Padyab et al. 2019). The latter constitutes *institutional privacy*—"how institutions such as governments, banks and businesses, use or misuse the personal information" (Raynes-Goldie 2010).[4]

Past studies that addressed both types of privacy show that users are far more apprehensive over social privacy than the institutional privacy[5] (Lutz and Ranzini 2017; Raynes-Goldie 2010; Sujon 2018; Young and Quan-Haase 2013) because of their lack of awareness (Padyab et al. 2016; Stutzman, Gross, and Acquisti 2013), poor understanding (Sujon 2018) and a sense of cynicism and apathy (Hargittai and Marwick 2016; Hoffmann, Lutz, and Ranzini 2016; Marwick and Hargittai 2019). For example, Stutzman, Gross, and Acquisti (2013) show that users exposed more information following changes in their privacy settings that increased their level of social privacy, resulting in lower levels of institutional privacy, as they did not realize that while sharing with a small circle of friends, they are also sharing information with *silent listeners*—Facebook and other companies. To understand such behavior, Lyon (2017) argues the role of culture in enabling economic surveillance needs to be studied explicity.

In the case of Facebook, the aggregate collected data is like an iceberg, with only a small fraction of it visible to users—primarily their interactions with other users, which renders social privacy issues more salient (Debatin et al. 2009). Furthermore, users are unaware of data collector's information processing. In effect, they are capable of perceiving only bits and pieces of the information their social media profiles actually contain. Consequently, they have very little understanding of the level of profiling third-party companies can perform on the data social media companies collect on their platforms (Padyab et al. 2016, 2019).

In general, it is far more complicated for users to understand institutional privacy than it is to grasp the

meaning of social privacy (Draper 2017; Stutzman, Gross, and Acquisti 2013). Moreover, economic surveillance is "deeply embedded in and obscured by social media infrastructures" (Sujon 2018, 3756)—user agreement forms, privacy policies, and copyright enforcement that present harvesting in a manner emphasizing users' possible benefits (personalization, customization etc.), while minimizing explanations of its commercial use (Nam 2020). Consequently, scholars question whether users are sufficiently informed to understand and consent to such surveillance (Turow, Hennessy, and Draper 2015).

Moreover, recent studies suggest that users experience feelings of powerlessness, apathy, and cynicism in the face of institutional privacy (Hargittai and Marwick 2016; Hoffmann, Lutz, and Ranzini 2016; Marwick and Hargittai 2019). Realizing that "privacy violations are inevitable and opting out is not an option" (Hargittai and Marwick 2016, 3753), users believe that they have no choice but to accept the terms and conditions, leaving them with little control over their data, an approach termed "resigned pragmatism" (Hargittai and Marwick 2016; Turow, Hennessy, and Draper 2015). The reason users cannot make rational decisions about their personal data is neither a lack of information necessary for informed choice nor disregard for their privacy, but rather their being compelled to accept the tradeoff offered to them by social media platforms (Draper 2017).

Regimes of justification

Boltanski and Thévenot (2006) identified six principal regimes of justification (Table 1) from which the issue at hand may be interpreted. The *civic* world focuses on collective welfare and public interest, favoring them over individual interest. The *domestic* world is grounded in hierarchy, conventions, and tradition, in a patriarchal society. The *market* world is based on economic value and competition. The *industry* world focuses on technological efficiency, progress, productivity, and professionalism. The *fame* world is oriented toward public opinion, recognition, and exposure. The *inspired* world is marked by vision, passion, and imagination, with creativity at its core.

In the case of our study, our guiding assumption is that the justifications respondents offer for their positions on economic surveillance reflect their general perception of - existing and desired - social order and conceptions of right and wrong (Bellman et al. 2004). For example, users may situate the issue of economic surveillance in the civic world, suggesting that they perceive it as a social issue. By contrast, those who situate it in the market world consider it to be a matter of commerce (De Wolf et al. 2017). Changes in justifications are typical of crises of legitimacy that occur as a result of disagreement over the pertinence of conventions in a specific situation (Arts, Buijs, and Verschoor 2018; Nyberg and Wright 2012; Reinecke, van Bommel, and Spicer 2017). When the legitimacy of a practice or norm is questioned, as in the instance under discussion (for example, see O'Hagan 2018), the challenged power structure is assessed[6] (Blokker 2011; Vaara 2014).

Methodology

Unlike past research that relied on focus groups (e.g., Hargittai and Marwick 2016; Hoffmann, Lutz, and Ranzini 2016;), we conducted in-depth interviews, which remove issues related to peer pressure. We conducted in-depth face-to-face interviews with 50 participants—45 participants were students at a major university in central Israel, and the other 5 were non-students.[7]

Following Marwick and Hargittai (2019), we focused on a sample of young adults, ages 20-35 (average age: 25.3[8] (for two reasons: (1) high engagement with social media, both in quantity (Poushter, Bishop, and Chwe 2018) and quality (Madden et al. 2014); (2) people in this age group tend to have less concern for maintaining their privacy (Marwick and Hargittai 2019), and exhibit more trust in Facebook (Malik, Hiekkanen, and Nieminen 2016).[9] Some young adults even consider online surveillance to be beneficial, in contrast to older users (Madden et al. 2014).[10] Participants were recruited using a Facebook advertisement, which indicated that the study is about Facebook use without mentioning the issue of privacy. The interviews lasted 35–60 minutes. Participants received $15 as compensation for their time.

We conducted interviews on two occasions: Before the scandal (December 2017: 26 participants) and while it unfolded (April 2018: 24 participants). Obviously, such a plan could not have been devised in advance and cannot be considered a truly comparative design. Rather, it leveraged available data (the corpus of the pre-scandal interviews) to enrich interpretation of themes identified in interviews conducted in light of the scandal.

The interviews were semi-structured, in accordance with a list of 20 questions, and were managed fluidly. We focused on the participants' relationship with Facebook, asking them to describe their likes and

Table 1. Regimes of justification (adapted from Boltanski and Thévenot 2006)

Justification	Mode of evaluation	Qualified objects	Keywords	Example
Civic	Collective welfare	Rules and regulations, fundamental rights, welfare policies	Rules and regulations, civic rights, social responsibility, legal, official, regulations	"[I don't like about FB] the invasion of your privacy, when they record you and track you … You feel you have no privacy, that they know anything about you."
Market	Gains and losses	Market circulation of goods and services	Gains and losses, market, value, economical logic, goods, services, customer, consumer, exchange	"FB profits from my activity, that's their gain, because if people are active on FB they make profits. If people won't use FB it'll disappear."
Domestic	Custom and tradition	Patrimony, heritage	Conventions, status quo, that's the way the world operates, tradition, heritage	"It (CA scandal) doesn't sound exceptional, I think FB has always done it … You assume all your information is exposed … it's quite naïve to assume that what you post is only yours."
Industrial	Technical efficiency	Infrastructure, project, technique	Progress, improving the world, efficiency, functional, operational, technical, competence, measurable, infrastructure	"At the end, their goal – and I'm not justifying them – was to make our lives easier … things are more accessible, you don't have to look for them. Yes, I'm aware of the consequences, that FB can take my profile picture and do something with it."
Inspired	Grace, singularity, creativity	Creation, emotional connection	Brilliance, vision, changing the world, inspiration, unusual, passion, enthusiasm, visionary	"I'll be sad for Mark Zuckerberg … the man started an empire … he's probably smart … it'll be sad because he revolutionized the way we consume content and interact with people, for better and for worse … our generation will remember him forever."
Fame	Renown	Attention, media, image	Public exposure, need for recognition, influencing public opinion, fame, popularity, celebrity	"I'm less bothered than others by FB [invading my privacy] because I don't have anything to hide. I'm one person in this world, not that significant. I'm not like Donald Trump who runs the world."

□ Regimes of justifications that were prevalent in the responses of current study's participants.
■ Regimes of justifications that were NOT prevalent in the responses of current study's participants.

dislikes, how they use the platform, their feelings about such use and that of others, and how they believe the Facebook feed works. As past work suggested that users are not preoccupied with institutional privacy (Stutzman, Gross, and Acquisti 2013; Young and Quan-Haase 2013), we allowed the issue of privacy and surveillance to emerge organically without asking participants about it directly. In the first series of interviews, three participants did not address privacy issues at all and two only mentioned social privacy.

In March 2017, three months after the first series of interviews, when the CA scandal erupted, we launched a second series of interviews, employing the same framework but this time focusing on possible changes in users' discourse regarding privacy. In these interviews, one participant did not raise the issue of privacy at all and four others did not mention institutional privacy. Toward the end of these interviews, we asked participants who had not referred to the CA scandal whether they had heard about it. Five reported that they were not familiar with it, although they did know that Facebook uses personal data to target users. We asked all participants what they thought about the issue. In the case of those who had heard about the scandal, we also asked whether it changed their opinions of Facebook, whether their engagement with the platform changed, whether they thought it changed the behavior of other users, and how they expected the scandal to affect Facebook. One participant said she heard about the scandal but did not believe Facebook could "do such a thing." Consequently, we asked her no further questions about this matter.

We recorded and transcribed all interviews. Before analyzing the transcripts, informed by Boltanski and Thévenot (2006) and Giulianotti and Langseth (2016), we created a word bank representing each regime of justification. We only analyzed interview transcripts that had mentions of privacy related issues. Each interview transcript was read by two coauthors to identify privacy related quotes—yielding 402 quotes. Each quote was examined to determine whether it was in accord with the values of the regimes of justification. For example, the civic world rests on collective welfare principle. Participants' support of users' rights to privacy is considered acceptance of this principle, whereas discourse claiming it is the user's responsibility to manage privacy is viewed as rejection thereof. Although they are two very different stands, they are both considered part of the civic world, as both express a civic standpoint with regard to users' privacy. We also determined whether or not participants mentioned social privacy issues and what they believed will happen to Facebook as a result of the scandal. Following this process, we ascribed the

identified quotes to *one or more* possible regimes of justifications. If a quote did not accord with any of the justifications listed, it was coded as such (6 quotes out of 402).

Findings

Social privacy versus institutional privacy

Since earlier research has indicated that users are unaware of institutional privacy (Padyab et al. 2016, 2019), we were especially intrigued by its mention in interviews conducted before the scandal. The first series of interviews revealed that although young adults do not have a full understanding of how economic surveillance actually operates, about two-thirds of the participants did appear to be aware of its occurrence even before the CA scandal broke out. For example, Sharon said: "There is no privacy. They know how to find out what interests me and how to make money out of it … That is what this industry does. You get addicted and there is nothing you can do about it … They have radio operators that sit and listen in on us … They have people who understand this whole world of big data. They know how to analyze my use."

The existing research suggests that users are far more concerned about their social privacy than the institutional variety (Young and Quan-Haase 2013). Consequently, we examined users' responses at the height of the scandal to determine whether the balance between their concerns about these two types of privacy had indeed shifted. We found that even at the outbreak of an institutional privacy scandal, young adults were still preoccupied with dangers presented by other users.[11] As noted above, in this series of interviews, 20% of the participants only mentioned social privacy and none exclusively addressed economic surveillance or any type of institutional privacy. Some participants framed CA as a social privacy danger that emerged from the institutional breach, describing a leak of personal information that may end up in the hands of unintended audiences. Some imagined a "big bad wolf" lurking in the dark net. Jennifer, for example, said that the data "can find its way to all kinds of forums in the deep web and could be abused to construct identities for spies or use credit cards for all kinds of suspicions transactions. There is no limit to the creativity of those people." Jennifer is not worried about the ways in which commercial companies can put her data into use. In that regard, she displays little concern about economic surveillance. Her take, however, demonstrates the close ties between the two types of privacy: How issues of institutional privacy—the collection of personal information by companies—can lead to social privacy concerns and even criminal activities perpetrated by individuals (Stutzman, Gross, and Acquisti 2013).

Finally, it should be noted that a quarter of the participants, in the first and second series alike, described the realities of economic surveillance in harsh, Orwellian language (including the term "Big Brother"). Jake, for example, who was interviewed before the scandal, remarked: "Facebook carries out experiments on human beings. They have a deep knowledge of the psychology of internet use, so they can manipulate you. I have no choice. They know me and my psychological makeup better than I know myself." Helen expressed similar sentiments, saying that "It's like a cult, jumping from the roof because Zuckerberg told us to." Noa, who was interviewed after the scandal, said: "There is nothing for me to do. If I do have something to hide, I'll find a way to express it without using words [because Facebook is listening] … I may have to leave notes at dead drops." Such rhetoric will be discussed in greater depth in the review of participants' domestic justifications, below.

Regimes of justification

Analyzing young adults' discourses, we found that three of the regimes of justification were highly prevalent: Civic (39% in the first series and 87% in the second), market (91% and 88%, respectively) and domestic (10%, 91%, respectively). Below, we focus on only these regimes of justification (other justifications appeared in fewer than 30% of interviews).

The civic world: From "I think Facebook is following me" to "It's your responsibility to know that it is"

A comparison between the two series of interviews indicates a change in the discourse following the scandal. In the first series, the civic world was less dominant. It was mentioned by six participants, whose primary focus was the right to privacy, indicating some acceptance of civic world principles, as evidenced in use of the expression "invasion of privacy." Dan, for example, said: "There was a rumor that Facebook is listening in on us. After you give Facebook permission to use your mobile mic for voice conversations, it stays live so that Facebook can listen to your conversations and then place ads on your feed … This is a gross invasion of my privacy, misusing me and my trust in Facebook just to sell me stuff."

In the second series, the civic world was far more dominant, mentioned by 17 participants. This time, however, users *renounced* the idea of privacy as a collective right or policy; the civic regime was deemed irrelevant and summarily rejected. Instead, participants displayed an anti-civic, neo-liberal perspective (De Wolf et al. 2017; Shade and Shepherd 2013), maintaining that users bore personal responsibility for understanding how their data is being used and for what purposes and should act accordingly. For example, Shirley said: "If someone thought it was a coincidence that he was seeing things that interest him, that would be a bit like turning a blind eye … Anyone who puts himself out there on Facebook needs to be aware of his exposure and its consequences … While it is not legitimate to do what that company did, when you use a platform like the internet, that is known for being [a place where] your photos can be appropriated by others because you posted them, you need to be mindful of what can happen. So it [using the information] is legitimate."

Even when participants wondered about the legality of actions concerning the CA scandal, they were unable to identify the regulator with authority over Facebook. When asked who is in charge of regulating Facebook, Hannah replied: "I have no idea, there must be some entity. I mean, if Mark Zuckerberg can choose to block me for something I posted … someone can block him." Interestingly, her conceptualization of regulation was entirely personalized: Speaking of Mark Zuckerberg (rather than the corporation itself) and the power he has over her, while relying on rhetoric drawn from the interpersonal relations of the platform itself. This conceptualization goes along with lack of respect for the legal system in place. For example, Barbara said: "Facebook will not be closed down as the result of legal proceedings. There will be a battery of lawyers to defend them in court." Similarly, Jennifer expressed ridicule when she noted that "it [the surveillance] did not surprise me. I don't know. Those Zuckerberg hearings in Congress [Senate] were a joke—a bunch of old people asking him how the internet works."

Ascribing responsibility to social media users undermines collective and general perspectives in favor of an individualistic point of view in which users are free agents and must take responsibility for their respective actions (Baruh and Popescu 2017). This concept sets aside all motivations connected with general public benefit and echoes the rhetoric used by Facebook itself to legitimize its actions (Freishtat and Sandlin 2010; Hoffmann, Proferes, and Zimmer 2018).

The market world: From "Facebook works for me" to "You can't get something for nothing"

As seen above, young adults consider themselves autonomous—a perspective reflected in their self-perception as consumers: "[In] federal regulatory discourse, civic needs and the public good are replaced by consumer demands and fair business practices" (Shade and Shepherd 2013, 8). This idea is at the heart of the market world, whose chief concerns are pricing, costs, and benefits. An overwhelming majority of participants discussed the costs (surveillance) and benefits of Facebook use in both series of interviews, indicating participants' acceptance of market world principles. Thus, in contrast to the civic world, where changes in discourse were abundantly clear, here there was relatively little change. Initially, users were preoccupied with the micro level—their consumer-supplier relations with Facebook (i.e., actor level)—while in the second, they shifted to macro-level rationalizations—discussing the free-to-use business models that dictate market relations (i.e., market level).

In the first series of interviews, interviewees focused on their benefits. While some participants discussed advantages unrelated to surveillance (e.g., connectivity) and accepted such scrutiny as a mandatory drawback, others linked the advantages of social media to surveillance: If Facebook needs to invade privacy so that ads and content can be targeted, it should do so. In one instance, Angela said: "Facebook ads don't bother me. I know Google and Facebook are tracking me … but I don't think that's bad. It has its unpleasant sides, such as lack of privacy, but in the end, the ads I see on Facebook are relevant to my needs … so it's good." The difference between these perspectives is of importance because the second identifies surveillance (in some form) as necessary for the materialization of social media's advantages. A few participants even considered surveillance an advantage in itself. Ariel uses her mobile phone because she believes Facebook is listening to her and will place the advertisements she wants on her Facebook feed: "Each of these platforms knows everything about me … so I just go along with it. If I want a new bike, I can shout 'Bike!' at my phone and it will display content according to my needs … I can use it to my benefit." Furthermore, many participants believed that they are gaining the upper hand, such as Roy: "I think I get more from Facebook than I give … I don't post anything, I just read a lot." In that sense, young adults present what appears to be a form of privacy calculus (Marwick and Hargittai 2019), wherein users decide

what and how much they should disclose by balancing gain-risk ratios.[12]

While the market world was dominant in both series, the justifications differed slightly: participants in the first series talked their own gains, and those in the second series talked about Facebook's need for profits showing young adults' understanding that Facebook is a for-profit corporation. Lucas said: "[Facebook] is a profit-making company. It's not as if someone were forcing me to use its platform. Whoever joins Facebook does so willingly, so Facebook has a right to the data."

Referring specifically to the CA scandal, some participants adopted critical tones toward other users (echoing civic justification), blaming them for believing naïvely that they can use Facebook without having to pay anything. Noa, for example, claimed that "it's free because they are using your shared information and data … [other users'] naïveté is absurd."

Participants justified Facebook surveillance by framing it as a market issue. They mentioned Facebook's business model and the costs and benefits for the service itself and its users, repeating the expression "you can't get something for nothing." Together with the civic world (or lack thereof), it appears that users do not frame economic surveillance as a violation of rights, but rather as a "terms and conditions" issue (Baruh and Popescu 2017).

The domestic world: From marginal justification to public relations

The domestic world centers on tradition, customs, and hierarchy, yet such justification was almost absent in the first series of interviews—only one participant discussed the lack of privacy on Facebook as something to be expected on such a platform. After the CA scandal, domestic-world justification was highly prevalent. Participants said that "there is nothing new under the sun" because advertising tools of this type have long been in place. Noa explained: "Actually, [people and companies] have been doing things like that since the dawn of history. After World War II, they started taking advantage of public relations … Why is it so surprising to you? That's how it is."

Since "there is no more privacy in this world" (Alex), participants noted that this is simply the way the world works—you either accept surveillance, as surveillance is a feature of every digital service, or reject it by going offline. As Jennifer described: "When I read about it [the scandal], I said: 'OK, what's new about that?' There was a breach and information leaked, but it leaks all the time from everywhere, so why is Facebook so important in this context? Biometric databases are being hacked, so what's Facebook [by comparison]?".

Many participants agreed that this is how the world works, but we found that this justification had two forms. Most people who responded in this manner have no objections to surveillance, as described above. Others, however, acknowledged that this is how the world works, yet were far more critical, claiming that it is now "too late" to change it. They regret that the world operates as it does but accept it because the ship has already sailed. Today, much like under a totalitarian regime, if we desired privacy, we would "have to leave notes at dead drops" (Noa, see above). Like the resigned pragmatists (Turow, Hennessy, and Draper 2015, Hargittai and Marwick 2016), they feel that surveillance is a necessary evil because disconnection is simply not an option. Consequently, these participants were in a limbo: While they did not fully accept the domestic-world justification, their discontent with the current situation did not mature into a full rejection of it either.

Unlike previous research, in our study we did not find this domestic-world justification (only seven participants expressed such feelings). Nevertheless, the "too late" justification is significant because it reflects a primarily passive reaction to the scandal, along with a feeling of helplessness (that was also evident in users' perceptions regarding lack of regulation, as noted above). As Dan said: "Facebook knows everything about you. People no longer defend their privacy as zealously as they once did. If you want to use the platform, you have to *surrender* and come to terms with your increased exposure. It takes away some of my privacy, but it also reminds me of birthdays and other events, so it's OK."[13] (emphasis added)

Together, these responses categorized in three worlds—domestic, market, and civic—–suggest that young adults perceive surveillance as a norm and privacy as a negotiable personal good, in keeping with van Dijck's (2014) observation: "Metadata and data have become a regular currency for citizens to pay for their communication services and security—a tradeoff that has nestled into the comfort zone of most people" (197).

A closer look at participants' responses in both series of interviews suggests that although the neo-liberal approach was widespread, there were nuanced differences in discourse before and after the CA scandal. The change was evident in the decrease in the civic world-justifications, the increase in the domestic world-justifications and the changes in the nature of market world-justifications. In the first series, there was higher criticism of economic surveillance, participants used the civic world-

justifications to argue for their right to privacy. A second prevalent yet contradicting approach was the use of the market world-justifications to support economic surveillance through the lens of the privacy calculus (Marwick and Hargittai 2019), wherein privacy is a commodity traded for free goods online. The period following the scandal saw increased acceptance of economic surveillance, accompanied by acceptance of (and even advocacy for) the data industry business model (data in exchange for services) as the backbone of a digital society.

The future of Facebook? Leaving Facebook is not an option

Participants were divided evenly in their predictions of the scandal's outcome. Half believed that Facebook will not be affected because "it is too strong a habit" and "people have a short memory." "All they [Facebook] have to do is promise not to let it happen again. People will give up and they [Facebook] will continue to grow."

By contrast, other participants mentioned that users are leaving Facebook and that the company will have to change. Jennifer noted: "Maybe it's because the media are making a big deal out of it, but people are leaving Facebook. There is even this #deletefacebook hashtag that is really ironic because it's on Instagram, that also belongs to Facebook." Jennifer's important observation about Instagram highlights an overarching theme that a vast majority of participants expressed: There can be no turning back at the societal level. If Facebook falls (a consequence they considered unlikely), it will simply be replaced by another platform because "by now, people need these media. It is hard for them to face one another" (Nate). It is "like air" (Rachel) or "electricity" (Jake).

This dependence on social media, that has a strong normative grip on society, was most clearly expressed when we asked participants about disconnecting from Facebook. Even young adults who believed Facebook will suffer the consequences of the scandal and lose some of its members did not consider leaving it themselves (a few reported that they had disconnected in the past, before the scandal, but changed their minds and started using it again). They do not consider leaving Facebook to be a valid option for three interrelated reasons: First, they need to be kept up to date—they rely on the information provided by the platform, emphasizing the advantages it offers (Marwick and Hargittai 2019). Second, they consider themselves "addicts," describing disconnection as a brave act that they are not strong enough to perform. Finally, people without Facebook accounts are considered "weird" or elitist. Participants ascribed such behavior to a desire to be unique, to go against the stream, connecting it to "social trends such as veganism." As Dan noted: "It's hipster-like: 'I don't have Facebook, only Instagram.' I have a friend who closed his Facebook account and moved to Berlin [in Israel, the common perception is that those who migrate to Berlin are young, left-wing, arty hipsters]." Ariel said: "If they don't have Facebook, they have Instagram. I don't know anyone who doesn't want it at all, who doesn't want to stay in touch." In her eyes, living without social media means you have no desire for social connection.

As suggested by van Dijck (2013), participants view social media as an integral part of today's society, a social norm so embedded that it became a "must have" channel for social interaction. Nevertheless, participants' claims that social media is the norm stand in sharp contrast to their contention that anyone who does not want to be under surveillance can simply go offline. While maintaining that "no one is forcing you" (as mentioned above in the discussion of the domestic world), they actually point to social norms that do apply compulsion. Consequently, as Marwick and Hargittai (2019) suggest, the calculi that users employ regarding their privacy cannot be included in any rational balance of possible gains and losses, as a rational choice is first and foremost a free choice.

Conclusions: Users' mandating economic surveillance

When crisis such as the CA scandal occurs, established discursive positions are challenged, revealing social conventions (Blokker 2011). By interviewing young adults before and after the CA scandal, we were able to gain insights into their sense-making processes with regard to online surveillance and to identify changes in their privacy-related discourse.

Our findings support previous work on institutional privacy, as they show that young adults we studied are more preoccupied with social privacy than with institutional privacy (Stutzman, Gross, and Acquisti 2013; Sujon 2018). Also, we found that some users showed resigned pragmatism (Hargittai and Marwick 2016; Turow, Hennessy, and Draper 2015)[14] but it was not the prevalent approach, rather one of several approaches. Most notably, most of the participants were accepting of economic surveillance.

Underlying these responses, we see an understanding: The idea of privacy as a negotiable commodity. As Van Dijck (2014) notes: "The currency used to pay

for online services and for security has turned metadata into a kind of invisible asset, processed mostly separate from its original context and outside of people's awareness" (220). This understanding is the bedrock over which the larger economic and technological logic of informational capitalism can play out (Allmer 2014; Andrejevic 2013; Andrejevic and Gates 2014; Sevignani 2015; Trottier 2016).

Although understanding of privacy as a commodity was widespread prior to the scandal and in its aftermath, there were nuanced differences in the justifications offered within the market world. Before the scandal, understanding of privacy as a commodity was mostly seen as a tradeoff made by the individual—information disclosure in exchange for free personalized digital services (i.e., privacy calculus, Marwick and Hargittai 2019). However, there were users who rejected the notion of privacy as a commodity and advanced an alternative perspective that considers it to be a human right. After the CA scandal, there was a marked shift away from understanding of privacy as a right, which was seen as neither an unconditional right nor something enforceable by regulators. Instead, they saw economic surveillance as something inherent to the digital world, which one needs to accept if one wants to participate in it. In that sense, they echoed the conception of "surveillance becoming part of a whole way of life" (Lyon 2017, 825). Here, young adults did not discuss their individual privacy calculus, instead justified the for-profit models that drive current information capitalism (Mai 2016).

Encountering a legitimacy crisis due to a privacy breach, young adults did not call for social change or interpret it as a prompt to end resigned pragmatism. If anything, they more strongly espoused the idea of privacy as a commodity and supported the "role of social media as data capitalists masquerading as social networks" (Sujon 2018, 3766). Unable to conceive regulatory measures for ensuring online privacy, while facing a world in which leaving Facebook is not a practical option, young adults do not simply take a passive position, rather support Facebook's surveillance methods. As noted by one participant: "I assume Facebook is listening, But Mark Zuckerberg said they don't … I choose to believe him, although I know it is not exactly true." Indeed, it appears that the "watershed moment" became yet another event in which the neo-liberal ideas of free market and minimal regulation triumphed. This time, however, in favor of a commercial, for-profit corporation that shirked its responsibility.

Notes

1. Alongside privacy, other issues were raised and discussed in light of this scandal, especially political meddling and dissemination of fake news. The latter issues mostly concerned the American public because of possible implications for domestic politics. In the present study we focus exclusively on privacy related issues.
2. Pew also reported that 54% of survey respondents changed their privacy settings, 42% refrained from checking updates, and 26% deleted the Facebook app from their phones, with younger users showing a greater tendency to do so. Authors of the Pew report interpreted this set of behaviors as a response to the CA scandal. It is important to note, however, that the data were first gathered through the annual Pew American Trends Panel Survey on May 2018 and could reflect a general trend among young users to replace Facebook with other social media platforms (Anderson and Jiang 2018). Second, as indicated above, changing privacy settings has no impact on institutional privacy; it only addresses social privacy. Consequently, this behavior could be unrelated to the scandal or a reflection of users' failure to understand privacy related issues.
3. Facebook's prominence as the leading social network in Israel resembles its usage patterns throughout the western world (Poushter, Bishop, and Chwe 2018). Although the political aspects of the scandal had no direct consequences for Israeli society, the scandal itself did affect Israeli users (data was extracted from nearly 50,000 Israeli accounts, according to Yaron 2018), and the potential privacy risks were covered widely by media outlets. According to *Ifat Digger*, Hebrew media database that archives data from most Israeli media outlets, since the outbreak of the scandal, more than 5000 such items were published outlets (not only websites). Moreover, comparative studies found that while privacy concerns and related behaviors vary among countries and cultures, Israeli internet users are not significantly different from other users in Western industrialized countries (Bellman et al. 2004; Reed, Spiro, and Butts 2016). Hence our approach builds on the notion that while our participants represent a specific social group, their perception of privacy may represent a more general view of a global issue.

   Privacy laws were first introduced in Israel in 1981. A decade later the right for privacy was declared as a basic human right to which Israeli citizens are entitled (akin to a constitutional right). Since then, the laws were modified once, in 2007. Consequently, the current laws are not oriented to new technologies such as social media and smartphones, and do not align with new notions of privacy (Shachaf 2020). The laws are silent regarding the right to be forgotten, withdrawing consent for use of one's data, data portability, and the right to demand and receive explanations about the way data are used. People can learn which company owns which of their data and for what purposes; however, changes or deletions are very difficult. Furthermore, minors' privacy is not

protected (Birnhack 2007, 2019; Shachaf 2020). In effect, although privacy is a constitutional-like right, it is defined vaguely and enforced poorly.

4. Trottier (2016) further differentiated between institutions and markets, suggesting that: "Institutions respond to new conditions of visibility offered by social media … they [institutions] are better suited to watch over target populations … Whereas institutional surveillance sets its gaze on the members of a fixed organization, market surveillance targets relevant demographics. It is an aggregate surveillance based on the collection and processing of information on all Facebook users" (30).
5. It is worth noting that while the studies cited in this section refer to users' perceptions of institutional privacy, most are focused on commercial aspects of such surveillance (much like the current study). Only two studies addressed the question of government surveillance in addition to market surveillance (Padyab et al. 2016; Sujon 2018).
6. The CA scandal resulted in a crisis of legitimacy (Blokker 2011; Johnson, Dowd, and Ridgeway 2006; Vaara 2014). According to Suchman (1995, 547), legitimacy is "a generalized perception or assumption that the actions of an entity are desirable, proper or appropriate within some socially constructed system of norms, values, beliefs and definitions." Facebook, like all social agents, needs legitimacy (Johnson, Dowd, and Ridgeway 2006). How, then, do social actors acquire and maintain legitimacy? According to Patriotta, Gond, and Schultz (2011), alongside formal actions such as legislation, acquisition and maintenance of legitimacy entails symbolic, rhetorical, and discursive work, carried out by the social actors themselves.
7. The students belonged to the upper middle class and are probably more literate than their disadvantaged peers (Marwick and Boyd 2018).
8. Age breakdown was as follows: 36 of the interviewees were ages 21–25, 5 were 26–30, and 5 were above 30.
9. Although relying on a sample of younger users is a common approach, this focus obviously restricts application of conclusions to broader user populations. Young adults who are digital natives (Prensky 2001) "think and process information fundamentally differently from their predecessors. These differences go far further and deeper than most educators suspect or realize" (Prensky 2001, 1).
10. Contrary to this common belief, there are mixed findings regarding the question whether young adults or their elders are more concerned with their privacy on social media (Madden et al. 2014; Malik, Hiekkanen, and Nieminen 2016; Sujon 2018). There is consensus, however, regarding the tendency of younger users to adjust their privacy settings more often than older users (Perrin 2018; Van den Broeck, Poels, and Walrave 2015). Even so, they hardly do so: Young adults tend not to protect their privacy regardless of their familiarity or lack of familiarity with privacy settings (Debatin et al. 2009).
11. When discussing social privacy, participants criticized other users' sharing behavior, decrying their naïveté and illiteracy. For example, Dana spoke of a common fear expressed by numerous participants: "It is very obtrusive, a violation of privacy. We do it to ourselves … We go abroad and share a picture without giving it a second thought. We overshare. Perhaps a thief will see the photo, realize you are not at home and break in. There are a lot of things that we give no thought to but do them anyway." Participants also disapproved of other users' need to share information that should not be made public. Many of them even took exception to their own behavior at a younger age. One participant commented: "It is an intrusion into my personal space that is outside the virtual world of the internet … For example, when I see things, I posted a while back, when I was younger, I now delete them. When I was a teenager, I dealt with topics like depression or altercations. Today, the posts look absurd, so I delete them."
12. This sentiment echoes previous survey data (Madden et al. 2014), suggesting that a majority of users are willing to sacrifice some of their personal data for free online services. In addition, Pew panel dataset shows that 41% (45 out of 109) of young users (ages 18–29) agreed with the statement: "I appreciate that online services are more efficient because of the increased access they have to my personal data" (37).
13. Feelings of powerlessness are not new. In fact, in a post-Snowden study conducted by the Pew Research Center, a vast majority agreed that "consumers have lost control over how personal information is collected and used by companies." or otherwise in their everyday life (Madden et al. 2014, 3). In this sense, such feelings are by no means the result of the scandal (it was yet another example of what users already know), but rather a reflection of the manner in which surveillance culture (Lyon 2017) gained its hold.
14. The all-Israeli participant group had response patterns similar to those found in previous studies conducted in other Western countries, suggesting that our findings in this study are not culture-specific and could be generalized.

Funding

This work was supported by the European Research Council (ERC) [680009].

References

Allmer, T. 2014. (Dis)like Facebook? Dialectical and critical perspectives on social media. *Javnost - The Public* 21 (2): 39–55. doi: 10.1080/13183222.2014.11009144.

Anderson, M., and J. Jiang. 2018. *Teens, social media & technology 2018*. Washington, DC: Pew Research Center. https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/. (accessed November 8, 2020).

Andrejevic, M. 2013. *Infoglut: How too much information is changing the way we think and know*: New York: Routledge.

Andrejevic, M., and K. Gates. 2014. Big data surveillance: Introduction. *Surveillance & Society* 12 (2):185–96. doi: 10.24908/ss.v12i2.5242.

Arts, I., A. E. Buijs, and G. Verschoor. 2018. Regimes of justification: Competing arguments and the construction of legitimacy in Dutch nature conservation practices. *Journal of Environmental Planning and Management* 61 (5–6):1070–84. doi: 10.1080/09640568.2017.1319346.

Baruh, L., and M. Popescu. 2017. Big data analytics and the limits of privacy self-management. *New Media & Society* 19 (4):579–96. doi: 10.1177/1461444815614001.

Beck, J. 2018. People are changing the way they use social media. *The Atlantic*, June 7. https://www.theatlantic.com/technology/archive/2018/06/did-cambridge-analytica-actually-change-facebook-users-behavior/562154/ (accessed November 8, 2020).

Bellman, S., E. J. Johnson, S. J. Kobrin, and G. L. Lohse. 2004. International differences in information privacy concerns: A global survey of consumers. *The Information Society* 20 (5):313–24. doi: 10.1080/01972240490507956.

Birnhack, M. 2007. Control and consent: The theoretical basis of the right to privacy [Hebrew]. *Mishpat Umimshal [Law and Government in Israel]* 11:9–73.

Birnhack, M. 2019. Privacy: A snapshot [Hebrew]. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3336050 (accessed November 8, 2020).

Blokker, P. 2011. Pragmatic sociology: Theoretical evolvement and empirical application. *European Journal of Social Theory* 14 (3):251–61. doi: 10.1177/1368431011412344.

Bogle, A. 2018. Facebook after Cambridge Analytica: Is this the beginning of the end? *ABC News*, March 26. http://www.abc.net.au/news/science/2018-03-27/facebook-after-cambridge-analytica:-what-now/9586604. (accessed November 13, 2020).

Boltanski, L., and L. Thévenot. 2006. *On justification: Economies of worth*: Princeton, NJ: Princeton University Press.

Brewster, T. 2018. Facebook's $660,000 Cambridge Analytica fine is almost meaningless: But that misses the point. *Forbes,* July 11. https://www.forbes.com/sites/thomasbrewster/2018/07/11/facebooks-ico-fine-is-tiny-but-what-of-its-reputation/#40be9bc85519 (accessed November 13, 2020).

Cadwalladr, C., and E. Graham-Harrison. 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*, March 17. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

De Wolf, R., E. Vanderhoven, B. Berendt, J. Pierson, and T. Schellens. 2017. Self-reflection on privacy research in social networking sites. *Behaviour & Information Technology* 36 (5): 459–69. doi: 10.1080/0144929X.2016.1242653.

Debatin, B., J. P. Lovejoy, A. -K. Horn, and B. N. Hughes. 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication* 15 (1):83–108. doi: 10.1111/j.1083-6101.2009.01494.x.

Draper, N. A. 2017. From privacy pragmatist to privacy resigned: Challenging narratives of rational choice in digital privacy debates. *Policy & Internet* 9 (2):232–51. doi: 10.1002/poi3.142.

Fisher, E. 2018. When information wanted to be free: Discursive bifurcation of information and the origins of Web 2.0. *The Information Society* 34 (1):40–8. doi: 10.1080/01972243.2017.1391910.

Freishtat, R. L., and J. A. Sandlin. 2010. Shaping youth discourse about technology: Technological colonization, manifest destiny, and the frontier myth in Facebook's public pedagogy. *Educational Studies* 46 (5):503–23. doi: 10.1080/00131946.2010.510408.

Fuchs, C. 2012. The political economy of privacy on Facebook. *Television & New Media* 13 (2):139–59. doi: 10.1177/1527476411415699.

Gartenberg, C. 2019. Facebook keeps growing despite scandals and privacy outrage. *TheVerge.com*, January 30. https://www.theverge.com/2019/1/30/18204186/facebook-q4-2018-earnings-user-growth-revenue-increase-privacy-scandals (accessed March 3, 2019).

Giulianotti, R., and T. Langseth. 2016. Justifying the civic interest in sport: Boltanski and Thévenot, the six worlds of justification, and hosting the Olympic games. *European Journal for Sport and Society* 13 (2):133–53. doi: 10.1080/16138171.2016.1183930.

Golbeck, J. and S. Aral. 2018. Why the Cambridge Analytica scandal is a watershed moment for social media. http://knowledge.wharton.upenn.edu/article/fall-out-cambridge-analytica/ (accessed November 13, 2020).

Griggs, I. 2018. "A watershed moment": Have people woken up to how their Facebook is used following the Cambridge Analytica scandal? *PR Week,* March 22. https://www.prweek.com/article/1460137/a-watershed-moment-people-woken-facebook-data-used-following-cambridge-analytica-scandal (accessed November 13, 2020).

Hargittai, E., and A. Marwick. 2016. What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication* 10:3737–57.

Hern, A. 2019. Facebook usage falling after privacy scandals, data suggests. *The Guardian,* June 20. https://www.theguardian.com/technology/2019/jun/20/facebook-usage-collapsed-since-scandal-data-shows (accessed November 23, 2020).

Hoffmann, A. L., N. Proferes, and M. Zimmer. 2018. Making the world more open and connected": Mark Zuckerberg and the discursive construction of Facebook and its users. *New Media & Society* 20 (1):199–218. doi: 10.1177/1461444816660784.

Hoffmann, C. P., C. Lutz, and G. Ranzini. 2016. Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10 (4):1–18. doi: 10.5817/CP2016-4-7.

Insider Intelligence. 2020. Facebook ranks last in digital trust among consumers. *Business Insider*, September 24. https://www.businessinsider.com/facebook-is-consumers-least-trusted-social-media-platform-2020-9?r=DE&IR=T

Jansson, A. 2012. Perceptions of surveillance: Reflexivity and trust in a mediatized world (the case of Sweden). *European Journal of Communication* 27 (4):410–27. doi: 10.1177/0267323112463306.

Johnson, C., T. J. Dowd, and C. L. Ridgeway. 2006. Legitimacy as a social process. *Annual Review of Sociology* 32 (1):53–78. doi: 10.1146/annurev.soc.32.061604.123101.

Kahn, C., and D. Ingram. 2018. Americans less likely to trust Facebook than rivals on personal data. *Reuters.com*, March 25. https://www.reuters.com/article/us-facebook-

cambridge-analytica-apology/americans-less-likely-to-trust-facebook-than-rivals-on-personal-data-idUSKBN1H10AF (accessed November 23, 2020).

Lutz, C., and G. Ranzini. 2017. Where dating meets data: Investigating social and institutional privacy concerns on Tinder. *Social Media + Society* 3 (1):1–12.

Lyon, D. 2017. Surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of Communication* 11:824–42.

Madden, M.,. L. Rainie, K. Zickuhr, M. Duggan, and A. Smith. 2014. Public perceptions of privacy and security in the post-Snowden era. Washington, DC: Pew Research Center. https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/ (accessed November 12, 2020).

Mai, J.-E. 2016. Big data privacy: The datafication of personal information. *The Information Society* 32 (3):192–9. doi: 10.1080/01972243.2016.1153010.

Malik, A., K. Hiekkanen, and M. Nieminen. 2016. Privacy and trust in Facebook photo sharing: Age and gender differences. *Program* 50 (4):462–80. doi: 10.1108/PROG-02-2016-0012.

Marwick, A. E., and d Boyd. 2018. Understanding privacy at the margins. *International Journal of Communication* 12:1157–65.

Marwick, A., and E. Hargittai. 2019. Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society* 22 (12):1697–713. doi: 10.1080/1369118X.2018.1450432.

Nam, S. 2020. Cognitive capitalism, free labor, and financial communication: A critical discourse analysis of social media IPO registration statements. *Information, Communication & Society* 23 (3):420–36. doi: 10.1080/1369118X.2018.1510535.

Nyberg, D., and C. Wright. 2012. Justifying business responses to climate change: Discursive strategies of similarity and difference. *Environment and Planning A: Economy and Space* 44 (8):1819–35. doi: 10.1068/a44565.

O'Hagan, E. M. 2018. No one can pretend Facebook is just harmless fun any more. *The Guardian,* March 18. https://www.theguardian.com/commentisfree/2018/mar/18/facebook-extremist-content-user-data (accessed November 13, 2020).

Padyab, A., T. PäIväRinta, A. Sta˚HlbröSt, and B. Bergvall-Ka˚Reborn. 2016. Facebook users attitudes towards secondary use of personal information. Paper presented at the Thirty Seventh International Conference on Information Systems, Dublin, December. https://www.diva-portal.org/smash/get/diva2:1049575/FULLTEXT02. (accessed November 13, 2020).

Padyab, A., T. Päivärinta, A. Ståhlbröst, and B. Bergvall-Kåreborn. 2019. Awareness of indirect information disclosure on social network sites. *Social Media + Society* 5 (2): 205630511882419–4. doi: 10.1177/2056305118824199.

Patriotta, G., J. -P. Gond, and F. Schultz. 2011. Maintaining legitimacy: Controversies, orders of worth, and public justifications. *Journal of Management Studies* 48 (8): 1804–36. doi: 10.1111/j.1467-6486.2010.00990.x.

Perrin, A. 2018. Americans are changing their relationship with Facebook. PewResearch.org, September 5. https://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/ (accessed November 13, 2020).

Poushter, J., C. Bishop, and H. Chwe. 2018. Social media use continues to rise in developing countries but plateaus across developed ones. Washington, DC: Pew Research Center. https://medienorge.uib.no/files/Eksterne_pub/Pew-Research-Center_Global-Tech-Social-Media-Use_2018.06.19.pdf (accessed November 12, 2020).

Prensky, M. 2001. Digital natives, digital immigrants – Part 1. *On the Horizon* 9 (5):1–6. doi: 10.1108/10748120110424816.

Raynes-Goldie, K. S. 2010. Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday* 15 (1). https://firstmonday.org/article/view/2775/2432 (accessed November 13, 2020).

Reed, P. J., E. S. Spiro, and C. T. Butts. 2016. Thumbs up for privacy? Differences in online self-disclosure behavior across national cultures. *Social Science Research* 59: 155–70. doi: 10.1016/j.ssresearch.2016.04.022.

Reinecke, J., K. van Bommel, and A. Spicer. 2017. When orders of worth clash: Negotiating legitimacy in situations of moral multiplexity. In *Justification, evaluation and critique in the study of organizations: Contributions from French pragmatist sociology,* eds. C. Cloutier, J-P. Gond, and B. Leca, 33–72. Bingley, UK: Emerald Publishing Limited.

Sevignani, S. 2015. *Privacy and capitalism in the age of social media*. New York: Routledge.

Shachaf, T. 2020. In Israel, no one is interested in your privacy [Hebrew]. *Ynet*, January 31. https://www.ynet.co.il/digital/technology/article/H1V1NdWGL (accessed November 13, 2020).

Shade, L. R., and T. Shepherd. 2013. Viewing youth and mobile privacy through a digital policy literacy framework. *First Monday* 18 (12):13–2020. https://firstmonday.org/ojs/index.php/fm/article/view/4807/3798. (accessed November). doi: 10.5210/fm.v18i12.4807.

Stutzman, F., R. Gross, and A. Acquisti. 2013. Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality* 4 (2):7–41. doi: 10.29012/jpc.v4i2.620.

Suchman, M. C. 1995. Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review* 20 (3):571–610. doi: 10.5465/amr.1995.9508080331.

Statt, N. 2018. Facebook growth slows in aftermath of privacy scandals. *TheVerge.com*, June 25. https://www.theverge.com/2018/7/25/17614518/facebook-q2-2018-earnings-cambridge-analytica-scandal-growth-stalling (accessed November 23, 2020).

Sujon, Z. 2018. The triumph of social privacy: Understanding the privacy logics of sharing behaviors across social media. *International Journal of Communication* 12:3751–71.

Trottier, D. 2016. *Social media as surveillance: Rethinking visibility in a converging world*. New York: Routledge.

Turow, J., M. Hennessy, and N. Draper. 2015. The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820060 (accessed November 13, 2020).

Ur Rehman, I. 2019. Facebook-Cambridge Analytica data harvesting: What you need to know. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=5833&context=libphilprac (accessed November 13, 2020).

Vaara, E. 2014. Struggles over legitimacy in the Eurozone crisis: Discursive legitimation strategies and their

ideological underpinnings. *Discourse & Society* 25 (4): 500–18. doi: 10.1177/0957926514536962.

Van den Broeck, E., K. Poels, and M. Walrave. 2015. Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood. *Social Media + Society* 1 (2):1–11.

van Dijck, J. 2013. *The culture of connectivity: A critical history of social media*. Oxford, UK: Oxford University Press.

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

Weisbaum, H. 2018. Trust in Facebook has dropped by 66 percent since the Cambridge Analytica scandal. *NBCNews.com*, April 18. https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-per-cent-cambridge-analytica-scandal-n867011 (accessed November 23, 2020).

Yaron, O. 2018. Facebook: 50,000 Israelis may have been exposed to Cambridge Analytica breach. *Ha'Aretz*, April 10. https://www.haaretz.com/israel-news/.premium-cambridge-analytica-breach-facebook-says-50k-israelis-data-at-risk-1.5990701 (accessed November 12, 2019).

Young, A. L., and A. Quan-Haase. 2013. Privacy protection strategies on Facebook: The internet privacy paradox revisited. *Information, Communication & Society* 16 (4): 479–500. doi: 10.1080/1369118X.2013.777757.