Article

new media & society
1–16
© The Author(s) 2019
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/1461444819833331
journals.sagepub.com/home/nms
SAGE

The corporate cultivation of digital resignation

Nora A Draper
University of New Hampshire, USA

Joseph Turow
University of Pennsylvania, USA

Abstract

The aim of this article is to propose a theoretical framework for studying digital resignation, the condition produced when people desire to control the information digital entities have about them but feel unable to do so. We build on the growing body of research that identifies feelings of futility regarding companies' respect for consumer privacy by suggesting a link between these feelings and the activities of the companies they benefit. We conceptualize digital resignation as a rational response to consumer surveillance. We further argue that routine corporate practices encourage this sense of helplessness. Illuminating the dynamics of this sociopolitical phenomenon creates a template for addressing important questions about the forces that shape uneven power relationships between companies and publics in the digital age.

Keywords
Privacy, privacy paradox, privacy policy, resignation, transparency

Introduction

Beginning in March 2018, news reports emerged about the unauthorized use of Facebook data by the political marketing firm Cambridge Analytica during the 2016 US Presidential election and the British referendum regarding withdrawal from the European Union in

Corresponding author:
Nora A Draper, Department of Communication, University of New Hampshire, 20 Academic Way, Durham, NH 03824, USA.
Email: nora.draper@unh.edu

the same year (Cadwalladr and Graham-Harrison, 2018). Although use of the acquired data for political campaigning violated Facebook's policies, critics pointed to the social network site's lenient rules governing data collection by third party apps as having enabled the misuse (Tufekci, 2018a). These reports were followed by a slew of calls for individuals to delete Facebook. While some news reports highlighted anecdotal evidence that individuals were closing their accounts (Hsu, 2018), others described instances where people had decided to maintain their presence on Facebook despite growing privacy concerns (Glaser, 2018; Wren, 2018).

Commentators have seized on the inaction of large segments of the public in response to the Facebook revelations and similar incidents as representing a "privacy paradox"—that is the idea that although people say they care about information privacy, they often behave in ways that contradict those claims (Barnes, 2006; Kokolakis, 2017). Explanations for the alleged paradox commonly describe people as uninformed about the ways their personal information is collected and used (Dommeyer and Gross, 2003; Park, 2013) or engaged in a rational cost–benefit analysis, disclosing only when they conclude the rewards accrued by sharing their data outweigh the possible risks (e.g. Westin, 2003; see also Draper, 2017; Hoofnagle and Urban, 2014).

More recently, however, a few studies have converged on an alternative explanation for the inaction, limited actions, or inconsistent actions that individuals take in relation to their privacy concerns: they are resigned. That is, while these people feel dissatisfied with the pervasive monitoring that characterizes contemporary digital spaces, they are convinced that such surveillance is inescapable. Yet, while recent empirical research has begun to consider futility and helplessness in the face of threats to data use, what is missing is a theoretical framework for understanding the phenomenon and driving new avenues of research regarding it. To address this absence, the present article builds on those studies in the context of scholarship from social psychology, critical sociology, and anthropology to offer a multi-faceted perspective on the causes and nature of digital resignation. In doing so, we delineate this concept as a sociopolitical phenomenon that simultaneously involves rational individual responses to corporate surveillance practices and patterned corporate practices which cultivate those responses.

To that end, the article has four aims: (1) to review recent empirical research to establish digital resignation as a contemporary social phenomenon, (2) to situate the concept of digital resignation within broader theoretical work that suggests it involves rational individual responses to seemingly inevitable conditions, (3) to provide a framework for examining and exploring how routine corporate practices of obfuscation may operate to cultivate and benefit from digital resignation, and (4) to identify key social and research implications emerging from this perspective.

Digital resignation as a contemporary phenomenon

The pervasiveness of resignation shows up in our 2015 empirical study (Turow et al., 2015, see also Draper, 2017). The US national survey, the results of which are detailed in a report entitled *The Tradeoff Fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation*, explores Americans' responses to the implicit deal that resides at the heart of many contemporary interactions, both digital and non-digital: personal information in exchange for content, promotions, or improved service. In this report, we characterize 58% of respondents as resigned based on their agreement with two statements: "I want control over what marketers can learn about me online" and "I've come to accept that I have little control over what marketers can learn about me online."[1] The *Tradeoff Fallacy* describes a pervasive feeling among Americans that the corporate practice of trading access to services and content for personal information is unfair (on issues of "fairness," see also Kennedy et al., 2017). It explores Americans' sense of resignation—as opposed to a calculated logic of trading data for benefits—through questions about supermarket shopping and loyalty programs. For example, the study finds that a large proportion of Americans—43%—say they would agree to let supermarkets collect data about them despite indications elsewhere in the survey that they disagree with consumer surveillance. The report also finds that knowledge of marketplace realities does not neatly correlate with support for or rejection of consumer tracking. Moreover, the more that Americans know about the laws and practices of digital marketing, the more likely they are to be resigned.

In the wake of *The Tradeoff Fallacy*, a handful of additional studies identified related sentiments, signaling a zeitgeist around the notion of digital resignation. Discussing focus groups with college students in the United States, Eszter Hargittai and Alice Marwick (2016) observe frustration as social media users describe efforts to negotiate between their desire to manage their digital privacy and the seeming inevitability that those efforts will be undermined. Hargittai and Marwick use the term resignation to refer to people's feeling that they are powerless to avoid the unwanted privacy violations that could occur as a result of any number of situations, from an online platform changing its privacy settings to a friend or family member sharing unwanted information. In a related article, Marwick and Hargittai (2018) describe the choices individuals make to disclose information to institutions. Although their respondents describe several advantages of information sharing—including content personalization, improved service, and convenience—the authors nevertheless find that compulsory engagement with structures that demand information disclosure reduce participants' sense of control. Feelings of resignation, they write, come from a perception that privacy violations are unavoidable (Hargittai and Marwick, 2016: 11).

Using a similar construction, Christian Hoffman et al. (2016) argue that when individuals are overwhelmed by threats to their ability to control how institutions access and use their personal data, they develop an attitude the authors call "privacy cynicism." Based on focus groups with internet users in Germany, the authors argue that while individuals recognize risks to their information privacy, they also describe a lack of power over the situation. They define privacy cynicism as "an attitude of uncertainty, powerlessness and mistrust towards the handling of personal data by online services, rendering privacy protection behavior subjectively futile" (Hoffman et al., 2016). Similar to Turow et al. (2015), Hoffman et al. find greater awareness regarding privacy risks corresponds to stronger feelings of powerlessness (see also Xie et al., 2018). Being resigned does not indicate a complete abdication of efforts to shield oneself from corporate surveillance. The studies cited here reveal that those who are resigned often engage in privacy guarding behaviors, but that they do not always feel those efforts are successful (see also Selwyn and Pangrazio, 2018).

Other studies hint at digital resignation without using that term or its precise formulation. For example, a 2016 Pew Research Center report reveals that over half of Internet users in the United States have "taken steps to avoid observation by specific people, organizations or the government" with large majorities reporting that is it "very important" to them that they be in control of who can access their information and what information is being collected (Rainie, 2016). And yet, that same report describes over 90% of Americans as agreeing that "consumers have lost control of how personal information is collected and used by companies." In a study of social activists in the United Kingdom, Lina Dencik et al. (2016) observe a reliance on mainstream communication platforms that limit options for enhanced privacy protection even among those who might be expected to seek data management strategies that support their anti-surveillance positions. The authors describe the participants as concerned about behavioral tracking and data collection, and at the same time dependent on platforms where these practices take place to support their activist efforts. Academics who identify what we here term digital resignation encourage research on the topic precisely because they recognize its pervasiveness has anti-social implications: a futility about technological systems that causes people to despair about their ability to guide their futures. Their hope, sometimes explicit and sometimes implicit, is that identifying resignation as a social problem will allow it to be addressed through public policy.

Toward a theoretical framework of resignation

While the recent empirical research cited above has begun to consider privacy fatigue, frustration, and helplessness in the face of threats to data use, what is missing is a theoretical perspective to place the phenomenon within the large-scale social context. To build this framework, we turn to a small but wide-ranging scholarly literature that engages with resignation from two perspectives. The first focuses on how individuals negotiate feelings of helplessness in crisis situations. The second emphasizes corporate attempts to encourage feelings of futility and cynicism to protect their interests.

In an early example of social psychological writings in this area, Robert Forman (1963) observed the relationship between resignation and individual responses during a crisis. He noted that most people in a midwestern town, upon hearing an air raid siren that signaled an incoming nuclear strike, paid little attention to the alert and went about their daily routines. When asked about their lack of action, town residents offered several responses: they did not know what action to take, they did not believe an airstrike was coming, or they saw no point in attempting to protect themselves if, indeed, a nuclear attack was imminent. This third conclusion, that nothing could be done, justifies what Forman (1963) called "fatalistic passivity," a response he described as "strangely comforting rather than alarming" (p. 289).

Carl Hammerschlag and Boris Astrachan (1971) pointed to a similar set of social dynamics in their assessment of collective behavior during an airport shutdown. Based on participant observation during a multiday snow-in at John F. Kennedy airport in 1969, the authors disputed theories that suggest, during a crisis, people band together to form a collective. Rather they observed that a lack of individual expertise through which to address the problem coupled with an absence of shared tasks that might unite them displaced collective unity and encouraged dependence on the technological systems and organizational structures that created the crisis (Hammerschlag and strachan, 1971: 303). Without the possibility of collective mobilization, the authors suggested, the would-be passengers reacted with resignation and apathy. The result, Hammerschlag and Astrachan contended, was the perception of isolation despite the existence of a group that shared similar frustrations and goals.

By offering resigned passivity as an understandable alternative to collective or individual action, Hammerschlag and Astrachan joined Forman in arguing that inaction, which could be interpreted as apathy, might instead constitute a rational response to a seemingly inevitable outcome. The critical social theorist Theodor Adorno indirectly supported that view. Just as Forman argued inaction is a reasonable reaction to a crisis in which the individual holds little power—in instances, for example, where individual action is unlikely to alter prevailing social, political, or economic forces—the decision not to engage may be a justifiable act of self-preservation. In defense of charges that he was doing too little in response to the power of the cultural industries to shape social reality, Adorno (2005) addressed the ethical implications of his decision not to engage in active protest. For Adorno, action for action's sake—that is, action that does not result in a dismantling of the status quo—was itself a version of resignation. Extending the argument a step further, Adorno argued the futile acts of the individual may do more to ensconce systemic power than to dispel it (see Bell, 2014). Rather than interpreting inaction as a sign of disengagement or a lack of concern, Adorno proposed that failure to take on a system that is designed to thwart the efforts of an individual is not only a reasonable reaction, but also a critical one.

Taken together, these perspectives suggest that feelings of resignation are a rational emotional response in the face of undesirable situations that individuals believe they cannot combat. The approach has similarities to the psychological theory of learned helplessness. It explains people's feelings of powerlessness and passivity when their actions to change circumstances appear routinely unconnected to subsequent outcomes (Peterson et al., 1993). When applied to digital privacy, scholarly writing has pointed out that companies, including online advertisers, benefit from learned helplessness insofar as people tend not to dramatically alter their behaviors when they learn about unwelcome data practices (see Shklovski et al., 2014). However, research has not yet examined the ways institutional systems encourage feelings of futility that benefit corporate interests. The approaches of Forman, Hammerschlag and Astrachan, and Adorno underscore the importance of noting those factors. They also point out that individual actions to reverse institutionally created circumstances may worsen the situations rather than improve them. Their arguments offer a counterpoint to the rationale of media resistance efforts in which individuals opt out of technical systems with the aim of altering the conditions that led to their dissatisfaction (Portwood-Stacer, 2013; Woodstock, 2014). Digital media firms clearly have an interest in discouraging media resistance—especially of the collective kind—among people concerned about their privacy and instead encouraging their feelings of resignation.

Key insights into the corporate processes that encourage digital resignation come from anthropologists Peter Benson and Stuart Kirsch (2010). They argue that capitalist systems benefit from the cultivation of resignation as a strategy to neutralize critical or political action. Resignation supports capitalism by constructing corporate power as an inevitable and immovable feature of contemporary life. They draw empirical support from a study of controversies centering on the tobacco and mining industries. They identify a set of predictable corporate responses to crises: first denial, then acknowledgment, and finally token accommodations and strategic engagement. They conclude that these routine responses aim to encourage public feelings of futility about the possibility of changing unwanted industry practices.[2] The authors propose that the public sense of helplessness allows companies in the tobacco and mining industries to cultivate a "politics of resignation" wherein they benefit from cynicism about the possibility for change. Benson and Kirsch's research converges on the scholarly and policy implications of industries' routinized crisis management responses aimed at undermining public frustrations that might otherwise coalesce into collective civic action. Their works suggests the importance of observing whether digital firms' ritualized communication patterns perform a predictable public rhetoric to instantiate similar feelings of resignation.

Benson and Kirsch argue that industrially cultivated futility is particularly pervasive in the United States. Dencik and Cable (2017), however, identify similar developments among politically active citizens in the United Kingdom. Focusing specifically on attitudes toward the collection of digital data in the post-Snowden era, they point to a lack of transparent data practices coupled with limited knowledge and control as producing a condition they refer to as "surveillance realism." Here, Dencik and Cable (2017) draw on the concept of "capitalist realism," (pp. 764–765) which identifies a belief that, despite its significant limitations, capitalism is the only feasible political-economic system (see also Dencik, 2018). Surveillance realism, they write, relies on a "lack of transparency and knowledge in conjunction with the active normalization of surveillance through discursive practices and institutional sanctions manifested in its ubiquity" as a strategy "to negate prominent concerns, ultimately limiting possibilities for alternative imaginations of organizing society" (Dencik and Cable, 2017: 777). Structures that normalize and justify contemporary surveillance systems, they argue, work to undermine alternatives even as concerns about pervasive monitoring persist.

The patterns noted in these industries also exist among firms that traffic in consumer surveillance. The works of Benson and Kirsch, along with Dencik and Cable, suggest two sociopolitical elements of digital resignation that reveal its benefits to corporations. The first is that digital resignation is often experienced at the individual, not collective, level among those who feel they lack sufficient influence or capabilities.[3] The second, a consequence of the first, is that despite individuals' worries about surveillance and data flows they cannot control, their concerns are unlikely to be accompanied by collective anger that motivates action to change the status quo. Rather, resignation likely results in frustration that such action would be futile. It stands to reason, then, faced with the danger of collective anger and withdrawal in response to their surveillance practices, companies have an interest in cultivating resignation. The upshot is that digital resignation becomes more than the reality of modern life that Hargittai and Marwick (2018), Hoffman et al. (2016), and Rainie (2016) suggest. Rather, it is in part a consequence of routine business practices that operate to forestall collective public anger at what a number of scholars describe as surveillance capitalism (Foster and McChesney, 2004; Wood and Ball, 2013; Zuboff, 2015).

The corporate cultivation of digital resignation

What corporate behaviors lead people to feel resigned about contemporary data collection practices rather than angry and motivated toward change? The answer lies in widespread obfuscatory communication practices used by companies across the digital-media landscape that cultivate confusion and cynicism regarding the collection and use of personal data. We use obfuscation differently from the way Finn Brunton and Helen Nissenbaum deploy it in their book *Obfuscation: A User's Guide for Privacy and Protest*. Although they note the potential for powerful players to engage in obfuscatory actions (Brunton and Nissenbaum, 2015: 9), Brunton and Nissenbaum (2015) focus on obfuscation as a strategy for citizen protection: "the deliberate addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection" (p. 1). Our use of the term, by contrast, emphasizes companies' interest in discouraging individuals from the kinds of actions which Brunton and Nissenbaum advocate. Ours is a definition that is more consistent with Glenn Ellison and Sarah Fisher Ellison's (2009) use of obfuscation to describe efforts that benefit corporations by introducing frictions that frustrate consumers (p. 427). Regardless of corporate intent, Ellison and Ellison argue, the consequence of these practices is to provoke confusion and discouragement among individuals.

Research in related fields identifies the organizational pattern we suggest is taking place within the context of consumer surveillance. Torin Monahan (2016) describes how firms' technological systems deliberately mislead individuals by presenting them with the illusion of control. Sarah T Roberts (2018), writing specifically about social media firms, suggests that through a combination of obfuscation and secrecy, digital platforms cultivate an "operating logic of opacity" that discourages users from efforts to understand or engage these systems. The industrial and organizational dynamics suggested by Roberts and Monahan are evident in the context of privacy concerns (see also Norwegian Consumer Council, 2018). Under the rubric of self-regulation, companies engage in obfuscatory strategies and tactics that cultivate the perception that efforts at control are pointless. The result is to encourage feelings of resignation by conveying a sense of normalcy around consumer surveillance practices and discouraging collective action.

Two common strategies that companies use to convey a commitment to consumer privacy, privacy policies and transparency initiatives, illustrate this practice. In the course of their activities, firms draw on four interrelated rhetorical tactics that embody the obfuscation process: placation, diversion, jargon, and misnaming. Placation involves efforts to falsely appease concerns. Diversion refers to efforts to shift individuals' focus away from controversial practices. The use of jargon—terminology that is difficult for those outside a specific group to understand—not only generates confusion, but may frustrate efforts at comprehension. Similarly, misnaming describes efforts to occlude industrial practices through the use of misleading labels. Here, we consider how these tactics operate in the case of privacy policies and transparency initiatives.

Privacy policies

Data use notices, most often referred to as "privacy policies," have been a feature of websites since the 1990s (Anthony, 2001, Turow et al., 2018a). From an organizational standpoint, the privacy policy, strongly urged by the Federal Trade Commission (FTC), is a legal document that offers clarity around a website's data collection and handling practices thereby supporting a framework for privacy based on principles of notice and choice (Reidenberg et al., 2015: 43). These documents have been instrumental in supporting industry self-regulation around digital privacy (Milne and Culnan, 2002).

Despite their role as "the single most important source of information for users to attempt to learn how companies collect, use, and share data" (Reidenberg et al., 2015: 41), debates over the effectiveness of privacy policies began almost as soon as they were introduced. Researchers have found that the US population consistently misunderstands the meaning of the term *privacy policy*. National survey research conducted between 2003 and 2015 finds that a majority of Americans believe incorrectly the mere presence of a privacy policy indicates a website will not share information without permission (Turow et al., 2018a). Although the FTC has recognized consumers' confusion regarding this wording (Hoofnagle, 2016: 294), privacy policy remains the most common name for these documents. The persistent use of this misleading label is consistent with the obfuscating practice we identify as misnaming (Turow et al., 2018a). If individuals are content that the existence of a privacy policy offers them protection, they may be unlikely to engage further with the document. Thus, the privacy policy label itself may function to divert attention away from its contents.

But even when users decide to engage with a website or app's privacy policy, there are significant barriers to their effectiveness. Not only does research find the documents take a long time to read (McDonald and Cranor, 2008), but their linguistic complexity means they are difficult to understand (Milne and Culnan, 2002; Reidenberg et al., 2015; Turow et al., 2018a). The result is that people frequently avoid privacy policies (Milne and Culnan, 2004; Obar and Oeldorf-Hirsch, 2018a), which further reduces their efficacy in providing consumers with sufficient notice about how their personal information will be used.

Based on a systematic critical linguistic analysis of privacy policies, Irene Pollach (2005) argues these documents use opaque and vague terminology in order to limit comprehension and discourage careful reading. This obfuscatory strategy—the use of jargon in the documents—discourages engagement with information about how data are collected and used. Those behind the policies, Pollach (2005) writes, "benefit from obfuscating, mitigating and enhancing data handling practices in that this helps them to obtain data they would not have access to if users were fully informed about data handling practices" (p. 232). Pollach points to the challenges of determining whether the construction of privacy policies represents intentional efforts to occlude corporate practices. Nevertheless, she argues, the resulting confusion functions to inhibit informed consent and provides companies with access to information they would be otherwise unlikely to obtain (see also Obar and Oeldorf-Hirsch, 2018b). The puzzling, difficult-to-understand details that firms present to individuals as a routine part of their everyday engagement with technical systems are unlikely to reduce feelings of helplessness.

Transparency initiatives

In addition to privacy policies, some firms have introduced what they characterize as transparency tools to respond to critiques regarding the clarity of their data practices.

These tools allow individuals to view and amend the information companies have about them. The search engine giant Google, for example, launched its "privacy dashboard" in 2009 to provide users with "a high-level summary of everything Google knows about you by virtue of the Google products you use" (Schonfeld, 2009). Facebook has a tool called "ad preferences" that shows which advertisers a user has engaged with as well as the interest categories the platform has identified based on user behavior (Griffin, 2016). In response to the Cambridge Analytica revelations, Facebook pointed users to a site where they could download all information the company had collected about them (Google has a similar feature called Google Takeout) (Chen, 2018). And in 2013, the data broker Acxiom introduced its "About the Data" feature, which allows individuals to review some of the data the company has collected across several categories—including demographic, residential, vehicle, economic, purchase history, and interests—and even provides users with some ability to amend the information.

But in the context of self-regulation, these "transparency" initiatives become part of an obfuscation process that often uses the rhetoric of placation and diversion. For example, examining Acxiom's "About the Data" program, Matthew Crain (2018) finds that the program's website placates—or falsely calms—visitors by suggesting individuals are empowered to control their digital data. In fact, the initiatives give little insight into the firm's actual practices. Crain's work points to another rhetorical tactic of obfuscation: diversion. He notes that Acxiom continues its industry's tradition of not providing the levels of disclosure necessary to achieve actual transparency. Instead, Acxiom's portal diverts its audience from the realities of the firm's activities. Doing so "exemplifies the political expediency of transparency for companies looking to continue or expand their surveillance practices unimpeded by consumer protection regulations" (Crain, 2018: 92). The rhetoric of placation—which is also present in privacy policies that strive to ease user concerns—comes in the form of a concession to user control that does little to shift the power imbalance between data collectors and the data subjects.

Mike Ananny and Kate Crawford (2018) reinforce this point, noting that "the implicit assumption behind calls for transparency is that *seeing* a phenomenon creates opportunities and obligations to make it accountable and thus to *change* it" (Ananny and Crawford, 2018: 974, emphasis in original). They describe the promise of transparency as being rooted in the connection between seeing, knowing, and controlling. The result of faux institutionalized openness—including the transparency initiatives and privacy policies noted here—is a sense that one has been granted access to the concealed systems (Pasquale, 2015) that inform technical processes without the necessary tools to make sense of the information to which one has been granted access. Moreover, insofar as privacy policies and transparency campaigns provide a misleading sense of the data collected or grant access to a limited selection of information, they discourage insight that considers how these data circulate as part of the broader systems that give them meaning.

The consequence of the rhetorical strategies that support both privacy policies and transparency initiatives is therefore to present people with information about data flows and uses that are so complex and contradictory that they yield two concurrent outcomes: (1) the companies can argue to individuals and government agencies that they have provided explanations of their data practices, while (2) individuals will consider the enterprise of engaging with the placations, diversions, jargon, and misnaming time consuming, confusing, and ultimately futile. Companies also discourage individuals from enlisting collective anger about, or even opting out of, commercial data retrieval, by highlighting conveniences and delights that come from engagement within systems that carry out surveillance (see Troullinou, 2017 on "seductive surveillance"). Searching for information, viewing videos, sharing photos, and playing games alone or with others are just a few of the pleasurable activities individuals enjoy regularly as firms trace what they do. Jennifer Whitson (2013) observes, for example, how the inclusion of gamification strategies in self-tracking tools emphasizes the enjoyable aspects of surveillance, thereby diverting attention from activities that may cause concern.

Understanding ways out of digital resignation

One implication of the corporate cultivation of digital resignation is that it turns individual concerns about surveillance and privacy inward, leading individuals toward confusion and indecision (rather than toward collective action) about whether and how to take on the burdens of privacy self-management (see Solove, 2013). As Adorno understood, the heart of the problem relates to corporate efforts aimed at disempowering the collective while keeping the focus on the individual. Implicitly agreeing, Julie Cohen (Forthcoming) argues that this view of privacy as centering on personal choice has proven untenable for finding a way to reshape the relationship citizens have with companies when it comes to their data (pp. 1–2). In fact, strategies that gesture publicly to individual control may function to depoliticize frustrations around privacy that could encourage collective action (Gürses et al., 2016). Consider, for example, calls to #DeleteFacebook in response to the Cambridge Analytica revelations discussed previously. As Laura Portwood-Stacer (2014) writes, media refusal—including independent decisions to "quit Facebook"—reflects efforts to intercede in social problems at the level of individual behavior (p. 1053). Several observers point out, moreover, that while decisions to end engagement with the social media platform could result in personal satisfaction, they are unlikely to bring about meaningful change (González-Bailón and Gorham, 2018; Statt, 2018; Vaidhyanathan, 2018). Even those who suspend their engagement with social media often return (Baumer et al., 2015). Too, action directed only at Facebook ignores the broader surveillance ecosystems in which myriad companies engage in similar data collection practices. Although individuals may be empowered to make independent choices, individual actions infrequently aggregate to facilitate changes in industrial infrastructure that result in collective empowerment or systemic change (Cohen, Forthcoming; see also Roessler, 2005 and Steeves, 2009).

Adorno (2005) would not have been surprised by this predicament. He implied that his decision not to engage directly with powerful cultural institutions was informed in part by his belief that individual action cannot address social problems. These one-off approaches rarely result in broad social change not necessarily because they fail to elicit widespread engagement, but because individual responses seldom succeed in undermining powerful systems. The Black feminist thinker, writer, and poet Audre Lorde takes this thinking in a more liberating direction. Lorde, unlike Adorno, did not submit to the inevitability of existing power structures or view inaction as the most effective form of resistance. In now-famous comments at the Second Sex Conference, held in New York City on 29 September 1979, Lorde concurred there are limitations of resistance within a system designed to marginalize and disenfranchise. However, where Adorno's response was to resist "action for action's sake," Lorde emphasized the necessity of action, stressing the need for collective participation to undermine the status quo. As Lester Olson (2000) writes, Lorde critiqued the practices of feminist reformers who work "to dismantle some forms of oppression and privilege across sex difference while perpetuating them across race, sexuality, age, or class because of feminists' unacknowledged desire to keep some symbolic and material privileges" (p. 261). Olson (2000) describes these comments as designed to incite a collective anger in her audience that would "challenge reformist feminists to become radical feminists" (p. 261). Lorde, Olson (2000) writes, wanted "to transform the uses of power, not reproduce them ironically in the process of protesting them" (p. 262). To define meaningful action, she considered it crucial to understand the ways systems work to encourage isolation and silence in the face of oppression, anger, and fear (Lorde, 2007).

One of the puzzles in the face of pessimistic views of social dynamics is to figure out ways to disrupt the rhetorical strategies, tactics, and technical tools that industries use to atomize groups and convince the public about the inevitability of data use while they remain reassuring regarding the consequences of these practices. Yielding informed suggestions for ways out of digital resignation requires systematic scholarly work. The work so far indicates a number of conundrums. Research suggests that merely providing information about data privacy threats may deepen rather than counter feelings of resignation (Hoffman et al., 2016; Turow et al. 2015). Moreover, because those who are resigned can exhibit behaviors that are similar to those who express indifference about digital surveillance, resignation can obscure signals that people care deeply about privacy. Failure to recognize digital resignation, therefore, allows to go uncontested arguments that people are willingly and knowingly consenting to take part in technical systems that harvest their personal information.

These findings point to a need for additional research that not only considers the pervasiveness and nature of resignation but questions the broader sociopolitical landscape around this emotion. What contributes to feelings of resignation? How might resignation look different among different communities and populations? How does resignation relate to people's willingness to engage in collective action to press for new policies regarding corporate use of data? Using the theoretical framework presented here, the scholarly and activist mandate is to explore in depth the structural and rhetorical ways commercial forces encourage digital resignation among populations. To do so, we must examine how individuals respond to specific broad corporate strategies (such as, but not only, privacy policies and transparency initiatives) and the rhetorical tactics connected to them (using approaches such as—but not only—placation, diversion, jargon, and misnaming). And we must also assess systematically how and to what extent resignation prevents individual frustration from being transformed into collective anger that might encourage institutional change.

The approach will lead us toward new views on people's interactions with the digital world that surrounds them. Instead of seeing the "choice" not to alter default privacy settings or opt-out of digital systems that engage in unethical data practices as an acceptance of the status quo, the concept of digital resignation encourages us to consider the possibility that this decision reflects, instead, frustration with the limited options available and/or a sense that available responses are meaningless in the face of various manifestations of corporate power. Probing these nuances will help make the processes of digital resignation visible, thereby creating opportunities to understand its causes and key barriers to resistance. Only then can we begin to examine possible paths out of feelings of what increasingly appears to be a major 21st-century malaise.

Acknowledgements

The authors wish to thank the journal editor and the anonymous reviewers for their thoughtful comments. Additionally, they wish to thank participants of the Data Power Conference (2017) and the Privacy Law Scholars Conference (2018) for their feedback on earlier versions of this piece.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Notes

1. These findings were reproduced in a 2018 national survey in which we posed the same two questions (Turow et al. 2018b). This study once again confirmed a majority of Americans—63%—met our definition of resigned.
2. Consider the similarities between the cycle articulated by Benson and Kirsch (2010) and the one described by Zeynep Tufekci (2018b) regarding Facebook's response in the wake of the Cambridge Analytica revelations:

   > The sight of lawmakers yelling at Mr. Zuckerberg might feel cathartic, but the danger of a public spectacle is that it will look like progress but amount to nothing: a few apologies from Mr. Zuckerberg, some earnest-sounding promises to do better, followed by a couple of superficial changes to Facebook that fail to address the underlying structural problems.

3. Although Forman (1963) and Hammerschlag and Astrachan (1971) refer to resignation as a collective behavioral response, their discussion focuses on individual actions in the aggregate as opposed to collective action.

ORCID iD

Nora Addario Draper https://orcid.org/0000-0003-0204-3031

References

Adorno TW (2005) *Critical Models: Interventions and Catchwords* (European perspectives). New York: Columbia University Press.

Anonny M and Crawford K (2018) Seeing without knowing: limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society* 20(3): 973–989.

Anthony SF (2001) The case for standardization of privacy policy formats. Available at: https://www.ftc.gov/public-statements/2001/07/case-standardization-privacy-policy-formats#N_3_

Barnes S (2006) A privacy paradox: social networking in the United States. *First Monday* 11(9). Available at: http://firstmonday.org/article/view/1394/1312

Baumer EPS, Guha S, Quan E, et al. (2015) Missing photos, suffering withdrawal, or finding freedom? How experiences of social media non-use influence the likelihood of reversion. *Social Media + Society*. Epub ahead of print 3 December. DOI: 10.1177/2056305115614851.

Bell A (2014) Notes on Adorno's "resignation." *TELOSscope*. Available at: http://www.telospress.com/notes-on-adornos-resignation/

Benson P and Kirsch S (2010) Capitalism and the politics of resignation. *Current Anthropology* 51(4): 459–486.

Brunton F and Nissenbaum HF (2015) *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, MA: The MIT Press.

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

Chen BX (2018) I downloaded the information that Facebook has on me. Yikes. *The New York Times*, 11 April. Available at: https://www.nytimes.com/2018/04/11/technology/personaltech/i-downloaded-the-information-that-facebook-has-on-me-yikes.html

Cohen JE (Forthcoming) Turning privacy inside out. *Theoretical Inquiries in Law* 20(1). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3162178

Crain M (2018) The limits of transparency: data brokers and commodification. *New Media & Society* 20(1): 88–104.

Dencik L (2018) Surveillance realism and the politics of imagination: is there no alternative? *Krisis: Journal for Contemporary Philosophy*. Available at: http://krisis.eu/surveillance-realism-and-the-politics-of-imagination-is-there-no-alternative/

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

Dencik L, Hintz A and Cable J (2016) Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society*. Epub ahead of print 24 November. DOI: 10.1177/2053951716679678.

Dommeyer CJ and Gross BL (2003) What consumers know and what they do: an investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing* 17(2): 34–51.

Draper NA (2017) From privacy pragmatist to privacy resigned: challenging narratives of rational choice in digital privacy debates. *Policy & Internet* 9(2): 232–251.

Ellison G and Ellison SF (2009) Search, obfuscation, and price elasticities on the Internet. *Econometrica* 77(2): 427–452.

Forman RE (1963) Resignation as a collective behavior response. *American Journal of Sociology* 69(3): 285–290.

Foster JB and McChesney RW (2004) Surveillance capitalism: monopoly-finance capital, the military-industrial complex, and the digital age. *Monthly Review* 66(3). Available at: https://monthlyreview.org/2014/07/01/surveillance-capitalism/?v=7516fd43adaa

Glaser A (2018) The problem with #DeleteFacebook. Available at: https://slate.com/technology/2018/03/dont-deletefacebook-thats-not-good-enough.html

González-Bailón S and Gorham AE (2018) Want to change Facebook? Don't delete your account—use it for good. *Quartz*. Available at: https://qz.com/1244750/the-delete-facebook-movement-is-ultimately-self-defeating/

Griffin A (2016) Facebook ad preferences: how to find out everything the site knows about you, and trick it into being wrong. *Independent*, 9 May. Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-ad-preferences-how-to-find-out-everything-the-site-knows-about-you-and-trick-it-into-being-a7020186.html

Gürses S, Kundnani A and Van Hoboken J (2016) Crypto and empire: the contradictions of counter-surveillance advocacy. *Media Culture & Society* 38(4): 576–590.

Hammerschlag CA and Astrachan BM (1971) The Kennedy airport snow-in: an inquiry into Intergroup Phenomena. *Psychiatry* 34: 301–308.

Hargittai E and Marwick A (2016) "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication* 10: 3737–3757.

Hoffman PH, Lutz C and Ranzini G (2016) Privacy cynicism: a new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10(4): 7. Available at: http://dx.doi.org/10.5817/CP2016-4-7

Hoofnagle CJ (2016) *Federal Trade Commission Privacy Law and Policy*. New York: Cambridge University Press.

Hoofnagle CJ and Urban JM (2014) Alan Westin's privacy homo economicus. *Wake Forest Law Review* 261: 261–317.

Hsu T (2018) Desertions in wake of missteps by Facebook. *The New York Times*, 22 March, p. B1.

Kennedy H, Elgesem D and Miguel C (2017) On fairness: user perspectives on social media data mining. *Convergence: The International Journal of Research into New Media Technologies* 23(3): 270–288.

Kokolakis S (2017) Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. *Computers & Security* 64: 122–134.

Lorde A (2007) *Sister Outsider: Essays and Speeches*. Berkeley, CA: Crossing Press.

McDonald AM and Cranor LF (2008) The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* 4(3): 543–568.

Marwick A and Hargittai E (2018) Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society*. Epub ahead of print 29 March. DOI: 10.1080/1369118X.2018.1450432

Milne GR and Culnan MJ (2002) Using the content of online privacy notices to inform public policy: a longitudinal analysis of the 1998-2001 U.S. web surveys. *The Information Society* 18(5): 345–359.

Milne GR and Culnan MJ (2004) Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing* 18(3): 15–29.

Monahan T (2016) Built to lie: investigating technologies of deception, surveillance, and control. *The Information Society* 32(4): 229–240.

Norwegian Consumer Council (2018) Deceived by design. *Forbrukerrådet*. Available at: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

Obar JA and Oeldorf-Hirsch A (2018a) The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465

Obar JA and Oeldorf-Hirsch A (2018b) The Clickwrap: a political economic mechanism for manufacturing consent on social media. *Social Media + Society*. Epub ahead of print 19 July. DOI: 10.1177/2056305118784770.

Olson LC (2000) The personal, the political, and others: Audre Lorde denouncing "the second sex conference." *Philosophy and Rhetoric* 33(3): 259–285.

Park YJ (2013) Digital literacy and privacy behavior online. *Communication Research* 40(2): 215–236.

Pasquale F (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.

Peterson C, Maier SF and Seligman MEP (1993) *Learned Helplessness: A Theory for the Age of Personal Control*. Oxford: Oxford University Press.

Pollach I (2005) A typology of communicative strategies in online privacy policies: ethics, power and informed consent. *Journal of Business Ethics* 62(3): 221–235.

Portwood-Stacer L (2013) Media refusal and conspicuous non-consumption: the performative and political dimensions of Facebook abstention. *New Media & Society* 15(7): 1041–1057.

Rainie L (2016) The state of privacy in post-Snowden America. Washington, DC: Fact Tank, Pew Research Center. Available at: http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ (accessed 7 February 2017).

Reidenberg JR, Breaux T, Cranor LF, et al. (2015) Disagreeable privacy policies: mismatches between meaning and users' understanding. *Berkeley Technology Law Journal* 30(1): 39–88.

Roberts ST (2018) Digital detritus: "error" and the logic of opacity in social media content moderation. *First Monday* 23(2–3). Available at: http://firstmonday.org/ojs/index.php/fm/article/view/8283/6649

Roessler B (2005) *The Value of Privacy*. Cambridge: Polity Press.

Schonfeld E (2009) Google gives you a privacy dashboard to show just how much it knows about you. Available at: https://beta.techcrunch.com/2009/11/05/google-gives-you-a-privacy-dashboard-to-show-just-how-much-it-knows-about-you/?_ga=2.57343722.1539881564.1530020072-1398430286.1522938979

Selwyn N and Pangrazio L (2018) Doing data differently? Developing personal data tactics and strategies amongst young mobile media users. *Big Data & Society*. Epub ahead of print 15 March. DOI: 10.1177/2053951718765021.

Shklovski I, Mainwaring SD, Skúladóttir HH, et al. (2014) Leakiness and creepiness in app space: perceptions of privacy and mobile app use. In: *Proceedings of the SIGCHI conference on human factors in computing systems* (CHI'*14*), Toronto, ON, Canada, 26 April–1 May. New York: ACM.

Solove DJ (2013) Introduction: privacy self-management and the consent dilemma. *Harvard Law Review* 126(7): 1880–1903.

Statt N (2018) Boycotting digital monopolies like Facebook is harder than it seems. *The Verge*, 22 March. Available at: https://www.theverge.com/2018/3/22/17152922/delete-facebook-boycott-cambridge-analytica-tech-monopoly-data-privacy

Steeves V (2009) Reclaiming the social value of privacy. In: Kerr I, Steeves V and Lucock C (eds) *Privacy, Identity and Anonymity in a Network World: Lessons from the Identity Trail*. Oxford: Oxford University Press, pp. 191–208.

Troullinou P (2017) *Exploring the subjective experience of everyday surveillance; the case of smartphone devices as means of facilitating "seductive" surveillance*. PhD Thesis, The Open University, Milton Keynes.

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

Tufekci Z (2018b) We already know how to protect ourselves from Facebook. *The New York Times* 9 April. Available at: https://www.nytimes.com/2018/04/09/opinion/zuckerberg-testify-congress.html

Turow J, Hennessy M and Draper N (2015) The Tradeoff Fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820060

Turow J, Hennessy M and Draper N (2018a) Persistent misperceptions: Americans' misplaced confidence in privacy policies, 2003–2015. *Journal of Broadcasting & Electronic Media* 62(3): 461–478.

Turow J, Hennessy M, Draper N, et al. (2018b) Divided we feel: Partisan politics drive American's emotions regarding surveillance of low-income populations. Available at: https://repository.upenn.edu/asc_papers/543/

Vaidhyanathan S (2018) *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy*. Oxford: Oxford University Press.

Westin AF (2003) Social and political dimensions of privacy. *Journal of Social Issues* 59(2): 431–453.

Whitson JR (2013) Gaming the quantified self. *Surveillance & Society* 11(1–2): 163–176.

Wood DM and Ball K (2013) Brandscapes of control? Surveillance, marketing and the co-construction of subjectivity and space in neo-liberal capitalism. *Marketing Theory* 13(1): 47–67.

Woodstock L (2014) Media resistance: opportunities for practice theory and new media research. *International Journal of Communication* 8: 1983–2001.

Wren I (2018) NPR survey: still on Facebook, but worried. *NPR's All Tech Considered*. Available at: https://www.npr.org/sections/alltechconsidered/2018/03/21/595770858/npr-survey-still-on-facebook-but-worried

Xie W, Fowler-Dawson A and Tvauri A (2018) Revealing the relationship between rational fatalism and the online privacy paradox. *Behaviour & Information Technology*. Epub ahead of print 4 December. DOI: 10.1080/0144929X.2018.1552717.

Zuboff S (2015) Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* 30(1): 75–89.

Author biographies

Nora A Draper is an assistant professor of Communication at the University of New Hampshire. Her research examines the sociocultural dimensions of media and technology industries.

Joseph Turow is the Robert Lewis Shayon professor of Communication at the University of Pennsylvania's Annenberg School for Communication. His most recent book is The Aisles Have Eyes (Yale University Press, 2017).