7 Complicity

Annie Ring

What are you swimming in that you can’t describe—won’t describe, because it’s too ordinary?
—Lockwood 2019

Complicity is the powerful element, with the translucency and insidiousness of water, through which technology users move in today’s increasingly networked and datafied environments. The large-scale use of smart networked devices by people all around the world, including many of us writing and reading this volume, allows vast archives of data to be routinely captured and analyzed and the results mobilized to generate profit and influence through techniques as dangerous and divisive as racialized profiling and personalized political propaganda. Such abuses of data often occur without the full knowledge of technology users, but the big data archives captured from everyday technology use represent an insistent sediment of complicity on the part of technology consumers, revealing us to be unofficial participants in the data-mining practices that are radically undermining the already delicate foundations of our contemporary shared world.

The 2013 revelations by Edward Snowden and Sarah Harrison (see Agostinho and Thylstrup 2019), about the espionage system developed after September 11, 2001 by the US National Security Agency (NSA) and its partners worldwide, caused neither unprecedented outrage nor noticeable shifts in technology use. Thereafter, many technology users were scandalized when it emerged in 2016 that Cambridge Analytica, the data-trading consultancy connected with the Brexit and Donald Trump campaigns, had covertly harvested data from more than eighty-five million Facebook users’ online activity. But the knowledge about such data mining for political manipulation did not suffice to cause a mass exodus from social media. This was partly because such scandals do not always influence a significant mass of technology users who either remain unaware of the surveillance or do not mind it
since they feel they have “nothing to hide.” Moreover, more informed technology users stay on social media for a variety of understandable reasons. As I argue below, there is something inherently problematic about the fantasy of a sovereign gesture of disconnection from technology, and the multiple obstacles to disconnection are compounded by the attractive aesthetic and psychological registers that new media designs and online data-mining platforms employ to hook users into habitual complicity.

Complicity, I argue here, is an epistemological problematic, a state of being at once forgetful and at least partially unconscious, in which knowledge only appears at moments of inflection such as leaks, when the ugly, unacknowledged material of surveillance and its attendant violent exclusions float to the surface. Compounding this problematic of forgotten or unconscious knowledge, it emerged during recent data-mining scandals that even the most robust democratic institutions do not know what to do about revelations of dataveillance happening on a scale that until recently was reserved for the most pessimistic sci-fi visions—or indeed about revelations that many democratic governments are themselves involved in it. Apparently without irony, WhatsApp (owned by Facebook) and Google protested government eavesdropping in 2019, in the interest of user privacy (Hern 2019). Unsurprisingly given this confounding context, revelations about both the scale of smart networked surveillance and the role that consumer complicity plays within it have generated a fundamental sense of uncertainty about what can be done to bring about a more just networked environment.

Complicities in the Age of Big Data: An Unconscious Folding Together into Wrongdoing

Complicities in the age of big data are so intimate as to be nearly undetectable, not least because they occur via devices kept perpetually within millimeters of the body. Awareness of this surveillance therefore exists below conscious levels of knowledge, as Wendy Chun (2017, xi) argues, since technology users engage in a habitual use of media that shapes their bodies into “archives” of the networked world. Unlike in twentieth-century espionage regimes, today there is no signature, as there would have been in a Stasi or KGB file, declaring agreement on the part of the owner of a smart networked device to collaborate in regimes of secret data trading and psychometric profiling for targeted propaganda.1 A look at the history of the word complicity illuminates this problem of unconsciousness through undetectability: while the Latin prefix com (with, together) suggests the consensual nature of the communication—an event decided or agreed upon together—the verb plicare (Latin: to fold, to weave) points to a less agentic enfolding or folding together of the technology consumer with big data companies. The word’s etymology underlines that technology users only partially consent to become accomplices to data abuse, and are partially folded into complicity
Complicity

by aesthetically appealing products and platforms that grab attention and encourage unconscious habituation.

Present-day use of the term *complicity* implies being an accomplice to wrongdoing, and there is certainly wrongdoing going on. Big data companies and governments are capturing data not to approach particular technical problems or solve specific crimes but rather to store up comprehensive archives of non-preselected information, an ethically and politically dubious practice. For instance, under the 2016 Investigatory Powers Act, the UK government harvests data from emails, social media interactions, and phone records under the aegis of “bulk warrants,” whether or not the data subjects of these warrants are of interest to intelligence agencies or suspected of a crime. Such bulk interception is carried out in collaboration with companies like Google, whose Chrome web browser has itself been defined as spyware (Fowler 2019) because its data defaults enable tens of thousands of tracker cookies to be installed weekly on a user’s computer, gathering data that advertising companies buy in order to construct psychometric and financial profiles. Shoshana Zuboff (2019, 96) analyzes such data trading in terms of “behavioral futures markets,” an apt expression for the ways in which human experience is profitably traded in the form of predictive psychometrics. The profit generated by data trading led the *Economist* to refer influentially to data as the new oil (*Economist* 2017); indeed, systematic mass mining of data certainly compares to the extraction of oil for profit and with considerable ethical compromises. The profits gathered from data mining produce unprecedented influence among unelected leader figures, such as Facebook CEO Mark Zuckerberg. Facebook does not advertise its origins in the sexist trolling project FaceMash, which presented early subscribers with pairs of women from Harvard’s student community and invited them to rank who was “hotter” (Weigel 2018). Facebook hides this abusive history, presumably fearing bad publicity for a social media platform that started out making young women’s lives less safe at an elite university and has since been weaponized for gross abuses of democracy.

When we visit social media platforms or simply carry a smart networked device around with us, technology users relinquish data to regimes permeated by inequality. Alongside conventional racist policing methods, algorithms that technology users cannot understand now process mined Internet data in ways that shape all areas of shared life, and programmed into those algorithms are human biases in the form of code. Safiya Noble (2018) has shown how the machine learning that search engines use entrenches racism into human-computer interaction. Cathy O’Neil (2016) and Virginia Eubanks (2018) have examined how the exploitation of big data and artificial intelligence harms data subjects differently based on their social positionality. Caroline Criado Perez (2019) has revealed wide-ranging gender bias in the way data are applied in areas as crucial as heart medication and car safety testing. Simone Browne (2015) has argued that contemporary surveillance technologies represent a modern
form of branding in which the biased categorization of race and gender in biometric coding leads to racist policing, thus adding to the inequalities already experienced in a racist world beyond the computer. Joy Buolamwini’s (2016) video installation *The Coded Gaze* masterfully demonstrates the trouble facial recognition software has recognizing Black women’s faces as faces, revealing that this software runs independently but according to extreme biases that underpin the apparently bland functioning of binary code.

N. Katherine Hayles rightly argues that “having a human in the loop . . . is no guarantee against bias, since most humans have conscious or unconscious biases” (Amoore and Piotukh 2019, 5). Indeed, and leaving aside the inequalities produced by biases in algorithmic data processing, the far right, with its entirely conscious biases, enjoys great success on the low-accountability, profit-oriented Internet. On YouTube, far-right influencers freely broadcast propaganda, gaining credibility through the seemingly personal contact social media enables. Rebecca Lewis (2018, 48) shows how these influencers benefit as YouTube incentivizes “shocking” content because it generates higher advertising revenue, making it a readily complicit platform. YouTube ruled in 2019 that homophobic content published by conservative supervlogger Steven Crowder did not breach its code of conduct, but it removed videos of human rights abuses in Syria, Egypt, and Pakistan, following its secretive content-moderation protocols. Sarah T. Roberts (2019) demonstrates the toll such protocols take on the workers tasked with sifting through the Internet’s most traumatizing content, thereby highlighting further problems with social media users’ unquestioning patronage of these platforms.

New technologies of data capture also contribute to the climate crisis due to designed-in features whereby networked devices stay switched on perpetually. Additionally, the data archives gathered from them require energy-intensive servers. Kaminska (2019) finds that the “ICT [information and communications technology] sector [is] using 50 per cent more energy than global aviation,” and the production of personal networked devices is especially carbon intensive. Furthermore, the unconscious content of complicity in the networked era includes the shared material histories of consumer technologies and war technology. War was the context in which the Internet was developed and where machine vision was first employed; virtual reality has long served to train soldiers for combat and now helps their recovery from posttraumatic stress disorder. War is where artificial intelligence and data analytics are most brutally applied, as drones carry out strikes against targets identified by means of algorithms that analyze data on the basis of probability. Lisa Parks writes of the foundational complicity between military and consumer technologies: “The mediated everyday is punctuated in innumerable ways by military logics and agendas, so much so that it is increasingly difficult to distinguish media and communication from militarization” (Parks 2016, 230). Consumers do not usually pick up a smartphone or tablet thinking it is made of the
same materials as a bomb or that the software it contains is also used to spy on human rights activists and incriminate political dissidents.

**The Ambivalence of Disconnection**

The complicities into which today’s technology consumer enters are disempowering precisely because they are built into devices and gestures of technology use that became integrated into daily life much more quickly than knowledge about data abuses could circulate. To win power back, we need to bring those complicities to the surface of knowledge, certainly, but the next steps after such a process of becoming conscious are more uncertain. Even though users do not trust new media not to spy on them, not many find it possible to switch off devices entirely, and it seems few people even get around to protecting personal data in the ways currently available. Tellingly, a US survey found that after the NSA revelations, only 30 percent of adults in the US said they had attempted to stop their online data being extracted without permission (Rainie and Madden 2015).

A later survey found that only 9 percent of social media users in the US trusted social media companies to protect their data (Rainie 2018), and yet disconnecting in a totally networked society is almost impossible. In response to the difficulty of withholding data entirely, some resistant technology users choose to supply false personal data online, thus producing a counterarchive that Hito Steyerl (2016) calls *dirty data* (see also Zer-Aviv, chapter 38, this volume). These actions—redolent of the recalcitrant law-copyist Bartleby in Herman Melville’s “Story of Wall-Street,” who famously “preferred not to” reproduce information for his financial-lawyer boss (Melville [1853] 2002)—are inspiring responses to the age of digitized bureaucracy. But Pepita Hesselberth (2017, 1) has rightly identified the structuring “paradox of dis/connectivity” whereby disconnection always implies connection, and disconnection discourses usually rely on the very media they advocate abandoning (see also Hesselberth, chapter 13, this volume). Another critic of the disconnection argument, Sarah Sharma (2017), demonstrates that the structuring of gender roles in patriarchy means the attractive dream of “exit” only functions as a “male fantasy . . . a deceptively simple solution to real-life entanglements.” Exit is not only a male fantasy but is also a privilege reserved for those whose lives can safely exist in the traditional or rural settings imagined by majority-white alternative lifestyle movements. Some people are more vulnerable to surveillance and to disconnection’s negative consequences, such as the economically disadvantaged, who, as Eubanks (2018) shows, must give up data privacy to access basic government services. A return to “nature” has always been an inherently conservative praxis so that the inequality besetting dataveillance regimes also makes for vastly different consequences of disconnecting for different subjects.
In place of masculinist and white-privileged fantasies of withdrawal from complicity in the networked age, Sharma (2017) proposes “a feminist project—one of extension.” Such a project, centered around “care,” would “respond . . . to the uncompromisingly tethered nature of human dependency” (Sharma 2017; see also Agostinho [chapter 6, this volume]; the seven principles for justice-oriented dealings with data in D’Ignazio and Klein [2018]). I would add that such a project of “extension” must take into account the problematic enfolding into complicity induced by human needs. Who among us can do without exchanging messages with loved ones or navigating new spaces with the help of GPS? Complicity with data exploitation also continues sustainably because users take immense pleasure in new devices that offer visual and tactile pleasures and opportunities to display wealth and commune with the state of the art. Technology users’ needs and these aesthetic fascinations blind us to the links between everyday technology use and data mining for far-right propaganda, to the inequality built into surveillance regimes, and to the drone strikes that characterize current high-tech global warfare.

Driven by these needs and fascinations, many technology consumers go so far as to merge with our machines. Referring to the continued validity of Marshall McLuhan’s (1969) view of media as prostheses, Hayles writes: “When my computer goes down or my Internet connection fails, I feel lost, disoriented, unable to work . . . as if my hands have been amputated” (Hayles 2012, 2). Further, Halpern and Simanowski have suggested that technology users are captured by a fascination with “beautiful data” themselves (Halpern 2015) such that we experience the counterintuitive phenomenon of “data love” (Simanowski 2018), in which the notion of data’s ungraspable potency extends the beauty of many of the devices we use. The most persuasive attraction of the machines of the information age, it seems, lies in the fact that they work so well even while unobtrusively gathering data and that they then respond in ways that make users feel recognized by content tailored specifically to manipulate. Because of these complications, it is not enough merely to see rationally how data-capture technologies are being exploited nor is it possible to decide, in a sovereign gesture of self-separation, to disconnect from the network. Rather, given the unconscious enfolding complicity implies, consideration is needed as to how more consciously cooperative practices could serve the deep human needs that data cultures exploit.

**From Complicity to Cooperation**

Many abuses of contemporary technology work covertly, servicing deep, often unconscious needs and so weaving users into habitual complicity. To tackle this covert work, we need to move from unconscious complicity to conscious cooperation. Technical knowledge and political analysis must join with cultural, ethical, and psychoanalytic approaches in order
to imagine new technologies for a public sphere in which manipulation and inequality give way to diversity, care, and protection. Natasha Dow Schüll (2014) has analyzed how complicity with data mining in the gaming industry is assured “by design,” through software that creates and perpetuates machine gambling addictions. But technically speaking, there can also be privacy by design—even consent by design and justice by design—and it is with these values in mind, rather than profit and mindless innovation, that an alliance for transforming our networked, datafied world must begin.

Donna Haraway encourages those concerned about unjust technological practices to develop “a good-enough idiom so you can work on something together” (Weigel 2019). In part, the shared language of a cooperative alliance will need to be a political and legal one since some abuses of data are so egregious as to make political opposition the most urgent response. Although the leaks about the NSA prompted some legislative change in the US, the UK’s Investigatory Powers Act increased data abuses, particularly against those already facing the country’s notorious “hostile environment.” Regulation is most likely to succeed with forceful challenges to policy by alliances of people, including software designers, opposition politicians, and policy campaigners. Liberty’s (2019) work challenging the British government’s unlawful use of bulk warrants to spy unselectively on technology users’ data is exemplary here. Yeshimabeit Milner’s (2019) talk on abolishing big data and the moratorium on facial recognition called for by the American Civil Liberties Union (ACLU 2018) in Massachusetts demonstrate the kinds of demands interested parties can make if they wish to bring theory and politics together to challenge the most racist kinds of dataveillance. I suggest, moreover, that the vast archives associated with the exploitation of data can themselves provide a resource for many such challenges to data abuse.

Like a flood, complicity leaves behind a sediment, a line drawn across the architectures of our shared lives as a species, in the form of the archives of dataveillance that are currently held by governments and corporations. Even given the questionable capacity of archives to bring about order or reliability (see the introduction to this volume), big data archives need to be employed for more just purposes than finding out how to profit more and gain more power from technology users’ emotional states and political viewpoints. For instance, while there is no positive ethical value produced when Spotify knows—and sells its knowledge of—what mood somebody is in based on music choices (Eriksson et al. 2019), it would be valuable for activists and nongovernmental organizations to access evidence of how data is used once it has been gathered by mood-tracking and mood-manipulating apps. Archival leaks such as those carried out by Snowden and Harrison could well mark the beginning of a shift of information monopolies into democratic governance. Then, rather than harvesting data for emotionally targeted advertising and personalized right-wing propaganda, it would be possible to collect data, for instance, on links between alt-right media networks and
political campaigns in order to bring about justice and enact appropriate legislation. Beyond legal challenges and legislation, theorists and activists can join together with engineers and designers to bring about a sea change in the values behind future software—moving toward the values of protection, justice, and meaningful data exchange.

Some steps toward cooperation and away from complicity are underway. Amnesty International’s Strike Tracker crowdsourcing project brought tens of thousands of volunteer decoders together in 2018 to organize unstructured data and establish a timeline for the Battle of Raqqa, Syria. That project demonstrates how an alliance for more just data use must involve nonhuman cognitive agents: alongside the decoding volunteers, Amnesty International trained algorithms to work with extant images of Raqqa to scale up the capacity of this important fact-finding mission. Leading machine-learning designers, too, are working with artificial intelligence to process data in environmentally friendly ways. For instance, the makers of AlphaGo have used their code to cool data centers, reduce energy use, and improve wind farm technology. In these projects, volunteers, designers, and artificial intelligence are uniting in service of more positive values than surveillance for profit, and for control. As Hayles notes, the cognitive capabilities of algorithms outstrip those of humans in complexity and capacity (Amoore and Piotukh 2019, 3). Given how closely technology users live alongside artificial intelligence, from smartphone cameras to high-frequency trading algorithms and neural networks, any genuinely cooperative thinking about data justice must also extend to just uses of nonhuman cognition. Such new and extensive modes of cooperation will bring with them uncertainties, of course, but they may also herald a less complicit, more conscious, and so more just networked world.

Addendum: Complicity with Data Use and Abuse after COVID-19

As this book is going to press, we find ourselves in the midst of the COVID-19 pandemic. Most of the book’s writers and editors are living in lockdown, a protective measure to slow the spread of the deadly novel coronavirus. People around the world are being asked to submit their GPS and even health data for the same reason. Whether the data gathered in aid of thwarting the virus will be protected from abuse in the form of data mining and trading, and how long the current forms of exceptional surveillance will be in place, remain unanswered questions. Meanwhile, the data we have about infection and death rates show that “we” are not all in it together: the virus does discriminate because societies discriminate, and people of color and people kept in systemic poverty are much more vulnerable to catching and dying from the virus because of the grossly unequal wealth and living and working conditions that hold sway in contemporary capitalism. These are the same groups who are more vulnerable to the data abuses I have written about here, and we urgently need to ask questions about
whether the data being gathered in the time of COVID-19 will be used in a way that will not further target and harm people needing protection: Will it be helpful, or complicit with more harm, if we give up more data now? Anxiety about abuse of data shared for protective measures is not new: for instance, it has always been a concern when it comes to policing to prevent terrorism. Though the anxiety is not new, the changed world after COVID-19 will urgently demand a turn toward data justice, one in which governments and corporations do not abuse data gathered for the good. Only then will people concerned about abuses give up data readily.

Note

1. I am drawing here on the differentiation I make in After the Stasi (Ring 2015, 16, 199–226, 238–239) between conscious collaboration by Stasi informants and the habitual, often invisible complicities underpinning present-day surveillance.

References


Chapter 7


