The Road to Digital Unfreedom: Three Painful Truths About Social Media

Ronald J. Deibert

Journal of Democracy, Volume 30, Number 1, January 2019, pp. 25-39 (Article)

Published by Johns Hopkins University Press
DOI: https://doi.org/10.1353/jod.2019.0002

The Road to Digital Unfreedom

THREE PAINFUL TRUTHS ABOUT SOCIAL MEDIA

Ronald J. Deibert

Ronald J. Deibert *is professor of political science at the University of Toronto and director of the Citizen Lab at the University's Munk School of Global Affairs and Public Policy. His books include* Black Code: Surveillance, Privacy, and the Dark Side of the Internet *(2013).*

Social media have taken a beating lately. The gloss has worn off the large companies that dominate the sector, and with it much of the internet. Facebook, Google, and Twitter, among others, have all been subjected to intense scrutiny because of the negative externalities that their services create. A focus of concern has been the abuse of social-media channels as part of efforts to influence the outcome of major political events, including the June 2016 Brexit referendum in the United Kingdom and the U.S. presidential election later that year. In both cases, studies and intelligence reports show, nation-states and nonstate actors alike exploited, manipulated, and abused social media as a tool of their "information operations." The role that social-media analytics firms played in these events was especially pronounced.[1]

The situation presents a striking contrast both to the ways in which social-media platforms present themselves, and to how they have been widely perceived in the digital age. Once it was conventional wisdom to assume that these platforms would enable greater access to information, facilitate collective organizing, and empower civil society. Now, they are increasingly seen as contributing to society's ills. Growing numbers of people are coming to believe that social media have too much influence on important social and political conversations.[2] Others are beginning to notice that we are spending unhealthy amounts of time staring at our devices, "socializing" online while in fact cut off from one another and from nature.

As a result of this growing unease, there are pushes to regulate social-media companies in ways that will encourage them to be better stewards of their platforms, to respect privacy, and to acknowledge the role of hu-

Journal of Democracy Volume 30, Number 1 January 2019

man rights. A prerequisite of any such regulation, however, is a shared understanding of what is wrong in the first place.

Increasingly, scholars and the public at large are coming to agree about what I call "three painful truths" concerning social media: 1) that the social-media business model is based on deep and relentless surveillance of consumers' personal data in order to target advertisements; 2) that we permit this staggering level of surveillance willingly, if not altogether wittingly; and 3) that social media are far from incompatible with authoritarianism, and indeed are proving to be among its most effective enablers. The observations concerned are not entirely novel. Yet when added up, they present a very bleak picture of our social and political reality, and presage a still bleaker future. As deeply troubling as the social and political implications of social media's pathologies may be, there can be no hope of meaningful reform unless we address them squarely.

Social Media Equal Surveillance Capitalism

Surveillance is an inherent characteristic of modernity, and perhaps even of our nature as a species. We observe, predict, and try to shape the world around us. Over time, the tools at our disposal to do so have grown more sophisticated and extensive. Since the Enlightenment at least, humans have been on a path driven by the belief that more information is better. But is it possible that this instinct can become counterproductive, especially when combined with the staggering powers of digital technology?

It is ironic to recall that there once was a time when people fretted about how to make a profit online. The 1990s dot-com boom and subsequent bust highlighted the "irrational exuberance" around the new information economy. Soon enough, however, innovations by companies such as Google, Facebook, and others not only provided a fresh model of how to draw revenue from internet connectivity, they spearheaded a radically new mode of production that has transformed the world. Called the "personal-data surveillance economy" or "surveillance capitalism,"[3] this mode has at its core a fairly simple transaction: Consumers get services (mostly free of charge) while industries monitor users' behavior in order to tailor advertisements to them.

The companies that make billions off this naturally tend to describe what they do in anodyne terms. Facebook, for example, refers to its users not as "consumers," but as a "community." Google says that its mission is "to organize the world's information and make it universally accessible and useful," which makes Google sound far more benign and empowering than what it really is: a massive commercial-surveillance system.

There is an inexorable logic to surveillance capitalism. This logic, made manifest by the industry's ceaseless innovations, is to acquire as

much data as possible about as many consumers as possible from ever more fine-grained, distributed, and overlapping sources of information. Data points revealing our habits, social relationships, tastes, thoughts, opinions, energy consumption, heartbeats, even sleep patterns and dreams are correlated ever more ingeniously, extensively, and precisely with still other data points. Then computers sort, analyze, and use it all to refine and target highly personalized ads for us to see online. From the industry's point of view, there can never be too much data. Sensors are built upon sensors in an endless quest for acquisition and control.

Facebook's patent applications provide a map of how the company "thinks about where its technology is going."[4] The company has taken out patents for ways to infer whether users are in a romantic relationship based on the number of times they visit friends' sites, their gender, and other indicators. Another patent is about examining the contents of your posts in order to assess your personality for extroversion, openness, and emotional stability. Then there is a patent for a technology that would use credit-card transactions and user locations to tell advertisers when someone is about to experience a life event, such as a graduation or the birth of a child. Even eerier are patents concerning the use of tiny scratches on camera lenses to create unique user "signatures," and the monitoring of electrical disturbances in television power cables in order to tell what shows someone is watching.

Behind the well-known frontline companies of this surveillance economy are numerous firms that are in the "analytics" business. Working behind the scenes, they glean from the information harvested by frontline companies business intelligence that can then be sold to advertisers and others. Even farther in the background hover companies that supply algorithms, software, techniques, and tradecraft to the analytics firms. Then there are the businesses that furnish the basic hardware, software, and energy required to keep it all operating. Most users, looking into the "front window" of social media, never hear of these obscure business-to-business outfits unless data gets hacked or there is a scandal, such as the Cambridge Analytica affair that broke out in early 2018.

Social-media companies make money by selling these third-party developers, applications, and other services access to customer data. These business deals can mean that users of one platform are unwittingly handing vast amounts of personal data to dozens of other services, in a behind-the-curtain information-sharing bonanza. For example, according to a *New York Times* investigation, Facebook has data-sharing deals with at least sixty device makers—including Amazon, Apple, BlackBerry, Microsoft, and Samsung. After installing an application from one of them, a journalist found that this app was able to gain access to unique identifiers and other personal information of hundreds of his Facebook friends, and close to three-hundred thousand online "friends of friends."[5]

The scale of the economic transformation that the surveillance econ-

omy has unleashed is hard to overstate. Consider how traditional industries are being transformed into vehicles for harvesting and analyzing personal data, even if they did not start out that way. Commercial airlines, for example, are now more than just modes of transportation. They are also data-gathering and marketing firms linked with other data-gathering and marketing firms such as hotel chains, taxicab companies, and vacation destinations. Loyalty-rewards programs offer a way to keep track of customers' preferences, movements, and spending habits. It is now commonplace to download an airline's mobile app to book flights, check in, and receive a boarding pass. The customer gets convenience. What does the airline get? As Air Canada's privacy policy states, it gets information about customers in order to allow the airline to "develop and recommend products and services based on an understanding of your interests and needs."

All social-media applications have higher- and lower-level functions. An application that you use to tease your brain might seem like a mere game, but in reality it doubles as a means to observe you and acquire data about you: your device, your other applications, your contacts, your pictures, your settings, your geolocation, and the like. In order to accomplish this "higher"-level function, apps give themselves permission to access parts of your device ranging from your address book to your operating system, various unique device identifiers, and even your camera and microphone. In 2014, Pew Internet discovered that apps can seek up to 235 different kinds of permissions from Android smartphone users, with the average app asking for five.[6]

We Consent (but Not Wittingly)

The second painful truth is that we like, or at least accept, this bargain. Knowledge of social media's ills and unintended consequences is spreading, and particular platforms rise and fall, but social media as a whole remain popular, and the surveillance-based economic system underlying them is constantly expanding.

To be sure, rational decisions inform the choices consumers make. The pervasiveness of social media creates strong incentives and disincentives favoring participation in these services. Teenagers often remark that they cannot leave Facebook because they would face social ostracization. Employing what one author calls "infrastructural imperialism," organizations often offer social media as the readiest way to access their services, excluding those who opt out of social media while subtly but powerfully shaping the choices of those who opt in.[7]

But do users fully understand the choices that they are making when they sign on to social media? It is common to download and install numerous applications, each with a long "terms of service" statement and an "accept" box that one clicks—one cannot complete the download

unless one clicks the box—without actually reading the terms, let alone grasping their details. Years ago, a software firm put an offer of a free US$1,000 at the very end of its terms of service, just to see how many would read that far.[8] Four months and three-thousand downloads later, exactly one person had claimed the offered sum. Add the boilerplate legal jargon that is used, and the cloud of unknowing around contractual obligations becomes denser. In short, the vast majority of users agree to terms that they do not understand.

While most would acknowledge the constraints on choice that are at work, a worldwide study of students who tried to go a day without social media points to a much more fundamental (and less witting) mechanism. According to this study, "most students from all [ten] countries failed to go the full 24 hours without media, and they all used virtually the same words to describe their reactions, including: Fretful, Confused, Anxious, Irritable, Insecure, Nervous, Restless, Crazy, Addicted, Panicked, Jealous, Angry, Lonely, Dependent, Depressed, Jittery and Paranoid."[9] Social media are, in other words, addiction machines.

Social media stimulate us in a powerfully subconscious and hormonal way. They affect the human brain in the same way that falling in love does.[10] Levels of oxytocin—sometimes called the "love hormone"—rise as much as 13 percent when people use social media for as little as ten minutes.[11] People addicted to social media "experience symptoms similar to those experienced by individuals who suffer from addictions to substances or other behaviors"—such as withdrawal symptoms, relapse, and mood modification.[12] Is it accurate to describe our embrace of social media as witting when that embrace has the properties of an addiction?

Companies pour extraordinary resources into research aimed at heightening the emotionally compelling and even addictive aspects of social media. Firms understand that winning the contest for people's scarce time and attention requires generating a kind of consumer compulsion. To encourage continued engagement, social-media companies borrow methods reaching back to psychologist B.F. Skinner (1904–90). Among these is operant conditioning, which is based on altering behavior through a system of rewards and punishments. Behavior that is followed by pleasant consequences is likely to be repeated.

A good example of operant conditioning in social media is what is known as a "compulsion loop." Compulsion loops are found in a wide range of social media, and especially online games. They work via "variable-rate reinforcement," in which rewards are delivered in an unpredictable fashion. Variable-rate reinforcement is effective at shaping a steady increase in the desired behavior, apparently affecting the hormonal dopamine pathways within the human brain. Game designers use variable-rate reinforcement to entice players to play the game repeatedly.

As players do this, slowly becoming addicted, the game's application

learns more and more about their devices, interests, movements, and so on. Social-media platforms even sense when you are disengaged and have designed techniques and tools to draw you back in: little red dots on app icons, banner notifications, the sound of a bell, a vibration.[13]

The cacophony of opinions and the flood of information on social media are degrading public discourse. Faced with information overload, consumers resort to cognitive shortcuts that tend to steer them toward opinions that fit what they already believe.

Sean Parker, who was Facebook's first president, recently made remarkable admissions about how the social-networking site employs such methods to hook people on its platform. Parker described how features such as the "like" button were designed to give users "a little dopamine hit." He explained: "It's a social-validation feedback loop . . . exactly the kind of thing that a hacker like myself would come up with, because you're exploiting a vulnerability in human psychology." As former Google employee Tristan Harris has remarked ominously, "our choices are not as free as we think they are."[14]

As is the case with other industries where addiction is a factor (tobacco, casinos), users of social media often have only a dim grasp of the behavioral-modification techniques that the people who run the industry and their paid consultants intensively study and apply. Psychological experiments on consumers are essential to refining products.[15] Lacking ethical oversight, these experiments can sometimes go wrong. The most infamous example is Facebook's January 2012 experiment that modified the emotions of more than 689,000 users by deliberately keeping positive or negative content out of their news feeds.[16] The experiment showed that such manipulation worked, as users displayed signs of "emotional contagion"—the less positive content they saw, the less positive were their own postings, while reduced exposure to negative content also led them to post fewer negative updates of their own. When the published study recording these results drew wide attention in 2014, the academic community roundly condemned the researchers' failure to secure their subjects' informed consent before conducting the experiment. Its disturbing implication remained, however: A social-media company had found a way to "uncover, and even trigger, consumer frailty at an individual level."[17]

Our less than full "wittingness" in using social media also flows from the way the systems that we depend on and that shape our lives have increasingly receded from firsthand apprehension. The "cloud" metaphor that is used to describe social media reveals this climate of obscurity. What is "the cloud"? It is layers upon layers of algorithms

hidden in tiny microprocessors, networked into sensors, and fed to data-processing warehouses that lie buried beneath mountains or stand sequestered behind barbed-wire fences. The whole enterprise is guarded by intellectual-property laws and nondisclosure agreements. This vast technological, physical, and legal infrastructure exerts control over our lives even as social-media companies seek to keep their products in the background of everyday existence—always on and used constantly, but so much as a matter of course that they are taken for granted and given little critical thought.

Social-media companies leverage the human trust that clusters around the activity of friends sharing information with one another in order to manipulate us into sharing information with advertisers.[18] The plan is to lull us into complacency so that we pay no heed to the intense surveillance, and the vast machinery behind it, while we use the service. If social media's continuing popularity is any guide, the plan is working.

Social Media Drive Authoritarian Practices

The last and most troubling of the painful truths about social media is that they propel authoritarian practices. Social media not only are compatible with authoritarianism; they may be one of the main reasons why authoritarian practices are now spreading worldwide. A particular practice that is authoritarian can occur even under a regime that is not.[19] Authoritarian practices aim to control people and to sow confusion, ignorance, prejudice, and chaos in order to undermine public accountability.

At the heart of this painful truth is a surprising inversion of an older and widely held assumption that digital technologies would prove incompatible with authoritarianism. It is now clear that this conventional wisdom was wrong. In fact, social media are driving the spread of authoritarian practices.

Consider the effects on public discourse of the massive volume of information that social media produce. While worries about "information overload" are as old as Johannes Gutenberg's printing press, we are arguably reaching a point where the sheer quantity of data is producing a qualitative shift. Twitter says that it hosts about six-thousand new tweets every second, which works out to about two-hundred billion new tweets a year. Almost a billion and a half people log onto Facebook daily.[20] Every minute, more than 3.87 million Google searches are conducted and seven new articles are added to Wikipedia.[21] And a vast swath of humanity now carries devices that are always on and connected. The staggering amounts of information produced have unleashed a constant, real-time tsunami of data.

The world of social media is more conducive to extreme, emotionally charged, and divisive types of content than it is to calm, principled

considerations of competing or complex narratives.[22] The rational, deliberate pursuit of consensus and the search for truth are losing out. The cacophony of opinions and the flood of information on social media are degrading public discourse.[23] Faced with information overload, consumers resort to cognitive shortcuts that tend to steer them toward opinions that fit what they already believe. At the same time, social media's own algorithms guide users into online "filter bubbles" in which they feel comfortable and ideologically aligned.

The constant bombardment of tainted leaks, conspiracy theories, and other misinformation in turn fuels cynicism, with citizens growing fatigued as they try to discern objective truth amid the flood of news.

An always-on, real-time information tsunami creates the perfect environment for the spread of falsehoods, conspiracy theories, rumors, and "leaks." Unsubstantiated claims and narratives go viral while fact-checking efforts struggle to keep up. Members of the public, including researchers and investigative journalists, may not have the expertise, tools, or time to verify claims. By the time they do, the falsehoods may have already embedded themselves in the collective consciousness. Meanwhile, fresh scandals or outlandish claims are continuously raining down on users, mixing fact with fiction. Worse yet, studies have found that attempts "to quash rumors through direct refutation may facilitate their diffusion by increasing fluency."[24] In other words, efforts to correct falsehoods can ironically contribute to their further propagation and even acceptance.[25] The constant bombardment of tainted leaks, conspiracy theories, and other misinformation in turn fuels cynicism, with citizens growing fatigued as they try to discern objective truth amid the flood of news.[26] Questioning the integrity of all media—one aim of authoritarianism—can in turn lead to a kind of fatalism and policy paralysis.[27]

Contributing to this problem are the actions (or inactions) of social-media companies that appear unwilling or unable to weed out malicious or false information. In spite of enormous public and governmental pressure following the 2016 U.S. election, a 2018 study found that "more than 80 percent of accounts that repeatedly spread misinformation during the 2016 election campaign are still active, and they continue to publish more than a million tweets on a typical day."[28]

One study estimates that between 9 and 15 percent of Twitter's active "users" are in fact bots.[29] When it was revealed in July 2018 that the microblogging service was deleting about a million bogus accounts a day, its stock price dropped sharply—a sign of the business reasons for *not* digging too deeply into one's own platform to rid it of fake us-

ers.[30] In September 2018, Facebook COO Sheryl Sandberg told a U.S. Senate committee that from October 2017 to March 2018, her company had deleted 1.3 billion fake accounts.[31] Malicious actors are now using WhatsApp groups as well as altered images and videos called "deep fakes"[32] to spread disinformation virally. These techniques are far harder for social-media platforms to combat than previous methods, and will almost certainly become a staple of discrediting and blackmail campaigns in the political realm.

Despite cleanup efforts, social media will remain easy to exploit for disinformation purposes so long as gathering subscribers is at the heart of the business.[33] In mid-2018, Google's security team failed to stop researchers posing as Russian trolls from buying political ads on Google.[34] The researchers paid in Russian currency and registered using a Russian postal code. They used indicators linking their advertisements to the Internet Research Agency, the very troll farm that was the subject of intense U.S. congressional scrutiny and special-counsel indictments. A system that makes its revenue on advertisements is unlikely to err on the side of caution when trying to distinguish authentic from malicious actors.

Quite apart from whatever actions social-media companies may or may not take to clean up their platforms is a more fundamental problem unlikely ever to be addressed as long as attracting and keeping users' attention is central to these companies' business model. As presently constituted, the algorithm-driven advertising system at the core of the surveillance economy surfaces and pushes extreme, inaccurate, and radical content—regardless of what malicious actors may do to seed it.[35]

Online advertising systems, the *Washington Post* has noted, "regularly put mainstream ads alongside content from the political fringes—and dollars in the pockets of those producing polarizing and politically charged headlines."[36] Of most concern is content that does not violate platforms' bans on hate speech or advocacy of violence, but that still uses emotionally charged or other sensationalist triggers to push conspiracy theories, disinformation, or propaganda. This type of content can be the most insidious since it is less easily spotted by company due-diligence mechanisms, yet attracts the largest numbers of consumers. To give just one example, a German study recently found that when otherwise-similar municipalities are compared, the ones where Facebook usage is higher also tend to have a higher incidence of violence against refugees.[37]

Not surprisingly, people with authoritarian inclinations are actively taking advantage of the propitious environment that social media offer.[38] A recent survey by the Oxford Internet Institute found that 48 countries have at least one government agency or political party engaging in shaping public opinion through social media. Authoritarian-minded leaders routinely lambaste "fake news" while at the same time

shamelessly pushing patent falsehoods. Jacob Weisberg lists some of the consequences:

> In Myanmar, hatred whipped up on Facebook Messenger has driven ethnic cleansing of the Rohingya. In India, false child abduction rumors on Facebook's WhatsApp service have incited mobs to lynch innocent victims. In the Philippines, Turkey, and other receding democracies, gangs of "patriotic trolls" use Facebook to spread disinformation and terrorize opponents. And in the United States, the platform's advertising tools remain conduits for subterranean propaganda.[39]

In 2017, political scientist Thomas Rid wrote that Twitter, the most open and loosely administered of the major social-media platforms, "has become a threat to open and liberal democracy."[40] Twitter does not require real-name registration, and there is no limit on how many accounts may be created. Account owners can easily delete accounts and content, and the service is highly automated—circumstances that have made the platform easy to exploit. Creating bots on Twitter is simple. Bots do not sleep or lose focus. They can hijack conversations and twist discourse in irrational directions. Is it any wonder that Twitter has become the tool of choice for authoritarian influence operations?

A Tool for Authoritarians

Authoritarianism thrives by taking advantage of another characteristic of social media: its inherent insecurity. Activists, dissidents, and journalists rely on social media as much as anyone. Platforms that explicitly encourage trust, intimacy, and sharing have opened up an easy avenue for authoritarians to infiltrate and disrupt those networks deemed threatening to their interests. Tactics range from cheap but effective phishing and social-engineering campaigns to the use of sophisticated, commercially available spyware to infect a target's devices (there is a large and poorly regulated market for easily abused spyware products).[41]

Civil society lacks the know-how and capacity needed to guard against such attacks. Although social-media companies have taken some laudable steps to protect users, the intensive data-sharing inherent in the social-media business model limits the effectiveness of such measures. Thanks to social media, autocrats can now reach across borders and steal silently into the pockets, papers, and communications of dissidents, secretly listening to and watching all that they do, often with perilous consequences.

Here is yet another piece of what was once conventional wisdom that now seems entirely wrong: Many thought that social media would empower transnational civil society, but now it seems that social media may be contributing to civil society's slow demise.

Finally, the very fine-grained surveillance that social media carry out

for economic reasons is proving to be an irresistible proxy for authoritarian control. Why would a government bother building its own surveillance machine when the private sector already provides one? As Edward Snowden's 2013 disclosures regarding the U.S. National Security Agency revealed, information that social-media companies share with law enforcement and intelligence is now essential to officials' "collect it all" approach. And while Western liberal democracies may regulate such public-private sharing with albeit imperfect legal safeguards, authoritarian regimes present a completely different environment—and an increasingly lucrative business opportunity.

The People's Republic of China (PRC) provides an ominous model. The PRC is working with social-media conglomerates such as Alibaba and Tencent to build an Orwellian-sounding Social Credit System that will rank citizens' and businesses' reputations based on their purchases, movements, and public communications while using that ranking to restrict access to jobs, travel, and credit. Companies operating in the PRC must comply with China's 2016 cybersecurity law, which requires them to police their networks, silently censor private chats and public posts, and share user data whenever PRC authorities demand it.

Western companies such as Apple, Facebook, and Google used to trumpet their safeguarding of users' rights. Now they have done a complete U-turn for the sake of gaining access to the booming, gigantic Chinese market (China has by far the world's largest pool of internet users within a single set of national borders). Recent leaks have shown Google reversing the stance it took in 2010 when it exited China on principled grounds. The company has been preparing a tailor-made-for-China search engine code-named Project Dragonfly.[42] This engine would censor results even as it identifies users so that security agencies would know who is searching for what.

In early 2018, Apple made similar compromises to enter the China market. The company now uses a government-controlled facility in Guizhou Province to host the iCloud accounts of Chinese citizens. Meanwhile, Facebook founder and CEO Mark Zuckerberg can barely contain his excitement over China-based business opportunities. What appears to be a successful model of social-media management will not remain limited to China, either. Autocracies the world over are proving receptive to Chinese companies and the authoritarian norms and practices they bring. Far from helping to doom autocracy, social media are proving to be among its best friends.

Can Social Media Be De-Toxified?

These painful truths add up to a bleak picture and a troubling forecast for the future of liberal-democratic practices. It seems undeniable now that social media must bear some of the blame for the descent into neo-

fascism, tribal politics, and spreading ignorance and prejudice that we have witnessed in recent years. Personal-data surveillance and authoritarian practices fit well together and are entangled in seemingly endless business opportunities that promise big profits but also threaten to undermine accountability, sow division, spread ignorance, and enforce autocratic control.

Once this is understood, it becomes clear that minor adjustments to social media—through voluntary corporate policies or a handful of regulations—will have negligible effects. There may be genuine good intentions behind social-media executives' promises to do a better job of protecting privacy or policing their networks, but the core business imperatives that drive these platforms make the efficacy of such vows highly doubtful.

How will major multinational companies be reined in to prevent the negative externalities of their services without at the same time eliminating the very business model upon which those services rest? The scope and scale of changes that may be needed to mitigate the consequences outlined above is daunting to contemplate. In a short period of time, digital technologies have become pervasive and deeply embedded in all that we do. Unwinding them completely is neither possible nor desirable. We need an open and secure means of communicating globally in order to manage our planet and our affairs. Yet we need to recognize that the current design, hinging on personal-data surveillance, works against those aims.

To restore liberal democracy, we will need a wholesale change in our way of life. That will obviously not be easy, nor will it happen overnight. There will be enormous social, economic, and political forces pushing back against it. A comprehensive strategy of long-term reform is therefore required, extending from the personal to the political, from the local to the global. We must learn to treat our information environment in the same way that we hope to treat our natural environment—as something over which we exercise stewardship and toward which we behave in a spirit of caution and restraint. If conserving energy is wise, conserving data consumption might be wise as well. Simultaneously, we must develop systems of public education with media literacy, ethics, civility, and tolerance at the foundation.

In the political and legal realm, citizens must gain the right to know what companies and governments are doing with all the personal data they are so assiduously collecting. It will also be crucial to extend this right internationally by holding autocratic regimes to account. Companies must be barred from selling products and services that enable infringements on human rights and harms to civil society. At the same time, we need to subject social-media platforms to strict oversight by independent agencies that have real power to hold them to account. Legislators should enact strong antitrust laws governing social-media companies, and officials should enforce these laws rigorously. The industry

is a highly concentrated one, dominated by just a few large enterprises wielding enormous power. That needs to change.

Finally, the world is crying out for technological innovations that will open up other means of distributed communication beyond the highly centralized, intensely surveilled, and too easily abused platforms of the social-media giants. The goal should be to preserve the great strides we have made in connecting people to one another and letting them access vast stores of information quickly from anywhere on the planet, but without steering them toward the indulgence of their basest instincts.[43] The tasks are enormous, yet we must avoid fatalistic resignation to the toxic world of personal-data surveillance. We need to imagine a better world and start making it happen, before it is too late.

NOTES

The author thanks Gabby Lim and Jane Gowan for research and editorial assistance, and John Scott-Railton for inspiration and guidance.

1. Matthew Rosenberg, Nicholas Confessore, and Carole Cadwalladr, "How Trump Consultants Exploited the Facebook Data of Millions," *New York Times*, 17 March 2018.

2. Janna Anderson and Lee Rainie, "The Future of Truth and Misinformation Online," 19 October 2017, *www.pewinternet.org/2017/10/19/the-future-of-truth-and-misinformation-online*.

3. Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* 30 (March 2015): 75–89.

4. Sahil Chinoy, "What 7 Creepy Patents Reveal About Facebook," *New York Times*, 21 June 2018.

5. Gabriel J.X. Dance, Nicholas Confessore, and Michael LaForgia, "Facebook Gave Device Makers Deep Access to Data on Users and Friends," *New York Times*, 3 June 2018.

6. Kenneth Olmstead and Michelle Atkinson, "Apps Permissions in the Google Play Store," Pew Research Center, October 2015, *http://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-play-store*.

7. Siva Vaidhyanathan, *The Googlization of Everything: (And Why We Should Worry)* (Berkeley: University of California Press, 2011).

8. Omri Ben-Shahar and Carl E. Schneider, "The Failure of Mandated Disclosure," *University of Pennsylvania Law Review* 159 (February 2011): 671.

9. "New Study By Merrill Prof Finds Students Everywhere Addicted To Media," *https://merrill.umd.edu/2011/04/new-merrill-study-finds-students-everywhere-addicted-to-media*.

10. Adam L. Penenberg, "Social Networking Affects Brains Like Falling in Love," *Fast Company*, 1 July 2010, *www.fastcompany.com/1659062/social-networking-affects-brains-falling-love*.

11. Courtney Seiter, "The Psychology of Social Media: Why We Like, Comment, and Share Online," *Buffer,* 20 August 2017, *https://blog.bufferapp.com/psychology-of-social-media*.

12. Debates and research on this topic are summarized in Mark D. Griffiths, "Social Networking Addiction: Emerging Themes and Issues," *Journal of Addiction Research and Therapy* 4, no. 5 (2013), *www.omicsonline.org/social-networking-addiction-emerging-themes-and-issues-2155-6105.1000e118.pdf*.

13. John Herrman, "How Tiny Red Dots Took Over Your Life," *New York Times Magazine,* 27 February 2018.

14. Olivia Solon, "Ex-Facebook President Sean Parker: Site Made to Exploit Human 'Vulnerability,'" *Guardian*, 9 November 2017.

15. S. C. Matz et al., "Psychological Targeting as an Effective Approach to Digital Mass Persuasion," *Proceedings of the National Academy of Sciences of the United States of America,* 114 (28 November 2017): 12714–19.

16. Charles Arthur, "Facebook Emotion Study Breached Ethical Guidelines, Researchers Say," *Guardian,* 30 June 2014.

17. Ryan Calo, "Digital Market Manipulation," *George Washington Law Review* 82 (August 2014): 995.

18. Ari Ezra Waldman, "Privacy, Sharing, and Trust: The Facebook Study," *Case Western Reserve Law Review* 67, no.1 (2016): 193–233.

19. Marlies Glasius, "What Authoritarianism Is . . . and Is Not: A Practice Perspective," *International Affairs* 94 (May 2018): 515–33.

20. "The Top 20 Valuable Facebook Statistics—Updated November 2018," *Zephoria*, 28 November 2018, *https://zephoria.com/top-15-valuable-facebook-statistics*.

21. See the graphics on data generation at "Data Never Sleeps 6.0," Domo, 2018, *https://web-assets.domo.com/blog/wp-content/uploads/2018/06/18_domo_data-never-sleeps-6verticals.pdf*.

22. Craig Silverman, *Lies, Damn Lies and Viral Content* (New York: Tow Center for Digital Journalism, 2015), *http://towcenter.org/wp-content/uploads/2015/02/LiesDamn-Lies_Silverman_TowCenter.pdf*. Silverman notes that established news organizations' websites also "frequently promote misinformation in an attempt to drive traffic and social engagement."

23. Jennifer Kavanagh and Michael D. Rich, *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life* (Santa Monica: RAND Corporation, 2018), *www.rand.org/pubs/research_reports/RR2314.html*.

24. Adam J. Berinsky, "Rumors and Health Care Reform: Experiments in Political Misinformation," *British Journal of Political Science* 47 (April 2017): 241.

25. Whitney Phillips, *The Oxygen of Amplification: Better Practices on Extremists, Antagonists, and Manipulators Online,* Part 2 (New York: Data & Society, 2018), 3, *https://datasociety.net/wp-content/uploads/2018/05/2-PART-2_Oxygen_of_Amplification_DS.pdf*.

26. Alexandra Stevenson, "Soldiers in Facebook's War on Fake News Are Feeling Overrun," *New York Times*, 9 October 2018.

27. Neil MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," *New York Times*, 28 August 2016.

28. Knight Foundation, "Seven Ways Misinformation Spread During the 2016 Elec-

tion," *Trust, Media, and Democracy*, 4 October 2018, *https://medium.com/trust-media-and-democracy/seven-ways-misinformation-spread-during-the-2016-election-a45e-8c393e14*.

29. Onur Varol et al., "Online Human-Bot Interactions: Detection, Estimation, and Characterization," Proceedings of the Eleventh International AAAI Conference on Web and Social Media (Palo Alto: AAAI Press, 2017), *https://aaai.org/ocs/index.php/ICWSM/ICWSM17/paper/view/15587/14817*, 280.

30. Max A. Cherney, "Twitter Stock Plunges 21% After Earnings Show Effects of Fake-Account Purge," MarketWatch, 28 July 2018, *www.marketwatch.com/story/twitter-shares-slide-16-after-fake-account-purge-new-rules-in-europe-2018-07-27*.

31. Siva Vaidhyanathan, "Why Facebook Will Never Be Free of Fakes," New York Times, 5 September 2018.

32. Matt Burgess, "The Law Is Nowhere Near Ready for the Rise of AI-Generated Fake Porn," *Wired*, 27 January 2018, *www.wired.co.uk/article/deepfake-app-ai-porn-fake-reddit*.

33. Leo G. Stewart, Ahmer Arif, and Kate Starbird, "Examining Trolls and Polarization with a Retweet Network," paper presented at MIS2: Misinformation and Misbehavior Mining on the Web, Del Rey, Calif., 9 Feburary 2018, *https://faculty.washington.edu/kstarbi/examining-trolls-polarization.pdf*.

34. Charlie Warzel, "This Group Posed as Russian Trolls and Bought Political Ads on Google. It Was Easy," *Buzzfeed News*, 4 September 2018, *www.buzzfeednews.com/article/charliewarzel/researchers-posed-as-trolls-bought-google-ads*.

35. Paul Lewis, "'Fiction Is Outperforming Reality': How YouTube's Algorithm Distorts Truth," *Guardian*, 2 February 2018.

36. Craig Timberg, Elizabeth Dwoskin, and Andrew Ba Tran, "Mainstream Advertising Is Still Showing Up on Polarizing and Misleading Sites—Despite Efforts to Stop It," *Washington Post*, 3 October 2018.

37. Karsten Müller and Carlo Schwarz, "Fanning the Flames of Hate: Social Media and Hate Crime," (2017), *http://dx.doi.org/10.2139/ssrn.3082972*.

38. See Seva Gunitsky, "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability," *Perspectives on Politics* 13 (March 2015): 42–54.

39. Jacob Weisberg, "The Autocracy App," *New York Review of Books,* 25 October 2018.

40. Thomas Rid, "Why Twitter Is the Best Social Media Platform for Disinformation," *Motherboard,* 1 November 2017, *https://motherboard.vice.com/en_us/article/bj7vam/why-twitter-is-the-best-social-media-platform-for-disinformation*.

41. Ron Deibert, "Authoritarianism Goes Global: Cyberspace Under Siege," *Journal of Democracy* 26 (July 2015): 64–78.

42. Sarah McKune and Ronald Deibert, "Google's Dragonfly: A Bellwether for Human Rights in the Digital Age," *Just Security*, 2 August 2018, *www.justsecurity.org/59941/googles-dragonfly-bellwether-human-rights-digital-age*.

43. See, for example, the proposal of Tim Berners-Lee at *www.inrupt.com*.