The Road to Digital Unfreedom: The Threat of Postmodern Totalitarianism

Larry Diamond

THE THREAT OF POSTMODERN TOTALITARIANISM

Larry Diamond

Larry Diamond *is senior fellow at the Hoover Institution and the Freeman Spogli Institute for International Studies at Stanford University, and founding coeditor of the* Journal of Democracy.

Rarely in history have views about the social impact of a new technology swung so quickly from optimism (if not euphoria) to pessimism (if not despair) as has been the case with respect to social media. Once hailed as a great force for human empowerment and liberation, social media—and the various related digital tools that enable people to search for, access, accumulate, and process information—have rapidly come to be regarded as a major threat to democratic stability and human freedom.

To be sure, even seven or eight years ago there was widespread recognition of the dark side of digital tools. Concern back then, however, mainly had to do with authoritarian regimes seeking to extend censorship and control deep into cyberspace. Governments and organizations in the advanced democracies thus invested in new tools (such as virtual private networks, or VPNs) and offshore platforms to help independent media and civic movements to expand the boundaries of freedom and accountability. From early on, there was also keen awareness of the adaptive ability of malign actors—jihadists, other violent extremists, and criminals—to exploit the openness of the internet for destructive ends.[1] But there was optimism that these dark forces could be contained, and that the positive, democratizing effects of people connecting more freely with one another and with diverse sources of information would outweigh authoritarian and criminal exploitation of the digital realm.

As the three articles that follow make clear, the perceived sources of threat are now much more ominous, powerful, and diverse. The prevailing view less than a decade ago was of "a technological race underway between democrats seeking to circumvent Internet censorship and dictatorships that want to extend and refine it."[2] That has now given way to

a sense that democrats worldwide are in a race against time to prevent cyberspace from becoming an arena of surveillance, control, and manipulation so all-encompassing that only a modern-day fusion of George Orwell's *Nineteen Eighty-Four* and Aldous Huxley's *Brave New World* could adequately capture it.

Part of the problem, we now better understand, is the business model of social-media companies. These derive their revenue streams from selling ads and commercializing access to user data. Both forms of revenue require harvesting as much data as possible about as many users as possible, who also must be induced to spend as much time as possible on social media. The major social-media platforms, and the staggering array of apps that people have on their computers and mobile phones, all have one common logic: attention addiction. The more users are riveted to a social-media platform, a website, or an app, the more ads they will see, the more personal data they will unwittingly give up, and the more revenue the company will gather.

In an influential 2016 essay, former Google "design ethicist" Tristan Harris—who trained as a magician in his youth—explored some of the similarities between magic and digital tools. First, both give people the illusion of choice, while actually controlling the menu of options—a crucial pathway to manipulation. Second, mobile phones, social media, and especially digital apps and games, function like slot machines, hooking people's attention by giving them "intermittent variable rewards," which psychological research has shown to be highly addictive—and for the provider, staggeringly profitable. Third, the constant novelty of social-media flows generates a "fear of missing something important," and hence addictive engagement.[3] (Even email has these addictive logics.)

Traditional media have had their own way of riveting attention, as reflected in the mantra "if it bleeds it leads"—meaning that gory and sensational content captivates readers and viewers. Social media do that, too, elevating content that is shocking, infuriating, controversial, hilarious, or emotive in some way—so long as it rivets our attention. The more that attention is riveted, the more time is spent on the digital tool, the more users are attracted to the site to spend time, the more personal data is accumulated, the more ads are seen and sold, the more those ads can be precisely targeted at users who will buy what they are selling, and the more revenue rolls in.

The fundamental dilemma is that what is good for digital business is not necessarily good for democracy—or even for our individual mental and physical health. This, as Ronald J. Deibert notes in his opening essay, is one of "three painful truths about social media." As he states it, the "social-media business model is based on deep and relentless surveillance of consumers' personal data in order to target advertisements." That surveillance comes when users check the box with the terms and conditions for use of digital platforms. Few people ever read these terms

carefully, and thus few are aware of how much information about their personal tastes, social experiences, friendships, political views, health, and even sexual preferences is being swallowed up by these vast data-gathering machines and made available commercially. Moreover, even if users do understand, they cannot restrain themselves because they are seriously *addicted* (in what Deibert calls "a powerfully subconscious and hormonal way") to social media.

Enter Big Brother

Now imagine that it is not just private companies that are collecting and integrating all this user data into comprehensive psychological and behavioral portraits of each individual, but governments as well. Democratic states may seek access to some user data to look for evidence relating to criminal investigations or threats to national security. And although these governments may be overzealous in their requests, at least their citizens have legal rights to privacy vis-à-vis the state. Authoritarian regimes, however, grant their citizens no effective rights of privacy and have no compunction about demanding unfettered access to all this data. What if a government not only wants to know everything there is to know digitally about all its citizens, but also has the means to collect it and analyze it? That, increasingly, is the Orwellian world which we are entering.

While social media still serve in many countries as outlets for dissidents, investigators of corruption, and mobilizers of political participation and protest, they are also increasingly straining democratic systems and, in Deibert's words, "driving the spread of authoritarian practices." In democracies, the deleterious political effects of social media are making themselves felt through three broad mechanisms. First, while social scientists debate whether politics is really more polarized online than offline, people clearly tend to gather into social-media echo chambers (what Deibert calls "filter bubbles") that reinforce their points of view.

Second, while many print publications and cable-television stations (and even radio networks) build echo chambers of their own with hard-edged, polarizing points of view, they at least tend to exercise some degree of editorial control over the tone and substance of their content. Online, however, anything goes; anyone can become a publisher or editorialist—or claim to be a journalist. Indeed, some sites have as their *raison d' être* the generation and dissemination of outrageous content—and the more offensive the better, regardless of the facts. Truth and civility, two of the most precious requisites for sustainable democracy, quickly become victims of this escalating information warfare, and the culture of democracy—of mutual tolerance, respect, and restraint—is severely degraded. It is hard to imagine that social media are not playing a significant role in the pervasive trend of deepening political polarization and increasingly strident, abusive politics in democracies around the world.

Third, social-media platforms lacking robust editorial filters—or at least struggling to figure out how to implement them—do not just give people wide scope to post hateful language, absurd rumors, and outrageous lies. Worse still, organized actors, including foreign governments, may manipulate information flows for carefully targeted political and social ends, as the Kremlin and its affiliated Internet Research Agency have done in elections in the United States and much of Europe. The campaign of information manipulation is waged by vast armies of state-sponsored trolls (paid agents of online provocation and conflict) and bots (automated accounts that can be programmed to post rapid-fire, provocative content). This may put even the core feature of democracy—the integrity of elections—gravely at risk. Moreover, the problem of malign disinformation (from both foreign and domestic sources) will mount alarmingly with the rapid progress of "deep fakes," which, as Steven Feldstein explains in his essay, use artificial intelligence to take the visual image and actual voice of a person and animate them convincingly to say things they never said.[4]

As all three articles in this cluster note, the revolution in artificial intelligence (AI) has become a boon to authoritarian forces. AI involves the ability of a computer to learn from data and then generalize and extrapolate to make decisions. Thus, it gets better—more effective and precise—as it is able to process more and more data, which enables it to decide, respond, or perform in a more and more accurate fashion. In fact, the more data AI researchers have, the further they will be able to push its limits. Here the advantage lies with the biggest information companies, such as Google, and the biggest authoritarian states, above all China.

This brings us to the most frightening element of the current critical juncture in the advance of digital technologies. As Feldstein indicates and as Xiao Qiang explores in greater depth in his essay, China is betting heavily on an integrated, holistic approach to information technology. It is suffusing cities with surveillance cameras that are capturing on video where people go, what they do, and whom they are with. Equipped with this vast trove of video imagery from a population of more than 1.4 billion people, China is refining what is generally regarded to be the most sophisticated facial-recognition software in the world. To this it is adding voice recognition, advanced biometrics, and increasingly aggressive collection of DNA, as well as all the private data from Chinese tech companies such as Alibaba, Baidu, and Tencent (in China there is no enforceable wall of separation between "private" companies and the party-state). Add in as well new scanning technology that can quickly capture the entire volume of data in an individual's mobile phone. The result is a nightmarish modern-day version of *Nineteen Eighty-Four,* or what I term "postmodern totalitarianism," in which individuals appear to be free to go about their daily lives, but the state controls and censors all information flows while compiling "social-credit scores" that mash up every type of digital

footprint an individual leaves into an overall indication of political and social reliability. Those who avoid criminal or antisocial behavior—and any kind of disrespect to the party-state and its leaders—can enjoy the fruits of a rapidly modernizing society and grow rich. Those who question (not to mention challenge) the system will face harsh consequences. They may not be arrested, for they may not need to be. But they will be unable to travel, to educate their children properly, or to leave the country. Under these circumstances, even if citizens refuse to drink the political Kool-Aid of Communist Party propaganda, they will not dare to speak the truth. Whether this system will be able to continue on its march to total social control—and whether U.S. digital giants such as Google and Facebook collaborate in this process—will have profound implications for the future of freedom not just in China but in the whole world.

The three essays that follow explore key challenges that are confronting contemporary democracies: their growing vulnerability to online polarization and manipulation; the new threats to individual rights and privacy in the digital age; how to reconcile the business model of social-media companies with their responsibilities to democratic societies; and how to rein in the efforts of authoritarians to advance and diffuse digital technologies of surveillance and control. As Feldstein suggests, democracies must establish for themselves clear human-rights frameworks for the use of AI and seek to have these adopted worldwide.

These are no longer problems of a specialized field of political studies. Increasingly, it is impossible to separate the spheres of online politics and offline politics. Digital rights are human rights, and human rights are digital rights. Hence, the *Journal of Democracy* will be addressing these questions extensively in its coming issues by featuring a variety of views, including some that will sound a more hopeful note.

NOTES

1. Ronald Deibert and Rafal Rohozinski, "Liberation vs. Control: The Future of Cyberspace," *Journal of Democracy* 21 (October 2010): 43–57.

2. Larry Diamond, "Liberation Technology," *Journal of Democracy* 21 (July 2010): 81.

3. Tristan Harris, "How Technology Hijacks People's Minds—from a Magician and Google's Design Ethicist," 19 May 2016, *www.tristanharris.com/2016/05/how-technology-hijacks-peoples-minds%e2%80%8a-%e2%80%8afrom-a-magician-and-googles-design-ethicist.*

4. James Vincent, "Watch Jordan Peele Use AI to Make Barack Obama Deliver a PSA About Fake News," *The Verge,* 17 April 2018, *www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peele-buzzfeed.*