8

Responding to Digital Repression

This book has sought to explain how authoritarian leaders wield digital technologies to advance their repressive objectives. But the intersection of politics and digital technology is not a one-way street in which repressive states always have the advantage. This domain also offers opportunities for democracies, civil society groups, and political activists to fight back against digital repression trends.[1] In this final chapter, I present ideas and solutions for how civil society and democracies can combat such repressive strategies.

Revisiting an earlier question provides a useful starting point: how is digital technology reshaping the balance of power between government and civil society? For states with highly developed coercive capacity, the emergence of formidable technological tools presents new opportunities to cement their power. As more and more citizens gravitate online, governments' have gained crucial advantages by honing their ability to track individuals' movements, snoop on their conversations, and obtain unprecedented insights into what dissidents and potential rivals may be thinking or planning. In some places, particularly China, the balance of power has clearly shifted. The possibility that civic activists will be able to reverse the CCP's governance consolidation is remote.

But China is fairly unique in this respect. Even in authoritarian states like Russia and Iran, their governments are keenly aware that the same tools they use to manipulate public opinion, tar opponents, and rig elections can easily be turned against them. This is why so many regimes are fearful (and frequently resort to violence) when mass demonstrations occur—particularly in light of the turmoil stemming from the Arab Spring protests. In several important ways, digital technology has corroded such states' prior advantages even while providing them with new repressive tools.

First, the state's information advantage has weakened. Thirty years ago, state media wielded real influence over what citizens saw and heard. In fact, one of the first principles to undertaking a successful coup was to occupy state television and radio broadcast stations in order to control the transition narrative. Such

The Rise of Digital Repression. Steven Feldstein, Oxford University Press (2021). © Oxford University Press.
DOI: 10.1093/oso/9780190057497.003.0008

advice seems archaic in the new information age. While governments can still dominate the airwaves, the emergence of alternative information sources has changed the dynamic.

Second, barriers to political mobilization have decreased. Social media has lessened collective action problems that previously had prevented masses of people from taking to the streets. Even as governments have begun monitoring and manipulating mainstream platforms (responding to the examples of Facebook and Twitter revolutions in the Middle East, Ukraine, and elsewhere), activists have innovated. They have embraced new messaging apps like Telegram or Signal that feature end-to-end encryption and are more difficult for state agents to monitor and manipulate. Just look at the difference in technologies wielded by Hong Kong protestors in 2019 compared to those of the 2014 umbrella movement (discussed in this chapter).

Third, there are more resources to support digital movements that challenge a state's power and more opportunities to activate transnational networks, as well as to get companies and democratic governments to push back against oppressive governments. A digital playbook has emerged. Activist organizations are sharing lessons learned.[2] They are setting up how-to workshops to provide tips about spreading protest hashtags, safeguarding communications from government intrusion, and determining if devices have been hacked. When governments lash out—when they shut down the Internet, acquire spyware to break into journalists' smartphones, or enact information controls to block access to websites and apps, for instance—their actions do not go unheeded. A constellation of actors immediately respond. Take Internet shutdowns. Netblocks and OONI are usually the first to sound the alarm and provide data measurements documenting that connectivity has been cut off. Groups like Access Now, Human Rights Watch, Privacy International, or Article 19 then circulate online petitions and policy briefs demanding that the offending government cease its actions. Lawsuits are readied that are designed to force telecoms to stop blocking Internet connectivity. And finally, democratic governments are lobbied so that they will raise concerns bilaterally or in multilateral forums to further pressure India, Iran, or Sudan to restore digital access.

In other words, the employment of digital tools in civic and political struggles is not one-sided. Civil society organizations possess many such tools with which they can combat state repression.

This chapter begins by discussing strategies civil society groups can use to raise the costs of repression associated with the dictator's digital dilemma. It then examines specific innovations activists can pursue to counter state repression. Turning to the private sector, I then discuss companies' roles and responsibilities in relation to digital repression. Finally, I review methods that local groups could potentially use to confront transnational support from

technologically sophisticated authoritarian states like China and Russia and reflect on what changes the Covid-19 pandemic may bring to this domain.

Raising the Costs of Repression: Shifting the Dictator's Digital Dilemma

In Chapter 2, I introduced the concept of the dictator's digital dilemma, the problem faced by repressive leaders who seek to benefit from the economic gains and political advantages of a digital society—without sacrificing political control. I offered China as a leading example of a country that has at least temporarily solved its digital dilemma, but noted that China's model is not applicable to most other countries. Instead, other authoritarian states or hybrid regimes have pursued alternative strategies: regional shutdowns targeting certain populations (Cameroon, Ethiopia), Internet restrictions designed to maximize state control while mitigating economic harm (Thailand), or social manipulation and disinformation tactics that supplement or replace Internet controls altogether (the Philippines, Myanmar). These tactics have been effective; many states have reaped considerable economic benefits from digital technology without paying a price for suppressing digital freedoms.

But this needn't be the case.

A strategic question civil society groups and their democratic partners should consider is how to raise the cost of digital repression so that solving the dictator's digital dilemma becomes prohibitively expensive for governments. As Table 8.1 summarizes, a successful strategy incorporates four points of pressure: reputational costs, economic costs, political factors, and supply-side considerations. In many respects, these actions reflect existing strategies rights activists use to push back against repression generally. But existing strategies must be extended to cover the new domains of digitally repressive technologies and actions.

First, governments pay attention to actions that affect their reputations. States spend inordinate amounts of time and political capital protecting their standing and pushing back against public criticism. During my time serving as a diplomat in the State Department, I saw this dynamic play out time and again in a variety of international forums. The UN Human Rights Council (HRC) is a good case in point. Despite absorbing a heavy dose of criticism for allowing countries with egregious human rights records to serve as members (current membership includes notorious abusers such as Cameroon, Pakistan, Qatar, and Venezuela), the HRC's resolutions and authorized investigations against alleged human rights violations carry significant weight. Governments go out of their way to water down human rights condemnations or to block embarrassing votes

Table 8.1 **Pressure Points Related to the Dictator's Digital Dilemma**

Pressure Points			
Reputational	***Economic***	***Political***	***Supply side***
Naming and shaming in international forums	Economic pressure campaigns	Raising public awareness about the repressive effects of digital instruments	Pressure campaigns against companies
Media strategies (traditional and social media)	Corporate boycotts	Electoral challenges to incumbents	Collaborating with companies on technical solutions and antirepression tools
Citizen documentation of repression	Sanctions		Government restrictions (e.g., export controls)

that would expose them to public censure. I recall several HRC votes that were nail-biters despite involving situation such as targeted violence in Burundi authorized by its president, mass imprisonments of protestors in Ethiopia, and constitutional manipulation in the Congo. Country delegations vigorously opposed these resolutions. Even with airtight evidence of human rights transgressions, the offending states pushed the Africa regional bloc to withhold support for the resolutions and threatened to obstruct future multilateral priorities. These situations demonstrate that even the proceedings of a secondary UN body matter greatly to scores of countries. Smaller countries are particularly sensitive to international disproval and are very willing to offer concessions in order to delay or reduce international censure.

Thus, a key point of leverage against digitally repressive governments is to use international forums like the HRC to raise the reputational costs of continued bad behavior. As countries perceive that the ongoing suppression of political freedoms is leading to an increase in international criticism, this shift may cause internal rethinking about whether the benefits of maintaining censorship controls or instigating Internet shutdowns is worth the price.

In addition to leveraging international forums, advocates can also make use of simple technological tools to spread awareness (and outrage) about government repression. States no longer enjoy a monopoly on information—save for a few closed regimes like North Korea. As the Pew Research Center details, around five billion people globally own mobile devices, half of which are smartphones outfitted with cameras.[3] This widespread access to mobile technology means that victims, observers, and even wrongdoers can document human rights violations and quickly disseminate them. Governments comprehend that their citizens will eventually learn about coercive actions that they have undertaken. In response,

they use counterstrategies such as filtering information their populations can access (this requires substantial resources and technical sophistication to sustain), or employing disinformation-flooding techniques to drown out unfavorable news. These tactics can be effective, but they also have limitations. On-the-ground documentation of repressive acts (such as violent crackdowns against protestors in Sudan and Iran in 2019) are difficult to suppress and have a powerful impact when they are exposed. Civil society groups that have established networks of individuals who can capture evidence of government repression and then publicize it to the outside world can galvanize internal dissent against a regime and generate critical shifts of opinion at home and abroad.

Correspondingly, it is important for groups to implement media broadcast strategies—using mainstream outlets and social media platforms—that will cut through obfuscation and disinformation generated by governments. No matter how egregious a regime's actions appear, it can be challenging for groups to disseminate a message that the public perceives as credible and that citizens will share widely. Governments are highly sophisticated when it comes to promoting narratives to delegitimize civil society (e.g., accusing groups of being foreign funded or antipatriotic). But when advocates' messages do break through, the reputational effects can be significant.

In Ethiopia's case, I saw such a reputational strategy pay off in relation to the imprisonment of members of an online collective known as the Zone 9 bloggers. In 2014, the government arrested this group on terrorism charges. While the US government pressed the Ethiopians for months to drop the charges and release the prisoners, a public pressure campaign led by groups such as the Committee to Protect Journalists, Global Voices, the Electronic Frontier Foundation, and Human Rights Watch gained steam.[4] They circulated international petitions, organized public events, and reinforced their messaging on social media. By 2015, prosecutors dropped charges and the journalists were freed. There was never any significant doubt about the Zone 9 bloggers' innocence. They had no known linkages to terrorist groups; their arrests were purely symbolic and meant as a warning to other dissenters. As long as the international community stayed quiet, Ethiopian authorities could get away with the imprisonments: the political costs were minimal, and the accrued benefits were high. Once external reputational costs to the regime began to rise, however, this dynamic changed their internal calculus and led to the bloggers' releases.

Second, imposing economic costs on state repression also contributes to changes in behavior. Many successful transnational movements—such as the Responsible Mineral Initiative or the antisweatshop movement (both of which generated economic boycotts)—sparked reforms in countries where there was little incentive to change the status quo. Financial penalties working in tandem with reputational costs can have a powerful effect. For example, if human rights groups

convince democratic member states to offer a UN resolution condemning online censorship in Egypt, this action may embarrass the regime, but it is unlikely to alter policy. However, if the resolution is reinforced by corporate boycotts, economic pressure campaigns, or even sanctions that cause governments and companies to refrain from doing business with the offending government until it alleviates digital restrictions, the collective pushback provides a lot more bite. Such situations directly address a key aspect of the digital dilemma, changing economic considerations and placing public support for the regime at risk.

As discussed in Chapter 4, the Thai public displayed far greater sensitivity to the perceived economic costs of the government's Internet control plan than outrage over reductions in political freedoms. When the government tried to establish a single Internet gateway to regulate all information coming in or out of the country, their actions generated a middle-class backlash—citizens were alarmed by the proposal's potential harm to the economy.[5] We should note, however, that a fine line exists between targeted economic actions intended to change specific behaviors—such as getting a government to withdraw a punitive cyber libel law used to persecute civil society—versus actions intended to bring systemic change, such as demanding an end to all government surveillance. The former represents a concrete step that governments can straightforwardly carry out; the latter represents an unattainable demand.

The third element involves imposing political costs on digitally repressive actions carried out by the regime. A key step is to raise public awareness about the repressive consequences of specific systems or functions that the regime is deploying. For example, in 2019, journalists disclosed that the Serbian government had partnered with Huawei to install a mass surveillance system powered by facial recognition in Belgrade that encompassed one thousand cameras in eight hundred locations throughout the city, as I mentioned in Chapter 7. The announcement came at an inauspicious moment—coinciding with months of political protests against populist president Aleksandar Vucic. As *AP News* noted, "Some protesters began having second thoughts about joining anti-government demonstrations in the Serbian capital."[6] There were reports that the police had leaked videos of individual protestors to pro-government outlets, which published their images and identities. Journalists even documented joint patrols undertaken with Chinese police officers in Belgrade, ostensibly to assist Chinese tourists visiting the city (although many ascribed darker purposes for this intimidating show of force).[7] As the public has become aware of this technology, concern has grown. The civil society group SHARE Foundation explains, "Hundreds of people have submitted freedom of information requests asking the Ministry of Interior about said cameras, while public officials made contradictory statements and withheld crucial information."[8] SHARE has joined with other oversight groups to publish a detailed brief laying out why the surveillance system violates Serbia's Law on

Personal Data Protection. The next step for these groups is to translate public backlash into political repercussions at the ballot box.

Similarly, in Uganda, the *Wall Street Journal* disclosed that authorities had purchased a facial recognition surveillance system from Huawei for $126 million.[9] Until journalists exposed the contract, there was zero public recognition about the existence of this technology, how the government planned to use it, or its intended purpose (in the same article, reporters uncovered that Huawei technicians helped the government spy on political opponents by breaking into social media accounts—establishing a clear link between government hacking and the state's repression agenda).[10] Ugandan opposition lawmakers have subsequently criticized the project for its lack of transparency and potential security vulnerabilities: "There appears to be a policy to hand over the country's entire communications infrastructure to the Chinese, . . . It's unwise given our concerns about spying and creating backdoor channels."[11] It is vital that civil society groups not only monitor Uganda's system for abuse, but that they also levy a political cost on the government for allocating scarce resources in order to acquire this tool. Possible outcomes include (1) the government rescinds its purchase of the system due to public backlash (bringing a victory against digital repression), (2) the government continues using the system but pays a political price at the ballot box, or (3) authorities continue employing the system but cancel plans to install additional networks—representing a partial win against the spread of digital repression in Uganda. Raising the political cost of digital repression through public campaigns and electoral challenges at the ballot box can cause governments to reconsider their digital repression agendas.

While the first three elements focus on demand side factors, the fourth element shifts attention to supply-side considerations. Here, the goal is to pressure technology platforms, manufacturers, and service providers to restrict capabilities provided to repressive governments.

One approach is for groups to directly pressure companies to reduce repressive uses of their technology. Facebook's actions in the Philippines illustrate that companies will take concrete steps to limit exploitation of their platforms if they receive enough negative attention. The general consensus, as Maria Ressa describes it, is that either through benign neglect or by deliberately overlooking rampant disinformation, Facebook facilitated Duterte's rise and "broke democracy" in the Philippines.[12] The company has belatedly responded as public outrage has grown; in 2019, Facebook removed two hundred pages, groups, and accounts for undertaking "coordinated inauthentic behavior." Among those penalized was Nic Gabunada, Duterte's online campaign manager.[13] Facebook has suggested that it may implement further removals. More recently in Brazil, Facebook, Google, and Twitter simultaneously removed posts that had been shared by President Jair Bolsonaro that included misinformation related to the

coronavirus. Facebook stated that the contents of Bolsonaro's posts violated their rules against sharing harmful content.[14] This action represented one of the first times that the company had chosen to deviate from stated policies of "not fact-checking politicians," and to specifically take down posts linked to a sitting head of state.[15] Subsequently, Twitter and Facebook revamped their rules ahead of the 2020 US elections and began attaching warning labels to misleading posts coming from US president Donald Trump and his allies.[16]

An important takeaway is that countering government disinformation by pressuring tech companies—who are themselves sensitive to reputational damage—can reap considerable dividends. Conversely, governments recognize the gatekeeping function that Facebook plays and are willing to employ their own hardball tactics as well. In Vietnam, Reuters reported that state-owned telecoms took Facebook's servers offline for nearly two months to pressure the company to censor antigovernment comments. During that period, Facebook "became unusable at times." The company caved to government demands, stating that it had decided to "restrict access to content which it has deemed to be illegal."[17]

Social manipulation and disinformation are not the only relevant digital repression techniques that governments use. Yet the same strategy also applies with regard to spyware providers or telecoms carrying out Internet shutdowns. For instance, when revelations first emerged about Sandvine's deep packet inspection technology enabling Belarus authorities to selectively block websites in response to mass protests, the company initially defended its conduct and bizarrely claimed that Internet content didn't count as "a part of human rights."[18] As outrage grew, Sandvine quickly changed its tune. Less than a week later, the company announced it had terminated its end-user license agreement with the Belarusian government, adding that the company "takes human rights abuses very seriously."[19]

Similarly, digital rights groups have pursued an increasingly active litigation strategy against telecoms that enact Internet shutdowns. In countries ranging from India and Zimbabwe to Sudan and Pakistan, advocates have scored courtroom victories where judges have ordered telecoms to restore Internet service. In Sudan, for instance, Abdelazeem Hassan sued telecommunications company Zain, arguing that depriving individuals of Internet access violated their consumer rights. He prevailed in the case (although Zain only restored service to his personal devices, contending that he filed the lawsuit in his personal capacity).[20] Hassan then went back to court and sued MTN and Sudatel to restore Internet access as well. In the second ruling, the court ordered the restoration of all Internet services in Sudan, not just for Hassan's devices.[21]

A second supply-side approach is for groups to work directly with technology companies to implement engineering safeguards or technological fixes that will constrain *ex ante* autocratic exploitation of products. In 2019, for example,

WhatsApp began imposing message-forwarding restrictions to stop misinformation. At first, the company reduced the number of groups users could forward messages to from 256 to 20. Then WhatsApp lowered the number to 5. Research suggested that these changes were having a positive effect in slowing down bad information.[22] In April 2020, WhatsApp imposed even more stringent controls in response to alarming levels of coronavirus misinformation, stipulating that messages flagged as "highly forwarded"—sent through a chain comprised of at least five people—could now only be forwarded to a single person.[23]

As a result of these changes, not only has WhatsApp slowed the spread of bad information, but it has also deprived autocrats of a key tool used to reinforce their political narratives. It's worth noting that WhatsApp's decisions have not come without cost. Far-right commentators in places like Brazil, Spain, the United States, Hungary, and the Philippines have blasted the company for engaging in Internet censorship, proving that, as one tech company official put it, "the right thing to do is oftentimes contested."[24]

A third supply-side approach is for advocates to pressure democratic governments to put export controls in place that limit the sales of certain technologies to repressive regimes. Currently, there are few formal mechanisms that exist, in part due to the newness of this field. The most applicable framework is the Wassenaar Arrangement, consisting of forty-two developed economies that coordinate export controls related to conventional arms and dual-use technology.[25] While the group added targeted surveillance tools to its list of technologies that require additional controls in 2013, this is the extent to which digital instruments face any sort of regulation.[26] Moreover, because Wassenaar is nonbinding and lacks an enforcement mechanism, it has not been effective in restricting unlawful software surveillance. (As Kaye observes: "It is insufficient to say that a comprehensive system for control and use of targeted surveillance technologies is broken. It hardly exists.")[27] This suggests that if groups hope to convince governments to restrict the exportation of digital tools to repressive regimes, they must rely on advocacy and ad hoc arrangements.

One of the most prominent recent efforts—intended to penalize Chinese companies responsible for providing repressive technology in Xinjiang—has borne some fruit. On October 9, 2019, the US Commerce Department announced it had added twenty-eight Chinese government and commercial firms to its "entity list" for human rights violations related to the "repression, mass arbitrary detention, and high-technology surveillance" against minority groups in Xinjiang.[28] Included among the twenty-eight entrants are leading Chinese AI companies such as Hikvision, iFlytek, SenseTime, Megvii, Yitu, and Dahua. The financial implications are considerable. Companies on the list are restricted from acquiring certain sensitive technologies and components from US firms pending specific licenses that the US government must approve (a time-consuming and

laborious process that can effectively serve as a de facto ban). High-profile partnerships with leading US universities have been cancelled, including a five-year venture between iFlyTek and the Massachusetts Institute of Technology.[29]

While some experts maintain that the United States had its own strategic motives for adding these companies to the list—including protecting US interests in AI—this announcement centered around major human rights violations in Xinjiang.[30] Without persistent advocacy, it is highly unlikely that the government would have moved this designation forward. These examples illustrate that imposing supply-side costs on digitally repressive regimes is an effective lever, particularly when implemented in conjunction with the other three elements.[31]

Some policymakers argue that leaning too heavily on supply-side measures to influence policy brings unintended consequences. When I was in government, a common refrain I heard was that restricting US exports to repressive regimes would simply cause countries to procure this equipment from authoritarian sources—such as from China or Russia. Officials claimed that it was preferable for US companies to supply this technology and influence recipient governments to use it responsibly rather than cede the market to the Chinese or Russians. They argued that end-use agreements were effective ways to ensure human rights compliance. In truth, such claims are specious—the evidence shows that no matter where such technology originates, it tends to enable bad outcomes when placed in the hands of repressive regimes (as Sandvine's technology in Belarus illustrates).

One exception relates to social media platforms: US and Chinese companies exhibit major differences with respect to human rights and civil liberties concerns. Chinese firms like WeChat or Weibo are essentially walled off from advocacy groups and immune to outside pressure on politically sensitive issues. Moreover, China's system of intermediate liability forces its Internet companies to implement a broad array of filtering and censorship. As researchers from the Citizen Lab write, "Any Internet company operating in China is subject to laws and regulations that hold companies legally responsible for content on their platforms. Companies are expected to invest in staff and filtering technologies to moderate content and stay in compliance with government regulations. Failure to comply can lead to fines or revocation of operating licenses."[32] Such regulation means that Chinese platforms facilitate two repressive techniques for the price of one: government disinformation with minimal restraints and extensive censorship subject to the whims of the Chinese state. In contrast, even though Facebook may have "broken democracy" in places like the Philippines, it is better positioned to make amends for its past decisions.

Deconstructing the dictator's digital dilemma and identifying relevant pressure points can yield tangible democratic benefits. The right strategy

implemented in the right contexts can be an important means to counter digital repression tactics. These methods are most effective in small or medium-sized countries where leaders' consent to govern is premised on solid economic growth. Countries like Kenya, Uganda, Brazil, Serbia, the Philippines, Thailand, Malaysia, and Ecuador are prone to using digital repression techniques. They fluctuate between autocratic and democratic periods of rule, have publics that are sensitive to economic conditions, and possess just enough political competition to keep the ruling coalition on edge. In such countries, well-timed interventions can make a difference. In contrast, larger states with more consistent patterns of digital repression (China, Russia, Iran, Turkey) or highly autocratic smaller states (Tajikistan, Oman) are less susceptible to these strategies.

Pushing back against discrete aspects of digital repression (punitive laws, egregious surveillance methods, persecutions of specific individuals) is much easier than effecting systemic change. Such is the difference between advocating for the release of the Zone 9 bloggers in Ethiopia versus pressuring Egypt to end mass surveillance and widespread suppression of dissent. An effective strategy provides offramps for change. It proposes achievable steps to alleviate the worst effects of digital repression, but is cautious about making excessive demands that would undercut the whole bargain.

Grassroots Strategies for Civil Society

The ideas above provide a macro framework for how civil society groups can leverage distinct points of pressure to shift government behavior and deter digital repression. It's useful to apply another layer of analysis to examine innovative local approaches that activists can pursue to counter state repression strategies.

First, there is a large investigative gap when it comes to adequately scrutinizing digital projects implemented in individual countries. Governments are able to get away with abusive tactics in part because of widespread public ignorance about which tools intelligence agencies are acquiring and how they are using those instruments. The good news is that exposing government secrets and enhancing accountability no longer requires a highly resourced media sector or established journalistic corps. Digital technology has changed the rules of the game. More than ever, citizen activists are able to employ open-source intelligence (OSINT) to expose government wrongdoing, publicize its impact, and catalyze reform.

The organization Bellingcat illustrates the rapidly changing nature of the field. Bellingcat was founded in 2014 by Eliot Higgins, an unemployed British journalist who had gained attention for his meticulous open-source investigation of 2013 chemical weapons attacks authorized by the Syrian government.[33] Higgins

initially funded the organization from a Kickstarter campaign, which listed two objectives: bring together reporters and activists who have transformed journalism through the use of open-source tools, and attract others to learn how to use these same tools and technologies.[34] The results have been impressive. Bellingcat's investigations of the 2014 downing of Malaysian airliner MH17—as well as the 2018 poisoning of Sergei Skripal (a former Russian spy) and his daughter in England by two Russian military intelligence officers—have received wide acclaim. The MH17 investigation illustrates how Bellingcat used a full range of open-source intelligence tools to put together a convincing case against Russian authorities. The Bellingcat team combed through social media for relevant image postings during the time frame of the airline crash. As images were identified, the team geolocated crash sites using Google Earth. This process allowed Bellingcat to construct a course for a specific Russian missile launcher—which was used to shoot down the airplane—by placing images on a map corresponding with the time for each sighting.[35]

Bellingcat's success is reflected in a trove of similar investigative efforts.[36] As Muhammad Idrees Ahmad writes, other examples include "the New York Times's investigations into the killing of the Gaza medic Rouzan al-Najjar and identifying the killers of Jamal Khashoggi; Africa Eye's work on the Cameroon killings; DFRLab's work on Twitter trolls; and UC Berkeley Human Rights Center's contribution to Reuters's Pulitzer Prize-winning investigation in Myanmar."[37] These investigations typically rely on detailed online forensics work using social media platforms that connect inputs from multiple analytic sources.

Consequently, there are many opportunities for civil society groups to learn the basics of how to conduct open-source investigations. Bellingcat itself sponsors "how to" trainings for citizen activists.[38] The company also publishes detailed guides tailored for specific issues, such as monitoring Covid-19 economic slowdowns using open-source data, or methods to probe coronavirus disinformation.[39]

Second, civic organizations should consider making emergent learning strategies a central feature of how they operate. In Chapter 6, I discussed how Jawar Mohammed used emergent strategies to circumvent Ethiopian information controls and sustain a broad-based protest movement. Such strategies are especially relevant for groups that confront governments with superior capabilities under conditions they are unable to control. The only way for organizations to remedy this imbalance is to pursue adaptive and creative measures. As researcher Ionut C. Popescu describes it, emergent strategies are a process of "navigating through an unpredictable world by improvisation and continuous learning." While "deliberate" strategies focus on control and ensuring that managerial directives are fulfilled, "emergent strategy emphasizes learning—coming to understand through the taking of actions what those intentions should be in the first place."[40]

What are the strategy's implications in practice? For civil society groups, defining a common organizational vision is important (e.g., promoting free and open discourse on the Internet protected from government interference), but must be balanced with abundant flexibility so that individual members can best determine how to advance the vision. Applicable elements include the following:

- Recursive approaches that emphasize experimentation, learning, and iteration, removing the distinction between planning and implementation
- Flexible, horizontal structures that empower individuals to innovate as needed and as circumstances dictate
- Efficient actions undertaken without the benefit of substantial resources relative to a well-equipped opponent
- Leveraging peer-to-peer communications via social media and messaging apps, enabling new innovations to bubble up[41]

As it turns out, terrorist organizations like al-Qaeda and the Islamic State have been particularly successful in adopting these approaches. For example, Daveed Gartenstein-Ross and Madeleine Blackman describe how the Islamic State pioneered a "virtual planner model" to manage lone attackers:

> In this model, operatives who are part of ISIL's external operations division coordinate attacks online with supporters across the globe. Most of these supporters have never personally met the ISIL operatives they are conspiring with. Most of ISIL's prominent virtual planners appear to be based in the group's "caliphate" in Syria and Iraq, in large part due to proximity and access to ISIL's top leadership. But since the main equipment that virtual planners require is an Internet connection and good encryption, they could theoretically operate from other geographic locations. Being geographically dispersed carries greater risk of detection, but particularly as ISIL continues to decline as a territorial entity, the emergence of prominent virtual planners operating from outside the Syria-Iraq theater is likely.[42]

What made this plan so innovative is that the Islamic State had to use online techniques to overcome a major practical constraint: not being able to manage its operatives face to face. Not only did virtual planning solve the problem at hand, but iterations arguably made it more difficult for intelligence agencies to keep track of ISIL's movements and deter potential attacks. Thus, initial constraints can spur tactical iterations that may be more effective in the long run.

On a more positive note, Jawar's tactics in Ethiopia encapsulate how grassroots strategies deployed by civil society groups against government adversaries can

have a significant impact. Jawar admits that "I really didn't know anything. I just posted on Facebook. I said, what is going to happen to us?" He goes on, "It would be a lie for me to think that I knew [what to do] about that. . . . People started dropping ideas. I said, okay, that's good. You have to be creative about it." Jawar mentions how the government set up mass internment camps to break the protests: "They [Ethiopian authorities] would take 20,000 people from one part of Oromia and put them in one military camp. That is networking. I created this training manual where they train, where they share experiences. They spent two months and they get out, well networked! And after that they don't even need Internet. They can just call each other."[43] This situation provides a textbook application of recursion theory. Rather than fall victim to the government's mass imprisonment program, the protestors turned the tables on their captors. They leveraged the fact that so many of them were detained in the same place and used that situation to their advantage. They emerged from prison considerably stronger and more cohesive.

In 2019, Hong Kong protesters provided another illustration of how iterative tactics helped level the playing field against a much stronger opponent. A critical tool was their incorporation of social media and messaging applications to facilitate collective decision-making while retaining an anonymous leadership structure. One of the most useful apps was LIHKG, which is similar to the online forum Reddit. It allows users to post new threads with various calls to action; the most popular threads were then pushed to the top. As one demonstrator described the app to the *New York Times*, "People will give responses or click push to make that specific thread a hot one. We can predict what's going to happen by which posts are the hottest."[44] This process allowed protestors to quickly move from place to place without substantial advance planning. For supporters providing aid and supplies, LIHKG enabled them to accurately determine where protestors were amassing.

The messaging app Telegram has also proven indispensable to protest movements worldwide (in fact several media outlets have begun hyping the platform's effect as the "Telegram Revolution").[45] Several design details offer unique benefits: one feature allows users to delete messages or set them to self-destruct after a certain period of time (meaning that if security agents force protestors to unlock their phones, they won't reveal their friends). A second design advantage is the ability to form groups with large memberships—which can number in the hundreds of thousands. This has not only facilitated rapid amplification of information, but when integrated with built-in polls, it has provided an easy way to collectively decide whether a mass of protestors should confront oncoming police or disperse.[46] Finally, it is much harder for governments to selectively block Telegram without shutting down the Internet completely. As Belarusian authorities learned in 2020, they could stop users from accessing

Twitter, Instagram, WhatsApp, or Facebook, but they were unable to take Telegram offline as well. (Telegram founder Pavel Durov tweeted: "We enabled our anti-censorship tools in Belarus so that Telegram remained available for most users there. However, the connection is still very unstable as Internet is at times shut off completely in the country.")[47] A defining legacy of these protests is their showcasing of new tactics and adaptive strategies to fight back against powerful state apparatuses.

Private Sector Responsibilities

Whether they desire it or not, companies increasingly stand at the forefront of digital rights struggles. Even corporations that seemingly have little to do with tech find themselves embroiled in digital controversy. The National Basketball Association's (NBA) dispute in China in October 2019 highlights how tensions can quickly erupt when two incongruous political systems—one open and permissive, the other closed and controlled—collide with one another. It began with a simple tweet: Daryl Morey, the Houston Rockets' general manager, sent out a short message of support for the Hong Kong protestors, commenting, "Fight for freedom, stand with Hong Kong." In rapid succession, the Chinese consulate in Houston denounced Morey, as did the Rockets' team owner. Morey deleted the offending tweet, but the controversy spiraled. The Chinese Basketball Association announced it was dropping its partnership with the NBA. Morey apologized and the NBA released a statement describing the tweet as "regrettable." The Rockets even considered firing Morey to appease the Chinese. Then US politicians got involved and the backlash began. Senator Ted Cruz, Texas representative Beto O'Rourke, and former HUD secretary Julián Castro—among many others—lambasted the NBA for caving to the Chinese.[48] Cruz released a blistering tweet: "We're better than this; human rights shouldn't be for sale & the NBA shouldn't be assisting Chinese communist censorship."[49] After many months, the situation slowly eased. But the economic damage to the NBA was significant. Sources estimate that Morey's tweet cost the NBA between $150 and $200 million in lost revenue.[50]

The larger lesson from the NBA-China controversy is that companies can be poor vehicles to carry messages concerning human rights and democracy. As researchers Jason Miklian, John E. Katsos, and Benedicte Bull write, "Even when companies want to support global democracy and human rights, they find it much harder than anticipated and trap themselves in unenviable choices."[51] At the same time, it is impossible to disaggregate corporate services and products from culture and politics. The NBA is part of the American zeitgeist, which markets itself as a force for individualism and free expression. It can't simply

walk away from these values when the politics get too dicey. The takeaway from Miklian, Katsos, and Bull is that while companies "can't force social change upon recalcitrant regimes by themselves," if they focus on tangible goals and "act in parallel with governments that also support human rights and democracy," they're less likely to find themselves in hot water and their efforts will probably have greater effect.

A strong normative framework supported by a plurality of democracies can give cover to corporations to pursue policies responsive to democracy and human rights interests. This relationship applies widely, from social media platforms to firms that supply software or hardware used for surveillance. The more democracies set clear guidelines about acceptable corporate behavior, the better those standards are in providing a clear basis for companies to take difficult steps that may be incompatible with the political demands from nondemocratic states.

In general, companies inherently oriented to protect privacy or free expression face fewer complications. In the case of a company like Telegram, there can be strong alignment. Its messaging application is known for using very strong encryption and for protecting private communications no matter the content (it is used by protestors for democracy as well as by affiliates of the Islamic State and al-Qaeda). During the Hong Kong protests, Chinese authorities became increasingly frustrated by organizers' reliance on Telegram to coordinate demonstrations. In June 2019, the Chinese government launched a massive DDoS attack to disable the service.[52] Subsequently, concerns arose that Chinese and Hong Kong security forces might be exploiting a Telegram function that automatically matches usernames with phone numbers in a particular group. As Reuters reported, this would mean that authorities only needed to "request the owners of the phone numbers from the local telecom service in order to learn the users' true identities."[53] In response, Telegram changed its policies so that users can now "cloak" their phone numbers in order to prevent police monitoring. This situation clearly illustrates how a company that is primarily geared toward protecting user privacy is willing to take continuous proactive measures to thwart government actions.

But Telegram is an exception. Most companies have less clear-cut privacy or human rights interests. Facebook, for example, continually finds itself in hot water for making negligent if not reckless decisions enabling governments to propagate repressive content. A host of damaging revelations have emerged detailing how the company's leaders either ignored or failed to act against a variety of abuses. Sophie Zhang, a former data scientist at Facebook, detailed in a lengthy memo in September 2020 how the company deliberately overlooked mass harassment by Azerbaijan's ruling party against opposition parties, Covid-19 manipulation in Spain and later the United States, coordinated inauthentic

activity in Bolivia and Ecuador, and "inauthentic scripted activity" around Ukraine's 2019 elections.[54]

In such cases, it is critical for democratic governments to take strong regulatory positions. When corporations debate whether to adhere to local laws or conform to international human rights norms, the degree to which democratic governments are willing to hold companies accountable to concrete standards can tip the scales when it comes to how strenuously a company will incorporate human rights protections in its operations. Norwegian telecommunications firm Telenor is a useful example. While Norway enjoys some of the strongest privacy protections in the world, Telenor runs mobile service providers in countries with high levels of repression, such as Pakistan, Bangladesh, Myanmar, and Thailand. The company faces constant pressure from those governments, rooted in local laws, to provide communications data, enact content restrictions, allow lawful interceptions, or enact Internet shutdowns.[55] As one international telecom executive told me, it is risky for companies to push back against government requests, no matter how problematic: "Noncompliance to authority requests can lead to risks to personnel security, license revocations, or forced shutdowns. There are also other reasons why it is not always helpful to alienate the authorities and to push back too hard."[56] Unless there is equivalent pressure coming from democracies to conform to human rights laws, the balance often tilts in favor of repressive governments. It is simpler for companies to accede to Thailand's or Pakistan's content restriction demands than to risk their ire. Companies have few incentives to shift their policies without counterbalancing pressure from democracies.

Some companies may not explicitly intend to violate human rights principles but employ business models that are reliant on exploiting user privacy and data. Scholars such as Tim Wu, Shoshanna Zuboff, Zeynep Tufekci, Ron Deibert, David Kaye, Tarleton Gillespie, Siva Vaidhyanathan, and Peter Pomerantsev have laid out public critiques of US social media platforms that employ sophisticated algorithms that purposefully peddle extreme content in order to keep users glued to their feeds (and then monetize this captured attention through microtargeted ads).[57] In other words, companies have their own revenue-seeking agendas that directly or indirectly enable a massive disinformation ecosystem to flourish.

When it comes to the role of algorithms in advancing disinformation and hateful speech, most of the focus has been on content moderation—to what extent algorithms are able to identify and suppress posts that break community standards and cross the line when it comes to spreading bad or false information. But an equally important and more troubling use of algorithms by social media companies is "content shaping" algorithms. Companies use algorithms such as Facebook's news feed, Twitter's timeline, and YouTube's recommendation

engine to determine what users will see, what posts are queued up in their recommended viewing, and essentially which posts will "go viral."[58]

Thus, while many tech platforms argue that they are simply allowing users to say what they would like and are choosing not to interfere with their free speech rights, this is a mischaracterization. What platforms are really doing is quietly putting their fingers on the scale to determine which posts will be viewed and read by millions of individuals. At present, the overriding incentive that Facebook and other platforms follow is revenue and profit, even if the content in question spreads misinformation. In most cases, if the content increases user engagement, then the algorithm will bump up its visibility. Facebook's internal research reinforces this view. As the *Wall Street Journal* has reported, Facebook officials found that "64 percent of all extremist group joins are due to our recommendation tools" and that the majority came from Facebook's Groups You Should Join and Discover algorithms. They concluded that "our recommendation systems grow the problem."[59] It is not accurate for platforms to claim they are pursuing a hands-off policy regarding content; their algorithms are shaping what users see and react to.

While platforms have implemented some technical fixes in response to public outcries, these tend to be patchwork solutions whose effectiveness erodes over time. YouTube's "watch-next" algorithm is a good illustration. Of the more than one billion hours users spend watching videos on YouTube, its recommendations are responsible for 70 percent of watched content.[60] In January 2019, YouTube tweaked its algorithm to reduce its recommendations of conspiratorial videos. Initial reductions were significant—resulting in a 70 percent reduction in viewership of these clips. Eventually though, the proportion of conspiratorial recommendations crept up. As of February 2020, recommendations for such videos are now only 40 percent less common than when YouTube first announced its changes.[61] Without complementary policy shifts, engineering solutions on their own are unlikely to solve bad information problems and may bring diminishing effectiveness over time.

Because social media so profoundly affects political discourse and electoral outcomes, it follows that public officials should have more consistent input into policies that considerably impact the public domain.[62] As it stands, governments have delegated full responsibility for these decisions to private actors (who have a fiduciary duty to their shareholders). This is publicly irresponsible. As Pomerantsev asks in his book *This Is Not Propaganda*: "Could we even be empowered to take a stake in the decision-making process through which information all around us becomes shaped, with public input into the Internet companies who currently lord over how we perceive the world in darkness?"[63]

One proposal would be for regulators to mandate that companies provide a higher level of what David Kaye terms "decisional transparency"—disclosing

why they make certain content decisions and what are the decision-making factors behind content-shaping algorithms and ad-targeting systems that determine who can pay to influence these algorithms.[64] While most social media platforms publish semi-annual transparency reports that provide country-by-country aggregated data about government takedown requests and demands for user data, these reports provide minimal information about why companies deny or agree to certain requests, the basis for their decisions, how they apply platform rules (e.g., Facebook's "community standards"), and how users can appeal certain decisions.

Regulators could also require platforms to conduct more systematic human rights due diligence in order to understand the social impact of their algorithms and targeted advertising strategies. At present, many companies claim they are upholding human rights principles or "do no harm" approaches without providing specific evidence of such actions. Companies should come up with quantifiable methods for assessing the impact of their products. For certain political events in which there are known disinformation risks, such as elections, platforms could even consider time-bound bans against political ads or promoted political content (this could be similar to French media rules that prohibit election coverage forty-four hours prior to every presidential and legislative election). Regardless of what mix of approaches regulators decide to pursue, it will be an improvement over an existing system of self-regulation that is clearly broken.

Some experts, such as danah boyd, head of Data & Society, have floated transforming Facebook, YouTube, Twitter, and Instagram into public utilities.[65] A more pragmatic option would be to set up co-regulation systems such as public-private oversight councils to influence aspects of platforms' governance.[66] There are many forms this could take; Article 19 has released a detailed consultation paper laying out possible solutions.[67] One of the most vexing issues is balancing legitimate concerns with how social media companies currently moderate content with proposals that lean too far in the opposite direction—giving governments a larger say in determining permissible content and potentially opening the door to censorship. As these ideas develop, it is important to keep the following principles in mind:

- Ensure that any regulatory structure reflects international standards of freedom of expression.
- Train technologists and engineers on the human rights implications of their products and instruct on international best practices for preventing abuse.
- Promote decentralized decision-making to appropriately reflect local contexts, and give local civil society advocates and users direct roles in shaping company policies.

- Incorporate a multistakeholder approach.
- Obtain participation and support from public authorities, but ensure this does not threaten the independence of the regulatory body.
- Emphasize transparency principles and tie them to effective remedies for individual users.

While social media companies receive the majority of negative attention for abuses linked to their products, just as concerning are private sector surveillance companies, which sell software intended to penetrate private communications and compromise personal information. Industry representatives claim that their technology is designed for legitimate law enforcement purposes only—to extract information to counter terrorist activities or to combat illicit criminal conduct. In reality, their most loyal clients are a who's who of repressive regimes, from Saudi Arabia and the UAE to Venezuela and Pakistan. As UN special rapporteur David Kaye notes, "Companies appear to be operating without constraint. . . . The private surveillance industry is a free-for-all."[68] Unsurprisingly, transparency in this sector is nonexistent. Experts have obtained most of their understanding about how these firms operate from leaked documents or detailed forensics studies linked to their products.

A starting point would be for democratic governments to require surveillance companies to publish annual transparency reports that included the following information: what human rights due diligence standards were implemented for sales to prospective clients, whether the firm enacted end-use agreements for their products and steps taken to monitor compliance, and actions taken by the firm when human rights violations linked to their products were disclosed.[69] Democracies could also require companies to include technical safeguards such as shutoff or claw-back provisions when there are documented abuses, firewalling products to prevent unauthorized law enforcement or intelligence agency access, limiting the duration of data records that are kept, or integrating data anonymization in algorithms.

Confronting Chinese and Russian Exports of Digital Repression Technology

The fundamental challenge associated with Chinese and Russian exports of digital repression technology and services is that there is a booming demand in autocratic countries for these tools. As data in Chapter 3 revealed, autocratic countries possess lower digital capacity than their actual rates of enacting digital repression. The implications are that countries should either adopt lower-capacity

strategies to support their repressive agendas—such as implementing Internet shutdowns and locking up online users posting prohibited content—or they should seek to make up their capacity gaps through external suppliers. At present, companies based both in democracies and in autocracies provide powerful instruments to repressive regimes. In each of the case studies documented in this book, regimes in Thailand, the Philippines, and Ethiopia sourced from Chinese companies, but also from US, Israeli, and European firms. One way to constrain the technology spigot would be to put in place stricter controls for how companies in democracies do business. This would entail everything from instituting mandatory human rights due diligence requirements to drawing up blacklists of human rights-violating governments, which would be restricted from accessing certain capabilities (perhaps paralleling the spirit of the "Leahy Law," which prohibits arms sales to foreign security forces where there is credible information implicating a unit in gross violations of human rights).[70]

The problem with enacting restrictions on a broad array of digital technology is that because of the dual-use nature of this equipment, a policy intended to block surveillance or censorship could unintentionally harm unrelated parts of a country's economy. For example, a serious criticism of the Wassenaar Arrangement (in addition to its lack of enforcement capacity) is that it uses an overly broad definition of intrusion tools, thereby including legitimate programs such as endpoint security systems.[71] Moreover, a valid argument can be made that limiting the provision of US or European technology would simply open the door for greater market share by unscrupulous Chinese and Russian companies. Thus, a set of policies must do more than simply restrict US sales of equipment to bad regimes. It also needs to change the behavior of Chinese and Russian firms. How might democracies accomplish this task? Four strategies are worth considering.

First, it is possible to raise public awareness in specific countries about repressive uses of technology provided by Chinese or Russian firms. One way to increase public knowledge is to ramp up support for digital rights organizations, media outlets, and citizen activists to conduct investigations, highlight concerning issues, and spur national conversations about the negative impact of authoritarian-supplied technology. Another method is to leverage parliamentary oversight and investigations. Even in countries with highly centralized executives, legislatures have a limited ability to authorize independent investigations. To the extent that more and more parliaments decide to scrutinize how Chinese and Russian technology is being used in their countries, this will provide additional pressure. Citizens should also push their governments to provide heightened transparency regarding state use of Chinese and Russian technology, economic ties between the government and Chinese or Russian firms, and costs for specific digital projects (e.g., Uganda's government should be mandatorily required

to disclose the cost of its Huawei safe city project rather than have this come to light following journalist inquiries).

Second, democratic countries must compete more vigorously against Chinese state-backed firms for crucial technology projects, such as building 5G networks. These systems will provide the foundation for critical network infrastructure, giving the underlying manufacturer a huge advantage. While the United States recognizes the risk posed by Huawei or ZTE dominating next-generation production of these systems, it has not satisfactorily addressed the principal advantage that Huawei or ZTE offers—considerably lower cost. In my conversation with Secretary Eliseo Rio, who was in charge of the Philippines' ICT department at the time, he indicated that 80 percent of the country's equipment consists of Huawei products: "We bid it out [network overhaul] and Huawei won. The next bidder, Ericsson, cost nearly twice that. And the quality of Huawei is just as good."[72] It is by design that Chinese firms are able to outbid their rivals. Chinese financial institutions provide conditional loans to countries that restrict tech purchases to Chinese companies. Chinese corporations are likewise subsidized at a heavy rate by the CCP; by one estimate, more than 3 percent of China's annual output goes toward direct and indirect business subsidies.[73] This cash infusion gives Chinese firms significant advantages vis-à-vis foreign rivals. They can access discounted loans from state banks, obtain low-cost inputs (cheap land, electricity), and receive direct cash infusions from government investment funds. This strategy enables firms like Huawei, ZTE, Hikvision, and others to consistently underbid rivals for digital technology contracts—from installing 5G networks and establishing data centers to building smart cities.

While it is neither practical nor desirable for democracies to compete head-on with China on subsidies, there are intermediate steps that democratic governments could take to level the playing field for their companies. For instance, in relation to high priority technologies, the US government could establish a digital technology infrastructure fund that would provide financial resources in the form of matching grants or low-interest loans to make US corporate bids more price competitive. Such a fund would offer several enhancements over existing mechanisms: upgrade the amount of resources available to companies, focus specifically on digital technology projects and reprioritize evaluation criteria so that strategic considerations become more important factors for determining whether financing is provided, and streamline lengthy administrative processes that US companies currently must undergo to obtain support.

Third, in addition to applying country-level strategies to counteract Chinese and Russian tech encroachment, democracies should continue to invest in building international norms and establishing standards that reflect democratic models of digital governance. Chinese and Russian delegations are making an all-out push to promote a cyber sovereignty vision of Internet governance that

entitles governments to determine their own Internet regulations and standards, even if these directives contravene international law.[74] The censorship and surveillance implications are ominous. Thus, it behooves policymakers in the United States and Europe to actively push back against such efforts. This not only means blocking worrisome proposals from Chinese and Russian delegations, but also offering a compelling, democratic vision of digital governance, and a common language for setting policy, that will protect security while advancing human rights and political freedoms.

AI systems illustrate how pursuing a human rights-oriented approach in a nascent field can significantly improve outcomes. How online platforms use automated techniques, the role AI plays in displaying or moderating content, the degree to which companies access personal data to inform and refine algorithms, and to what extent racial and gender discrimination affects AI systems' inputs and outputs are outstanding questions. Individuals such as David Kaye, and groups such as Global Partners Digital, advocate for making human rights a central consideration when assessing AI impact.[75] For obvious reasons, such an approach would be anathema to Chinese or Russian interests. But this represents an opportunity for democracies to shape a fledgling technology and advance common principles to mitigate risks to human rights from AI systems, incentivize rights-respecting practice in public institutions and private entities, and incorporate grievance and remediation procedures for potential violations.

Fourth, export restrictions can be effective instruments when deployed sparingly and in a precise and consistent manner. In general, instituting blanket export controls linked to Chinese technology companies is not prudent either for the United States or other democracies. The economic consequences are damaging and there are real questions about whether such actions are actually effective. But that doesn't mean that Chinese companies directly linked to repressive activities shouldn't face penalties. This is why the US government's inclusion of twenty-eight Chinese companies on its Entity List for human rights violations committed in Xinjiang is symbolically important (even if imperfectly implemented). The United States and other like-minded democracies should seek concrete ways to build on such efforts. For example, the extent to which democracies act in concert when implementing these restrictions (e.g., coordinating US Entity List inclusions with parallel EU restrictions) leads to a better prospect of changing egregious Chinese behavior. In addition, democracies should consider imposing targeted penalties, such as visa bans or financial sanctions, on individuals responsible for carrying out digital repression activities (in the waning days of the Trump administration, the US government imposed sanctions on a slate of Chinese officials responsible for carrying out human rights violations in Xinjiang, as well as against Chinese officials authorizing the Hong Kong crackdown).[76] The United States already has an applicable law on

the books, the Global Magnitsky Act, that is an appropriate vehicle for such sanctions. There is no reason the United States could not expand the law's use to include perpetrators of serious forms of digital repression. Democracies could also consider investment legislation that would restrict the provision of financing to Chinese or Russian technology companies that are building documented tools for repression. Finally, democratic governments should also scrutinize the conduct of their own companies. In the United States, for example, firms such as Sandvine, Thermo Fisher, and even Intel and Nvidia, have provided advanced technology to authoritarian governments to accomplish surveillance and censorship objectives.[77] Lawmakers would be wise to scrutinize the existing rules and determine how to tighten the export of intrusive US technology to repressive regimes.

Covid-19 Implications of Digital Technology

The Covid-19 pandemic has caused governments around the world to turn to digital tools to fight its spread. [78] While there are legitimate epidemiological reasons for states to deploy contact-tracing apps or use location-monitoring technology to track viral outbreaks, there are increasing reports of privacy violations and human rights abuses.[79] As governments deploy new tools in enlarged numbers, there has not been a corresponding debate to define protections, safeguards, and standards of use. Even more troubling, many governments have refused to set limits regarding how long they intend to use these tools. It is conceivable that for countries like Russia, China, Singapore, or Turkey, enhanced surveillance is here to stay.

This problem is not limited to autocratic governments; certain democracies have also embraced mass surveillance measures.[80] At least in democracies, there is some comfort that emergency measures will comply with basic human rights guarantees and include rudimentary safeguards to protect citizen data from public exposure and illegitimate use. But blanket authorizations of emergency powers taken in times of crisis can persist over time and lead to permanent erosions of political freedoms (as evidenced by the sharp curtailments of civil liberties in the United States after the 9/11 attacks, or elevated securitization measures imposed in Europe in response to Islamic State suicide attacks between 2014 and 2017). As the pandemic continues to rage, four emerging patterns are relevant.

First, the coronavirus has accelerated existing methods of repression. Governments already prone to using digital surveillance and censorship or peddling disinformation—such as China, Saudi Arabia, Turkey, and Thailand—have precipitously moved ahead to deploy facial recognition surveillance,

contact-tracing apps, and social media monitoring, along with information controls.[81] However, there appears to be a gap between a broader array of countries carrying out general democratic violations linked to the pandemic (e.g., constraints on media freedom, legislative restrictions, abusive security enforcement), and a narrower set of countries specifically using digital repression tactics in response to Covid-19.

Second, states have become central in gathering and providing information. As analysts Nathan Brown, Intissar Fakir, and Yasmine Farouk write, "Technology may facilitate daily lives under lockdown, but it also aids in the official control of information."[82] The enduring implications of this shift are yet unclear, but they present flashing warning signs for citizens living in autocracies.

Third, arrests for violations of "fake news" laws linked to the pandemic are on the rise along with a corresponding increase in official disinformation on Covid-19. Governments are persecuting scores of individuals for spreading fake news about the coronavirus in countries such as Myanmar, Cambodia, Kenya, Uganda, China, and Morocco. Targets for arrest are often civil society activists and political opposition figures.[83] At the same time, many governments have ramped up their own disinformation efforts. The V-Dem project identifies 25 countries that have propagated government disinformation on Covid-19 along the following lines: *denialist* (authorities discredit or reject reports of Covid-19 outbreaks in their territories), *anti-science* (officials downplay Covid-19 dangers while disputing accepted medical recommendations), and *curist* (leaders promote unfounded treatments for the virus).[84]

Fourth, governments are implementing new surveillance techniques in a rushed and ad hoc manner. States have not yet established clear rules of the road regarding safeguards, data privacy protections, or remediations for abuse, even while launching intrusive health-monitoring applications. For example, Amnesty International revealed that contact-tracing apps launched by Bahrain, Kuwait, and Norway contained serious privacy and security risks for users. All three apps employ "live or near-live tracking of users' locations" through recurrent uploading of GPS data to a centralized server, signifying that state authorities can track an individual's movements at all times.[85] Norway subsequently retracted the app after Amnesty International published its report. Authorities in Bahrain and Kuwait continue to deploy their contact-tracing apps.

Concluding Thoughts

When it comes to the impact of digital technology on governance and repression, I am neither a techno-optimist nor a techno-pessimist. I do not believe there is anything inherently good or bad about the political impact wrought by

technology. I remain inspired by spontaneous grassroots efforts that against all odds have deposed dictators in places like Tunisia, Sudan, and Burkina Faso. I have also been dismayed by the sinister effects of omniscient surveillance deployed in Xinjiang, state-sponsored hacking used by Saudi Arabia and the UAE to target independent journalists, and sophisticated disinformation campaigns in the Philippines and Russia. I foresee an unremitting struggle between specific regimes that will find clever ways to exploit technology to enhance their political control, and other places where digitally savvy civic activists will deploy innovative tactics to circumvent authoritarian governments, break the state's monopoly on information, and mobilize protests.

I am most concerned about the repressive impact of technology in contexts where the state already exercises an inordinate degree of control over people's daily lives—such as in China or Russia. There are few checks to limit how the Chinese state deploys increasingly intrusive technology and there are vast incentives for the CCP to invest heavily in surveillance and censorship methods. It has sufficient resources and capacity to sustain digital systems of control for the foreseeable future. Similarly, in Russia, a predatory regime distrustful of the broader public and possessing sufficient resources to maintain an elaborate monitoring and tracking apparatus doesn't auger well for Russians' future political freedoms—even when Putin departs from the scene.

I am also worried about contested states and illiberal regimes undergoing autocratization, where savvy leaders are using digital technology to enhance their political agendas and solidify control of formerly democratic systems. The Philippines, India, Hungary, and Sri Lanka, to name a few, all evince signs of serious political deterioration. While technology has not been the main impetus for democratic backsliding, it nonetheless plays an important role in assisting the rapid dismantlement of political rights. The Covid-19 epidemic adds another unexpected twist to digital repression trends. In the spirit of never letting a good crisis go to waste, many autocratic leaders (or autocratically inclined leaders) are shamelessly exploiting the pandemic. It just so happens that some of the most effective ways to combat the spread of the virus are through the deployment of digital surveillance technology that has the secondary effect of allowing governments to closely track their citizens' movements and communications. While I don't believe that the coronavirus's impact on repression will be politically transformative, the pandemic may considerably accelerate repressive trends by providing a suitable rationale for leaders to authorize new powers for the organs of the state.

I believe liberal democracies have faltered the most when it comes to delivering a compelling vision for how to balance innovative uses of technology while ensuring appropriate protections. In this respect, the United States has been particularly neglectful. The government has turned a blind

eye while many Silicon Valley behemoths have violated public trust, run roughshod over privacy standards, and monetized personal data for commercial exploitation. Internationally, the United States continues to trot out repeated lines about supporting a free and open Internet. Meanwhile, it takes few steps to confront the viral dissemination of disinformation or to address the spread of polarized information polluted by extremist and conspiratorial narratives. The government's failure to adopt basic regulatory approaches to promote a healthy online ecosystem is a disservice to principles of free expression. Free speech does not mean that those who shout the loudest and spout the most polarizing rhetoric are the only ones who should be heard.

For democracies, solving the digital repression puzzle begins at home. Liberal democratic governments are obligated to ensure that privacy is safeguarded from corporate surveillance interests as well as from state intrusion. Freedom of speech must be protected, not only from prior constraints linked to the state, but also from disinformation agents who are weaponizing discourse to promote their agendas. And finally, economic competition must be reinvigorated through strengthened antitrust enforcement that allows new innovations to flourish and prevents oligopolistic accumulations of power by a small group of powerful companies.

Can we turn this state of affairs around?

In my conversation with *Rappler* head Maria Ressa, I asked her what steps democracies need to take to push back against the digital repression challenge. She responded, "Think about what happened post–World War II. There was Bretton Woods. There was NATO. There was the UN Declaration of Human Rights. These are the kinds of things we need now." She concluded, "Is this a fantasy?"[86]

Whatever the mechanism, the crucial question is this: Can democracies empower civic activists to reverse global digital repression trends while summoning requisite political will to undertake painfully needed reforms at home?

I believe this is a struggle and a story that is far from finished. Technology doesn't stand still. It exists in a constant state of iteration and advancement. This means that while digital technology has fueled a shift toward autocratization, I am certain that circumstances will change many times over in the future.

Notes

1. Portions of this chapter derive from previously published material by the author, including Steven Feldstein, "Testimony—Hearing on China's Strategic Aims in Africa," US-China Economic and Security Review Commission, May 8, 2020, https://www.uscc.gov/hearings/chinas-strategic-aims-africa; Feldstein, "Beware the Implications."

2. A good illustration of their enhanced organizing power is reflected in the numerous digital rights conferences and convenings that occur throughout the year, such as RightsCon (sponsored by Access Now) and the Internet Freedom Festival.
3. Laura Silver, "Smartphone Ownership Is Growing Rapidly around the World, but Not Always Equally," Pew Research Center, February 5, 2019, https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/.
4. See, for example, "Campaign to Free Ethiopia's Zone9 Bloggers," GlobalVoices Advox, 2020, https://advox.globalvoices.org/campaigns-research/behind-bars-in-ethiopia-campaign-to-free-the-zone9-bloggers/.
5. Janjira Sombatpoonsiri, "Growing Cyber Activism in Thailand," Carnegie Endowment for International Peace, 2017, https://carnegieendowment.org/2017/08/14/growing-cyber-activism-in-thailand-pub-72804.
6. Dusan Stojanovic, "Chinese Snooping Tech Spreads to Nations Vulnerable to Abuse," *AP News*, October 17, 2019, https://apnews.com/9fd1c38594444d44acfe25ef5f7d6ba0.
7. Stojanovic, "Chinese Snooping Tech Spreads."
8. "Serbia: Unlawful Facial Recognition Video Surveillance in Belgrade," SHARE Foundation, December 4, 2019, https://edri.org/serbia-unlawful-facial-recognition-video-surveillance-in-belgrade/.
9. Biryabarema, "Uganda's Cash-Strapped Cops."
10. Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *Wall Street Journal*, August 15, 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.
11. Parkinson, Bariyo, and Chin, "Huawei Technicians."
12. Alexandra Stevenson, "Soldiers in Facebook's War on Fake News Are Feeling Overrun," *New York Times*, October 9, 2019, https://www.nytimes.com/2018/10/09/business/facebook-philippines-rappler-fake-news.html.
13. "Removing Coordinated Inauthentic Behavior from the Philippines," Facebook, March 28, 2019, https://about.fb.com/news/2019/03/cib-from-the-philippines/.
14. Kurt Wagner, "Facebook, Twitter, YouTube Remove Posts from Bolsonaro," *Bloomberg*, March 30, 2020, https://www.bloomberg.com/news/articles/2020-03-31/facebook-twitter-pull-misleading-posts-from-brazil-s-bolsonaro.
15. Josh Constine, "Facebook, Twitter, YouTube Remove Posts from Bolsonaro," *Techcrunch*, March 30, 2020, https://techcrunch.com/2020/03/30/facebook-removes-bolsonaro-video/.
16. Abby Ohlheiser, "Twitter Fact-Checks a Misleading Trump Tweet for the First Time," *MIT Technology Review*, May 26, 2020, https://www.technologyreview.com/2020/05/26/1002274/twitter-fact-checks-trump-mail-in-voting-tweet/.
17. James Pearson, "Exclusive: Facebook Agreed to Censor Posts after Vietnam Slowed Traffic—Sources," *Reuters*, April 21, 2020, https://www.reuters.com/article/us-vietnam-facebook-exclusive/exclusive-facebook-agreed-to-censor-posts-after-vietnam-slowed-traffic-sources-idUSKCN2232JX.
18. Ryan Gallagher, "U.S. Company Faces Backlash after Belarus Uses Its Tech to Block Internet," *Bloomberg*, September 11, 2020, https://www.bloomberg.com/news/articles/2020-09-11/sandvine-use-to-block-belarus-internet-rankles-staff-lawmakers?sref=QmOxnLFz.
19. Ryan Gallagher, "Francisco-Backed Sandvine Nixes Belarus Deal, Citing Abuses," *Bloomberg*, September 15, 2020, https://www.bloomberg.com/news/articles/2020-09-15/sandvine-says-it-will-no-longer-sell-its-products-in-belarus?sref=QmOxnLFz. Digital rights groups also initiated a pressure campaign against cybersecurity outfit NSO Group to limit the spread of its hacking tools that were used by repressive governments to target journalists, civil society activists, and political opponents. They have pursued a multipronged approach that includes publicly urging NSO Group's new private equity owner, London-based Novalpina Capital, to clamp down on abuses associated with NSO Group's products. Activists have also coordinated with WhatsApp to sue NSO Group in US federal court for harms linked to its hacking tools. Whether these actions will ultimately change NSO Group's behavior remains

to be seen, but at a minimum the company faces heightened public scrutiny, limiting its present and future client base. Sean Lyngaas, "Rights Groups Probe Investments in NSO Group's Private Equity Firm," *Cyberscoop*, May 29, 2019, https://www.cyberscoop.com/nso-group-novalpina-capital-pension-groups-investment/; Erik Manukyan, "Summary: WhatsApp Suit against NSO Group," *Lawfare*, November 7, 2019, https://www.lawfareblog.com/summary-whatsapp-suit-against-nso-group.

20. "Sudan Crisis: Internet Restored—but Only for Lawyer," *BBC*, June 24, 2019, https://www.bbc.com/news/world-africa-48744853.
21. "Judges Raise the Gavel to #KeepItOn around the World," Access Now, September 23, 2019, https://www.accessnow.org/judges-raise-the-gavel-to-keepiton-around-the-world/.
22. Angela Chen, "Limiting Message Forwarding on WhatsApp Helped Slow Disinformation," *MIT Technology Review*, September 26, 2019, https://www.technologyreview.com/2019/09/26/434/whatsapp-disinformation-message-forwarding-politics-technology-brazil-india-election/.
23. Casey Newton, "WhatsApp Puts New Limits on the Forwarding of Viral Messages," *The Verge*, April 7, 2020, https://www.theverge.com/2020/4/7/21211371/whatsapp-message-forwarding-limits-misinformation-coronavirus-india.
24. Author interview with a tech company official, April 27, 2020.
25. See Feldstein, "Can a U.N. Report Help Rein in Surveillance."
26. Garrett Hinck, "Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research," *Lawfare*, January 5, 2018, https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research.
27. Kaye, "Report of the Special Rapporteur."
28. "Addition of Certain Entities to the Entity List," U.S. Federal Register, October 9, 2019, https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list.
29. Will Knight, "MIT Cuts Ties with a Chinese AI Firm amid Human Rights Concerns," *Wired*, April 21, 2020, https://www.wired.com/story/mit-cuts-ties-chinese-ai-firm-human-rights/.
30. William A. Carter and William Crumpler, "Understanding the Entities Listing in the Context of U.S.-China AI Competition," CSIS, October 15, 2019, https://www.csis.org/analysis/understanding-entities-listing-context-us-china-ai-competition.
31. Similarly, in November 2020, the EU agreed to new export rules that governing the granting of licenses. It adds new controls for cyber surveillance tools and other dual use products contributing to human rights violations. "Dual use goods: Parliament and EU ministers agree on new EU export rules," European Parliament—News, November 9, 2020, https://www.europarl.europa.eu/news/en/press-room/20201105IPR90915/dual-use-goods-parliament-and-eu-ministers-agree-on-new-eu-export-rules.
32. Lotus Ruan et al., "One App, Two Systems: How WeChat Uses One Censorship Policy in China and Another Internationally," Citizen Lab, November 30, 2016, https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems/.
33. Higgins was cited in a Human Rights Watch report on chemical weapons attacks in Ghouta, Syria, which helped establish government culpability. See "Attacks on Ghouta: Analysis of Alleged Use of Chemical Weapons in Syria," Human Rights Watch, September 10, 2013, https://www.hrw.org/report/2013/09/10/attacks-ghouta/analysis-alleged-use-chemical-weapons-syria.
34. "Brown Moses Announces Bellingcat—Open Source Investigations for All," Brown Moses (blog), July 1, 2014, https://brown-moses.blogspot.com/2014/07/brown-moses-announces-bellingcat-open.html.
35. Muhammad Idrees Ahmad, "Bellingcat and How Open Source Reinvented Investigative Journalism," *New York Review of Books*, June 10, 2019, https://www.nybooks.com/daily/2019/06/10/bellingcat-and-how-open-source-reinvented-investigative-journalism/.
36. Some efforts predate Bellingcat, such as the site 38 North (https://www.38north.org/), which provides analysis using street-level and satellite imagery of North Korea.
37. Ahmad, "Bellingcat."
38. Ned Beauman, "How to Conduct an Open-Source Investigation, According to the Founder of Bellingcat," *New Yorker*, August 30, 2018, https://www.newyorker.com/culture/culture-desk/how-to-conduct-an-open-source-investigation-according-to-the-founder-of-bellingcat.

39. See, for example, Charlotte Godart, "COVID-19: Monitoring the Global Slowdown," Bellingcat, April 10, 2020, https://www.bellingcat.com/news/2020/04/10/covid-19-monitoring-the-global-slowdown/; Natalia Antonova, "Investigating Coronavirus Fakes and Disinfo? Here Are Some Tools for You," Bellingcat, March 27, 2020, https://www.bellingcat.com/resources/2020/03/27/investigating-coronavirus-fakes-and-disinfo-here-are-some-tools-for-you/.
40. Ionut C. Popescu, "Grand Strategy vs. Emergent Strategy in the Conduct of Foreign Policy," *Journal of Strategic Studies* 41, no. 3 (2018): 446.
41. The Boston Consulting Group (BCG) has invested considerable resources in developing an in-depth curriculum focused on enhancing adaptive strategies for organizations. It defines three "R's" that are essential for surviving in an unpredictable environment: readiness (anticipating relevant trends affecting the organization), responsiveness (agilely confronting challenges as they arise), and resilience (ability to withstand obstacles and maintain organization cohesion). But BCG emphasizes that a fourth "R"—recursion—is perhaps the most important element. Recursion emphasizes experimentation, learning, iteration, and "modulation based on experience." It removes the distinction between planning and implementation, "since successful strategies emerge from practice rather than from analysis and design." Martin Reeves et al., "Adaptive Advantage," BCG, January 20, 2010, https://www.bcg.com/publications/2010/strategy-business-unit-adaptive-advantage.aspx.
42. Daveed Gartenstein-Ross and Madeleine Blackman, "ISIL's Virtual Planners: A Critical Terrorist Innovation," *War on the Rocks*, January 4, 2017, https://warontherocks.com/2017/01/isils-virtual-planners-a-critical-terrorist-innovation/.
43. Gartenstein-Ross and Blackman, "ISIL's Virtual Planners."
44. K. K. Rebecca Lai and Jin Wu, "Protesters in Hong Kong Have Changed Their Playbook. Here's How," *New York Times*, July 4, 2019, https://www.nytimes.com/interactive/2019/06/28/world/asia/hong-kong-protests.html.
45. Daria Litvinova, "'Telegram Revolution': App Helps Drive Belarus Protests," *AP*, August 21, 2020, https://apnews.com/823180da2b402f6a1dc9fbd76a6f476b.
46. Maciej Ceglowski, "Observations on Technology Use in Hong Kong Protests," remarks on the situation in Hong Kong at the Stanford Internet Observatory E2E Encryption Workshop, September 12, 2019, https://idlewords.com/talks/hk_stanford.html.
47. Pavel Durov, Twitter post, August 10, 2020, https://twitter.com/durov/status/1292912756233048064.
48. Matthew Yglesias, "The Raging Controversy over the NBA, China, and the Hong Kong Protests, Explained," *Vox*, October 7, 2019, https://www.vox.com/2019/10/7/20902700/daryl-morey-tweet-china-nba-hong-kong.
49. Ted Cruz, "tweet message," October 6, 2019, 8:16 p.m., https://twitter.com/tedcruz/status/1181030466247417861?lang=en.
50. Adrian Wojnarowski and Bobby Marks, "Sources: NBA Set to Release Revised 2020–21 Salary and Luxury Tax Projections," *ESPN*, January 29, 2020, https://www.espn.com/nba/story/_/id/28596920/sources-nba-set-release-revised-2020-21-salary-luxury-tax-projections.
51. Jason Miklian, John E. Katsos, and Benedicte Bull, "China's Conflict with the NBA Shows Why Companies Can't Force Social Change by Themselves," *Washington Post*, October 13, 2019, https://www.washingtonpost.com/politics/2019/10/13/chinas-conflict-with-nba-shows-why-companies-cant-force-social-change-by-themselves/.
52. Pavel Durvo, "tweet message," June 12, 2019, 4:54 p.m., https://twitter.com/durov/status/1138942773430804480.
53. Joel Schectman, "Exclusive: Messaging App Telegram Moves to Protect Identity of Hong Kong Protesters," *Reuters*, August 30, 2019, https://www.reuters.com/article/us-hongkong-telegram-exclusive/exclusive-messaging-app-telegram-moves-to-protect-identity-of-hong-kong-protesters-idUSKCN1VK2NI.
54. Craig Silverman, Ryan Mac, and Pranav Dixit, "'I Have Blood on My Hands;: A Whistleblower Says Facebook Ignored Global Political Manipulation," *Buzzfeed News*, September 14, 2020, https://www.buzzfeednews.com/article/craigsilverman/facebook-ignore-political-manipulation-whistleblower-memo.
55. See "Authority Requests Disclosure Report," Telenor Group, 2018, https://www.telenor.com/wp-content/uploads/2019/03/Telenor-Authority-request-report-2018.pdf.

56. Author interview with an international telecommunications official, July 9, 2019.
57. See for example, Tim Wu, *The Attention Merchants: The Epic Scramble to Get Inside Our Heads* (New York: Vintage Books, 2016); Ronald J. Deibert, "The Road to Digital Unfreedom: Three Painful Truths about Social Media," *Journal of Democracy* 30, no. 1 (2019): 25–39; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Profile Books, 2019); Kaye, *Speech Police*; Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (New Haven, CT: Yale University Press, 2018); Zeynep Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest* (New Haven, CT: Yale University Press, 2017); Vaidhyanathan, *Antisocial Media*; Pomerantsev, *This Is Not Propaganda*.
58. Nathalie Maréchal and Ellery Roberts Biddle, "It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge," New America—Ranking Digital Rights, March 17, 2020, https://www.newamerica.org/oti/reports/its-not-just-content-its-business-model/.
59. Jeff Horwitz and Deepa Seetharaman, "Facebook Executives Shut Down Efforts to Make the Site Less Divisive," *Wall Street Journal*, May 26, 2020, https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499?campaign_id=158.
60. Charlotte Jee, "YouTube Has Nearly Halved the Number of Conspiracy Theory Videos It Recommends," *MIT Technology Review*, March 3, 2020, https://www.technologyreview.com/2020/03/03/905565/youtube-halved-conspiracy-theory-videos-recommends/. There is some debate about the extent to which algorithms drive viewing patterns. A November 2020 study of YouTube concluded that recommendation algorithms led "only a fraction" of users to view far-right videos. Instead, most views originated from cross-platform traffic. The researchers also found consecutive sessions of video viewership showed no greater trend towards larger consumption of extreme content (a further indication about the dampened impact of recommendation algorithms). It is worth noting that this is a single study—yet to be peer reviewed—analyzing one particular type of content (extreme rightwing videos on YouTube), but it does reveal basic limitations to our current understanding about the dissemination of disinformation. Homa Hosseinmardi, Amir Ghasemian, Aaron Clauset, David M. Rothschild, Markus Mobius, and Duncan J. Watts, "Evaluating the scale, growth, and origins of right-wing echo chambers on YouTube," *arXiv preprint arXiv:2011.12843* (2020).
61. Marc Faddoul, Guillaume Chaslot, and Hany Farid, "A Longitudinal Analysis of YouTube's Promotion of Conspiracy Videos," *arXiv* preprint arXiv:2003.03318 (2020).
62. One thorny issue to guard against would be the removal of intermediate liability protection for social media companies. In the United States, Section 230 of the 1996 Communications Decency Act protects companies from responsibility for content posted by users. While there is growing public frustration with pervasive levels of misinformation and disinformation, removing the liability shield would likely have the perverse effect of increasing corporate surveillance to ensure user content conforms to legal requirements, and potentially instigating overcompliance (and de facto censorship) as platforms take down any speech that would expose them to liability. At the same time, the current system has left platforms unaccountable for egregious content and communications. An alternative could be for policymakers to consider adopting a "quid pro quo benefit." In exchange for being shielded from liability, platforms would be compelled to fulfill certain public interest obligations related to transparency, accountability, or ensuring their algorithms do not skew toward extreme or violent content. See Guy Rolnik et al., "Protecting Journalism in the Age of Digital Platforms," George J. Stigler Center for the Study of the Economy and the State, University of Chicago Booth School of Business, July 1, 2019, https://research.chicagobooth.edu/-/media/research/stigler/pdfs/media---report.pdf; Steven Feldstein, "How to tackle Europe's digital democracy challenges," Carnegie Endowment for International Peace, October 15, 2020, https://carnegieendowment.org/2020/10/15/how-to-tackle-europe-s-digital-democracy-challenges-pub-82960.
63. Pomerantsev, *This Is Not Propaganda*, 187.
64. Kaye, *Speech Police*, 121–22.

65. See danah boyd, "Facebook Is a Utility; Utilities Get Regulated," *Apophenia*, May 15, 2010, https://www.zephoria.org/thoughts/archives/2010/05/15/facebook-is-a-utility-utilities-get-regulated.html.
66. Facebook has taken fledgling steps in this regard. In November 2018, responding to numerous scandals regarding its content moderation practices, Zuckerberg announced the creation of an independent oversight board that would make binding decisions about whether to restore removed content and would explain its reasons for doing so. While this is a positive step, it leaves many concerns unaddressed. For one, the number of cases taken up by the body, which has been compared to a "supreme court" for content moderation, will be minuscule. More importantly, key parts of its operations will not be eligible for review. This includes " content posted through marketplace, fundraisers, Facebook dating, messages, and spam" or pertaining to services such as WhatsApp, Facebook Messenger, or Instagram. It is also unclear whether the board's decisions will have precedential effect and generate structural changes—such as modifying algorithmic content filtering. Finally, the board isn't mandated to address the proliferation of social manipulation and disinformation occurring on the platform. See "A Blueprint for Content Governance and Enforcement," Facebook, November 15, 2018, https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/?hc_location=ufi.
67. "The Social Media Councils: Consultation Paper," Article 19, June 2019, https://www.article19.org/wp-content/uploads/2019/06/A19-SMC-Consultation-paper-2019-v05.pdf.
68. "UN Expert Calls for Immediate Moratorium on the Sale, Transfer and Use of Surveillance Tools," United Nations Office of the High Commissioner on Human Rights, June 25, 2019, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736.
69. For a more detailed list of potential questions surveillance firms should be obligated to disclose, see https://www.accessnow.org/open-letter-to-novalpina-capital/.
70. "Leahy Law Fact Sheet," US Department of State, January 22, 2019, https://www.state.gov/key-topics-bureau-of-democracy-human-rights-and-labor/human-rights/leahy-law-fact-sheet/.
71. Hinck, "Wassenaar Export Controls."
72. Eliseo Rio (acting secretary, Department of Information and Communications Technology), interview with the author, May 21, 2019.
73. David J. Lynch, "Initial U.S.-China Trade Deal Has Major Hole: Beijing's Massive Business Subsidies," *Washington Post*, December 31, 2019, https://www.washingtonpost.com/business/economy/initial-us-china-trade-deal-has-major-hole-beijings-massive-business-subsidies/2019/12/30/f4de4d14-22a3-11ea-86f3-3b5019d451db_story.html.
74. Many experts contend that China is leveraging forums like the International Telecommunication Union (ITU), a specialized agency of the United Nations, to push an alternative digital vision. At an ITU meeting in September 2019, for example, a large Chinese delegation that included Huawei representatives proposed establishing a "New IP" (Internet protocol) to replace the existing version. New IP would feature a "top-to-bottom design" and would potentially permit Internet service providers, many of which are state-owned, to have "control and oversight of every device connected to the network and be able to monitor and gate individual access." Madhumita Murgia and Anna Gross, "Inside China's Controversial Mission to Reinvent the Internet," *Financial Times*, March 27, 2020, https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f; Hascall Sharp, "Discussion Paper: An Analysis of the 'New IP' Proposal to the ITU-T," Internet Society, April 24, 2020, https://www.Internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/.
75. David Kaye, "Report of the Special Rapporteur to the General Assembly on AI and Its Impact on Freedom of Opinion and Expression," UN A/73/348, August 29, 2018, https://undocs.org/A/73/348. See also Charles Bradley, Richard Wingfield, and Megan Metzger, "National Artificial Intelligence Strategies and Human Rights: A Review," Global Partners Digital, April 2020, https://www.gp-digital.org/wp-content/uploads/2020/04/National-Artifical-Intelligence-Strategies-and-Human-Rights%E2%80%94A-Review_April2020.pdf.
76. Demetri Sevastopulo and Christian Shepherd, "US sanctions top Chinese officials over Xinjiang detentions," *Financial Times*, July 10, 2020, https://www.ft.com/content/

c7c70bb0-00df-4a23-9126-d44ac4c99f02; Austin Ramzy and Tiffany May, "U.S. Imposes Sanctions on Chinese Officials Over Hong Kong Crackdown," *New York Times*, December 16, 2020, https://www.nytimes.com/2020/12/08/world/asia/hong-kong-china-us-sanctions.html.

77. Paul Mozur and Don Clark, "China's Surveillance State Sucks Up Data. U.S. Tech Is Key to Sorting It," *New York Times*, November 24, 2020, https://www.nytimes.com/2020/11/22/technology/china-intel-nvidia-xinjiang.html.
78. See Steven Feldstein, "What Democracy Will Fall Next?," *Foreign Policy*, May 7, 2020, https://foreignpolicy.com/2020/05/07/democracy-pandemic-coronavirus-hungary-populism/.
79. Several researchers and rights groups have compiled useful trackers to provide a global snapshot of digital measures countries are taking in response to COVID-19. See, for example, Woodhams, "COVID-19 Digital Rights Tracker"; "Tracking the Global Response to COVID-19," Privacy International, April 26, 2020, https://www.privacyinternational.org/examples/tracking-global-response-covid-19.
80. Joshua Mitnick, "Better Health through Mass Surveillance," *Foreign Policy*, March 16, 2020, https://foreignpolicy.com/2020/03/16/israel-coronavirus-mass-surveillance-pandemic/.
81. Kareem Fahim, Min Joo Kim, and Steve Hendrix, "Cellphone Monitoring Is Spreading with the Coronavirus. So Is an Uneasy Tolerance of Surveillance," *Washington Post*, May 2, 2020, https://www.washingtonpost.com/world/cellphone-monitoring-is-spreading-with-the-coronavirus-so-is-an-uneasy-tolerance-of-surveillance/2020/05/02/56f14466-7b55-11ea-a311-adb1344719a9_story.html.
82. Nathan J. Brown, Intissar Fakir, and Yasmine Farouk, "Here to Stay?" Carnegie Endowment for International Peace, *Diwan*, April 22, 2020, https://carnegie-mec.org/diwan/81611.
83. In Niger, for example, authorities arrested prominent journalist Kaka Touda for his reporting on the virus. His arrest stemmed from a complaint from the General Reference Hospital alleging that Touda's posts about a potential coronavirus case was a threat to public order. Authorities have charged Touda under Niger's 2019 cybercrime law.

    "Journalist Kaka Touda Mamane Goni Arrested in Niger over COVID-19 Report," Committee to Protect Journalists, March 24, 2020, https://cpj.org/2020/03/journalist-kaka-touda-mamane-goni-arrested-in-nige.php.
84. Anna Lührmann, Jean Lachapelle, Sandra Grahn, and Amanda B. Edgell, "Pandemic Backsliding: Democracy and Disinformation Seven Months into the Covid-19 Pandemic," V-Dem Institute, 2020, https://www.v-dem.net/media/filer_public/37/de/37defb66-9457-4eeb-887a-f0c168dc4365/v-dem_policybrief-25_201002_v2.pdf.
85. "Bahrain, Kuwait and Norway Contact Tracing Apps a Danger for Privacy," Amnesty International, June 16, 2020, https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/.
86. Maria Ressa (cofounder, *Rappler*), interview with the author, August 27, 2019.