IDEAS

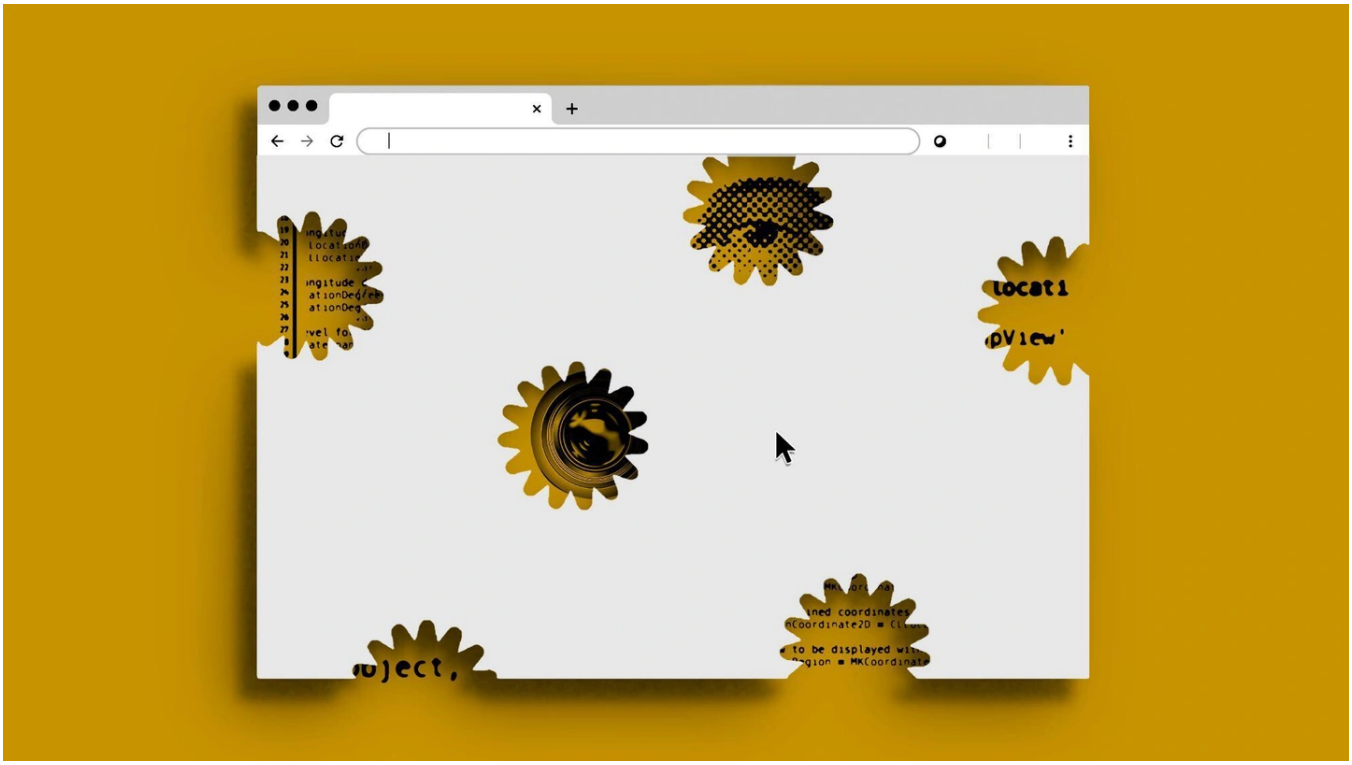
Internet Speech Will Never Go Back to Normal

In the debate over freedom versus control of the global network, China was largely correct, and the U.S. was wrong.

APRIL 25, 2020

Jack Goldsmith
Harvard Law School professor

Andrew Keane Woods
Professor of law at the University of Arizona College of Law



THE ATLANTIC

Updated at 3:15 p.m. ET on April 27, 2020.

COVID-19 HAS EMBOLDENED American tech platforms to emerge from their defensive crouch. Before the pandemic, they were targets of public outrage over life under their dominion. Today, the platforms are proudly collaborating with one another, and following government guidance, to censor harmful information related to the coronavirus. And they are using their prodigious data-collection capacities, in coordination with federal and state governments, to

improve contact tracing, quarantine enforcement, and other health measures. As Facebook's Mark Zuckerberg recently boasted, "The world has faced pandemics before, but this time we have a new superpower: the ability to gather and share data for good."

Civil-rights groups are tolerating these measures—emergency times call for emergency measures—but are also urging a swift return to normal when the virus ebbs. We need "to make sure that, when we've made it past this crisis, our country isn't transformed into a place we don't want to live," warns the American Civil Liberties Union's Jay Stanley. "Any extraordinary measures used to manage a specific crisis must not become permanent fixtures in the landscape of government intrusions into daily life," declares the Electronic Frontier Foundation, a digital-rights group. These are real worries, since, as the foundation notes, "life-saving programs such as these, and their intrusions on digital liberties, [tend] to outlive their urgency."

But the "extraordinary" measures we are seeing are not all that extraordinary. Powerful forces were pushing toward greater censorship and surveillance of digital networks long before the coronavirus jumped out of the wet markets in Wuhan, China, and they will continue to do so once the crisis passes. The practices that American tech platforms have undertaken during the pandemic represent not a break from prior developments, but an acceleration of them.

[Read: No, the internet is not good again]

As surprising as it may sound, digital surveillance and speech control in the United States already show many similarities to what one finds in authoritarian states such as China. Constitutional and cultural differences mean that the private sector, rather than the federal and state governments, currently takes the lead in these practices, which further values and address threats different from those in China. But the trend toward greater surveillance and speech control here, and toward the growing involvement of government, is undeniable and likely inexorable.

In the great debate of the past two decades about freedom versus control of the network, China was largely right and the United States was largely wrong. Significant monitoring and speech control are inevitable components of a mature and flourishing internet, and governments must play a large role in these practices to ensure that the internet is compatible with a society's norms and values.

Beginning in the 1990s, the U.S. government and powerful young tech firms began promoting nonregulation and American-style freedom of speech as essential features of the internet. This approach assumed that authoritarian states would crumble in the face of digital networks that seemed to have American constitutional values built into them. The internet was a vehicle for spreading U.S. civil and political values; more speech would mean better speech platforms, which in turn would lead to democratic revolutions around the world.

China quickly became worried about unregulated digital speech—both as a threat to the Communist Party's control and to the domestic social order more generally. It began building ever more powerful mechanisms of surveillance and control to meet these threats. Other authoritarian nations would follow China's lead. In 2009, China, Russia, and other members of the Shanghai Cooperation Organisation announced their "agreement on cooperation in the field of international information security." The agreement presciently warned of a coming "information war," in which internet platforms would be weaponized in ways that would threaten nations' "social and political systems."

[Evelyn Douek: The internet's titans make a power grab]

During the George W. Bush and Obama administrations, the United States helped secure digital freedoms for people living in authoritarian states. It gave them resources to support encryption and filter-evasion products that were designed to assist individuals in "circumventing politically motivated censorship," as then–Secretary of State Hillary Clinton put it in 2010. And it openly assisted Twitter and other U.S. tech platforms that seemed to be fueling the Arab Spring.

In these and so many other ways, the public internet in its first two decades seemed good for open societies and bad for closed ones. But this conventional wisdom turned out to be mostly backwards. China and other authoritarian states became adept at reverse engineering internet architecture to enhance official control over digital networks in their countries and thus over their populations. And in recent years, the American public has grown fearful of ubiquitous digital monitoring and has been reeling from the disruptive social effects of digital networks.

Two events were wake-up calls. The first was Edward Snowden's revelations in 2013 about the astonishing extent of secret U.S. government monitoring of digital networks at home and abroad. The U.S. government's domestic surveillance is

legally constrained, especially compared with what authoritarian states do. But this is much less true of private actors. Snowden's documents gave us a glimpse of the scale of surveillance of our lives by U.S. tech platforms, and made plain how the government accessed privately collected data to serve its national-security needs.

The second wake-up call was Russia's interference in the 2016 election. As Barack Obama noted, the most consequential misinformation campaign in modern history was "not particularly sophisticated—this was not some elaborate, complicated espionage scheme." Russia used a simple phishing attack and a blunt and relatively limited social-media strategy to disrupt the legitimacy of the 2016 election and wreak still-ongoing havoc on the American political system. The episode showed how easily a foreign adversary could exploit the United States' deep reliance on relatively unregulated digital networks. It also highlighted how legal limitations grounded in the First Amendment (freedom of speech and press) and the Fourth Amendment (privacy) make it hard for the U.S. government to identify, prevent, and respond to malicious cyber operations from abroad.

These constitutional limits help explain why, since the Russian electoral interference, digital platforms have taken the lead in combatting all manner of unwanted speech on their networks—and, if anything, have increased their surveillance of our lives. But the government has been in the shadows of these developments, nudging them along and exploiting them when it can.

Ten years ago, speech on the American Internet was a free-for-all. There was relatively little monitoring and censorship—public or private—of what people posted, said, or did on Facebook, YouTube, and other sites. In part, this was due to the legal immunity that platforms enjoyed under Section 230 of the Communications Decency Act. And in part it was because the socially disruptive effects of digital networks—various forms of weaponized speech and misinformation—had not yet emerged. As the networks became filled with bullying, harassment, child sexual exploitation, revenge porn, disinformation campaigns, digitally manipulated videos, and other forms of harmful content, private platforms faced growing pressure from governments and users to fix the problems.

The result a decade later is that most of our online speech now occurs in closely monitored playpens where many tens of thousands of human censors review

flagged content to ensure compliance with ever-lengthier and more detailed "community standards" (or some equivalent). More and more, this human monitoring and censorship is supported—or replaced—by sophisticated computer algorithms. The firms use these tools to define acceptable forms of speech and other content on their platforms, which in turn sets the effective boundaries for a great deal of speech in the U.S. public forum.

After the 2016 election debacle, for example, the tech platforms took aggressive but still imperfect steps to fend off foreign adversaries. YouTube has an aggressive policy of removing what it deems to be deceptive practices and foreign-influence operations related to elections. It also makes judgments about and gives priority to what it calls "authoritative voices." Facebook has deployed a multipronged strategy that includes removing fake accounts and eliminating or demoting "inauthentic behavior." Twitter has a similar censorship policy aimed at "platform manipulation originating from bad-faith actors located in countries outside of the US." These platforms have engaged in "strategic collaboration" with the federal government, including by sharing information, to fight foreign electoral interference.

The platforms are also cooperating with one another and with international organizations, and sometimes law enforcement, on other censorship practices. This collaboration began with a technology that allows child pornography to be assigned a digital fingerprint and placed in centralized databases that the platforms draw on to suppress the material. A similar mechanism has been deployed against terrorist speech—a more controversial practice, since the label *terrorist* often involves inescapably political judgments. Sharing and coordination across platforms are also moving forward on content related to electoral interference and are being discussed for the manipulated videos known as deepfakes. The danger with "content cartels," as the writer Evelyn Douek dubs these collaborations, is that they diminish accountability for censorship decisions and make invariable mistakes more pervasive and harder to fix.

And of course, mistakes are inevitable. Much of the content that the platforms censor—for example, child pornography and content that violates intellectual-property rights—is relatively easy to identify and uncontroversial to remove. But Facebook, for example, also takes down hate speech, terrorist propaganda, "cruel and insensitive" speech, and bullying speech, which are harder to identify objectively and more controversial to regulate or remove. Facebook publishes data

on its enforcement of its rules. They show that the firm makes "mistakes"—defined by its own flexible criteria—in about 15 percent of the appealed cases involving supposed bullying and about 10 percent of the appealed hate-speech cases.

All these developments have taken place under pressure from Washington and Brussels. In hearings over the past few years, Congress has criticized the companies—not always in consistent ways—for allowing harmful speech. In 2018, Congress amended the previously untouchable Section 230 of the Communications Decency Act to subject the platforms to the same liability that nondigital outlets face for enabling illegal sex trafficking. Additional amendments to Section 230 are now in the offing, as are various other threats to regulate digital speech. In March 2019, Zuckerberg invited the government to regulate "harmful content" on his platform. In a speech seven months later defending America's First Amendment values, he boasted about his "team of thousands of people and [artificial-intelligence] systems" that monitors for fake accounts. Even Zuckerberg's defiant ideal of free expression is an extensively policed space.

Against this background, the tech firms' downgrading and outright censorship of speech related to COVID-19 are not large steps. Facebook is using computer algorithms more aggressively, mainly because concerns about the privacy of users prevent human censors from working on these issues from home during forced isolation. As it has done with Russian misinformation, Facebook will notify users when articles that they have "liked" are later deemed to have included health-related misinformation.

But the basic approach to identifying and redressing speech judged to be misinformation or to present an imminent risk of physical harm "hasn't changed," according to Monika Bickert, Facebook's head of global policy management. As in other contexts, Facebook relies on fact-checking organizations and "authorities" (from the World Health Organization to the governments of U.S. states) to ascertain which content to downgrade or remove.

[Read: How to misinform yourself about the coronavirus]

What is different about speech regulation related to COVID-19 is the context: The problem is huge and the stakes are very high. But when the crisis is gone, there is no unregulated "normal" to return to. We live—and for several years, we have been living—in a world of serious and growing harms resulting from digital speech.

Governments will not stop worrying about these harms. And private platforms will continue to expand their definition of offensive content, and will use algorithms to regulate it ever more closely. The general trend toward more speech control will not abate.

Over the past decade, network surveillance has grown in roughly the same proportion as speech control. Indeed, on many platforms, ubiquitous surveillance is a prerequisite to speech control.

The public has been told over and over that the hundreds of computers we interact with daily—smartphones, laptops, desktops, automobiles, cameras, audio recorders, payment mechanisms, and more—collect, emit, and analyze data about us that are, in turn, packaged and exploited in various ways to influence and control our lives. We have also learned a lot—but surely not the whole picture—about the extent to which governments exploit this gargantuan pool of data.

Police use subpoenas to tap into huge warehouses of personal data collected by private companies. They have used these tools to gain access to doorbell cameras that now line city blocks, microphones in the Alexa devices in millions of homes, privately owned license-plate readers that track every car, and the data in DNA databases that people voluntarily pay to enter. They also get access to information collected on smart-home devices and home-surveillance cameras—a growing share of which are capable of facial recognition—to solve crimes. And they pay to access private tow trucks equipped with cameras tracking the movements of cars throughout a city.

[Derek Thompson: The technology that could free America from quarantine]

In other cases, federal, state, and local governments openly work in conjunction with the private sector to expand their digital surveillance. One of the most popular doorbell cameras, Ring, which is owned by Amazon, has forged video-sharing partnerships with more than 400 law-enforcement agencies in the United States. Ring actively courted law-enforcement agencies by offering discounted cameras to local police departments, which offered them to residents. The departments would then use social media to encourage citizens to download Ring's neighborhood application, where neighbors post videos and discuss ostensibly suspicious activity spotted on their cameras. (A Ring spokeswoman said the company no longer offers free or discounted cameras to law enforcement.)*

Meanwhile, the company Clearview AI provides law-enforcement agents with the ability to scan an image of a face across a database of billions of faces, scraped from popular apps and websites such as Facebook and YouTube. More than 600 law-enforcement agencies are now using Clearview's database.

These developments are often greeted with blockbuster news reports and indignant commentary. And yet Americans keep buying surveillance machines and giving their data away. Smart speakers such as the Amazon Echo and Google Home are in about a third of U.S. households. In 2019, American consumers bought almost 80 million new smartphones that can choose among millions of apps that collect, use, and distribute all manner of personal data.. Amazon does not release sales numbers for Ring, but one firm estimated that it sold almost 400,000 Ring security devices in December alone.

America's private surveillance system goes far beyond apps, cameras, and microphones. Behind the scenes, and unbeknownst to most Americans, data brokers have developed algorithmic scores for each one of us—scores that rate us on reliability, propensity to repay loans, and likelihood to commit a crime. Uber bans passengers with low ratings from drivers. Some bars and restaurants now run background checks on their patrons to see whether they're likely to pay their tab or cause trouble. Facebook has patented a mechanism for determining a person's creditworthiness by evaluating their social network.

These and similar developments are the private functional equivalent of China's social-credit ratings, which critics in the West so fervently decry. The U.S. government, too, makes important decisions based on privately collected pools of data. The Department of Homeland Security now requires visa applicants to submit their social-media accounts for review. And courts regularly rely on algorithms to determine a defendant's flight risk, recidivism risk, and more.

The response to COVID-19 builds on all these trends, and shows how technical wizardry, data centralization, and private-public collaboration can do enormous public good. As Google and Apple effectively turn most phones in the world into contact-tracing tools, they have the ability to accomplish something that no government by itself could: nearly perfect location tracking of most the world's population. That is why governments in the United States and around the world are working to take advantage of the tool the two companies are offering.

Apple and Google have told critics that their partnership will end once the pandemic subsides. Facebook has said that its aggressive censorship practices will cease when the crisis does. But when COVID-19 is behind us, we will still live in a world where private firms vacuum up huge amounts of personal data and collaborate with government officials who want access to that data. We will continue to opt in to private digital surveillance because of the benefits and conveniences that result. Firms and governments will continue to use the masses of collected data for various private and social ends.

[Edward Tenner: Efficiency is biting back]

The harms from digital speech will also continue to grow, as will speech controls on these networks. And invariably, government involvement will grow. At the moment, the private sector is making most of the important decisions, though often under government pressure. But as Zuckerberg has pleaded, the firms may not be able to regulate speech legitimately without heavier government guidance and involvement. It is also unclear whether, for example, the companies can adequately contain foreign misinformation and prevent digital tampering with voting mechanisms without more government surveillance.

The First and Fourth Amendments as currently interpreted, and the American aversion to excessive government-private-sector collaboration, have stood as barriers to greater government involvement. Americans' understanding of these laws, and the cultural norms they spawned, will be tested as the social costs of a relatively open internet multiply.

COVID-19 is a window into these future struggles. At the moment, activists are pressuring Google and Apple to build greater privacy safeguards into their contact-tracing program. Yet the legal commentator Stewart Baker has argued that the companies are being too protective—that existing privacy accommodations will produce "a design that raises far too many barriers to effectively tracking infections." Even some ordinarily privacy-loving European governments seem to agree with the need to ease restrictions for the sake of public health, but the extent to which the platforms will accommodate these concerns remains unclear.

We are about to find out how this trade-off will be managed in the United States. The surveillance and speech-control responses to COVID-19, and the private sector's collaboration with the government in these efforts, are a historic and very

public experiment about how our constitutional culture will adjust to our digital future.

** An earlier version of this article misstated the status of a now-discontinued Ring initiative providing local police with discounted cameras. The company no longer extends that offer.*

We want to hear what you think about this article. Submit a letter to the editor or write to letters@theatlantic.com.