New American

Written by **Steve Bonta** on May 23, 2023

Published in the June 12, 2023 issue of the New American magazine. Vol. 39, No. 11

High-tech Power: Government Surveillance & Censorship

In the 2002 film *Minority Report*, based on a story by famed science-fiction writer Phillip K. Dick, Tom Cruise's John Anderton lives in a dystopian future Washington, D.C., where ubiquitous retina scanners track your every move, allowing the government to locate you within seconds and intrusive holographic commercials to target your tastes in any public place. The police have become almost omnipotent and all-seeing, able to deploy unstoppable robotic spiders to search for criminals, and reliant upon psychic "precogs," who can predict murders before they even occur. In such a world, Anderton and his fellow "precrime" investigators have managed to eliminate murder — and personal freedom along with it.

AP Images

Health code: Security guards block the entrance to a Chinese neighborhood during the Covid pandemic. The QR codes displayed must be scanned with one's smartphone, to allow authorities to collect information on travel and contact tracing.

Such a view of America in the 2050s may have seemed fantasy to audiences two decades ago, but the coming of age of a panoply of new surveillance and control technologies is more and more imparting to such disturbing sci-fi an aura of prophecy. In particular, the sophisticated new tools for censorship — of controversial ideas and truths inconvenient to America's ruling establishment — have become so pervasive and so effective that the future of free speech, and even the long-term viability of free and independent thought, is coming increasingly into question.

Dystopia With Chinese Characteristics

For the 1.3 billion citizens of the People's Republic of China, the future techno-dystopia is already here. In devising ways to harness the oppressive potential of 21st-century technology, Communist China is setting the pace. With the help of Western techie quislings, China erected the so-called Great Firewall, the most comprehensive censorship and surveillance mechanism ever devised, a bewilderingly complex array of jamming, blocking, and tracking contrivances that now allows China to almost completely block access to the virtual outside world, and to keep tabs on the thoughts and deeds of all of its hundreds of millions of citizens who surf the web and use smartphones. The only way that the Chinese (and foreigners residing in China) can normally breach the Great Firewall is with a reliable VPN (virtual private network), which allows access to sites such as Google, Facebook, Instagram, YouTube, Western news media, and other social and informational online media that Westerners take for granted. Since 2017, however, the Chinese government has made even the use of VPNs illegal, and has been jailing Chinese with the forbidden software on their phones and laptops.

Instead of Western social media and information and news sites, the Chinese government has created an entire range of domestic apps and online companies that are in effect extensions of the Communist Party, whose employees know better than to allow users access to anything that the Communist Party has declared off-limits, such as discussion of the Tiananmen Square massacre or Taiwan's de facto

independence. To counter any would-be dissidents on Chinese state-approved media such as WeChat and Weibo, the government employs millions of zealous party supporters who comb through every article, message, and post online for criticism of the party, of its paramount leader Xi Jinping, of the government, of the economy, or of Chinese society and culture. The technology at their disposal allows them to proscribe words and phrases that are associated with anything objectionable, to take down posts and terminate accounts that violate the party's Byzantine standards of acceptability, and even to digitally cancel the social-media accounts of refractory citizens.

And it doesn't stop with information control. China has erected a modern society completely dependent on smartphones and apps, not only for communication but also for travel, shopping, banking, and identification. Lose your WeChat account and you not only lose the ability to text and video chat with friends, as well as post photos on WeChat Moments, you also lose access to WeChat-based QR codes that are used for identification, the purchase of train and airplane tickets, shopping, and entry into many public places. The QR-code regime of microcontrols came of age during the Covid era, when smartphone-based health QR codes for contact tracing and travel QR codes were developed with the ambitious aim of tracking the movements and potential contagion of every person in China. Without a smartphone and the associated QR codes, it was impossible to comply with the onerous and ever-changing local requirements for Covid testing, to travel inside or out of China, or even to enter most eateries and shopping centers. And although the Covid pandemic has been declared over and its more visible signs of oppression — the barricaded neighborhoods, the quarantine barracks, and the Covid checkpoints — have disappeared, the technology for virtual oppression developed in response to the pandemic remains in place.

Nor is this all. China has embraced the oppressive potential of CCTV-camera tech like no other country. Ubiquitous banks of CCTV cameras, monitored in real time by huge numbers of police in every town, city, and neighborhood, are now equipped with facial-recognition software so advanced it can allegedly identify people wearing medical face masks. This technology, too, was created during the pandemic, to rectify the unacceptable circumstance of a billion-plus people appearing in public with their identifying facial features covered. Now the CCP has figured out how to see through masks, scarves, and other gear partially concealing faces from the naked scrutiny of the panopticon state.

All-seeing camera eye: Supporters of Hong Kong activists are shown here waiting to enter a court room under the watchful eye of ubiquitous CCTV cameras, which in China are used to garner

information on movements of all citizens. (AP Images)

China and her growing retinue of techno-socialist wannabe regimes around the world are rapidly turning into a 21st-century high-tech totalitarian gulag that would make John Anderton and his fictional "pre-crime" cohorts proud; a finely tuned, sanitized showpiece of dystopian social engineering, where the slightest peep of dissent or free expression — let alone actual resistance — has been rendered all but impossible by cutting-edge technology, and always in the name of perfecting national security.

But such an outcome would surely be impossible in America, where individuality, dissent, and diversity are prized cultural attributes, and where the government is prohibited from spying on its own people without oversight and without limits — that, at least, is what we would all like to believe. In reality, much of the technology now used in China to keep the unruly masses cowed was developed first by Western firms, and its use in China may be regarded as beta testing for potential use in the West. In 2003, China launched its "Golden Shield" project that led to the creation of the Great Firewall. Most of the hardware for the project was provided by Western tech companies such as Cisco Systems rather than being developed indigenously.
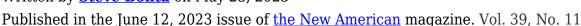
Nowadays, Chinese tech giants such as Huawei and Weibo are the primary producers of the tech used in Chinese censorship, but Western tech giants such as Google have been trying for years to curry favor with the Chinese regime by developing software compatible with the Chinese system. Google, for example, spent a significant amount of time with its secret "Project Dragonfly" trying to develop a search engine with self-censorship capabilities consistent with Chinese standards. Moreover, China has exported its censorship tech to a number of repressive regimes, including Iran, Cuba, Zimbabwe, and Belarus — but also Australia. So while the erection of a Western counterpart to Communist China's Great Firewall does not seem politically viable at this point, both the technical knowhow and government interest in such a project are very real.

The American Model

For the short term, though, the American approach to high-tech censorship and thought control is likely to be of the subtler sort, only now coming to light in the wake of massive internet censorship and narrative-molding campaigns targeting Covid etiology and vaccines, Donald Trump, the January 6 protests, and various other topics regarded by the entrenched American elites as too toxic to allow unfiltered into American minds.

In theory, at least, the federal government is legally very limited in its power to surveil and censor Americans' online activities. In practice, the picture is far different. Ever since Ronald Reagan signed Executive Order 12333 in 1981, U.S. government agencies and departments have been under orders to comply fully with any requests by the CIA for information. The order is the seminal document authorizing virtually unlimited data collection by American intelligence agencies — collection ostensibly confined to foreign sources, but vaguely conjoined with information obtained "incidentally" that might have bearing on domestic infractions. Among other things, this has been construed to allow the NSA to collect bulk communications data and to store it for up to five years. The PATRIOT Act and its successor, the unironically named USA FREEDOM Act signed by President Obama, both built upon the already-formidable federal powers of surveillance that existed pre-2001 by constituting a secret Foreign Intelligence Surveillance Court (FISA) designed to rubber-stamp requests by the likes of the NSA and FBI to conduct surveillance of American citizens' phone logs and internet activities. Much of the federal

harassment of the Trump campaign and of Trump's associates was carried out thanks to abuse of the FISA warrant system.

Thus de facto federal power to exploit the reach of modern technology to surveil American citizens is little less than what is done in Communist China.

However, in stark contrast to China and other totalitarian governments, much less can actually be done by our government to use tech directly and openly to mold public opinion, suppress information, and even cancel individuals who challenge regime orthodoxies. But where China has recourse to cyberpolice and other unsubtle instruments of high-tech tyranny, the American government is perfecting the art of molding consensus, manufacturing mass consent, and suppressing dissent by partnering with dominant private players in the world of internet news, social networks, and smartphone apps. And the tools this public/private partnership has at its disposal are nearly as powerful as those on display in *Minority Report's* fictional dystopia.

For starters, there are the innocuously named "cookies," which, most of us are at least vaguely aware, are used to track our internet activity. Cookies are simply text files with small pieces of data used to identify a computer. On one hand, they are absolutely indispensable to the modern internet, allowing websites to recognize computers that have previously visited and autofill personal data and passwords. Without them, the internet user would have to keep detailed and completely accurate records of browsing history, passwords, usernames, and the like; thanks to cookies, browsing histories can be maintained and the URLs of frequently visited sites autofill on web browser tabs. But, of course, cookies are not deployed out of pure benevolence. Sites that depend on advertising for revenue, as well as sites that sell products, use cookies professedly to "improve your browsing experience," i.e., remember your personal tastes and interest in order to generate ads and product placement that will more likely induce you to spend your money. For those inclined to decry the commercialization of the internet, the smothering blanket of personalized ads that typically follows the web user everywhere he goes online, thanks to the magic of cookies, is cause enough for concern. But quite aside from the unending annoyance of popup, banner, and video ads that always seem to target our own age groups and personal interests, cookies are a veritable bonanza for criminals bent on finding out everything about us in order to hijack our personal identity. The trail of virtual breadcrumbs strewn in the wake of every web user is often enough for scammers to figure out personal passwords and even impersonate users on social media, as anyone whose Facebook account has ever been cloned is well aware.

But the worst cybercriminals are not faux Nigerian princes or hackers in Bangalore. Those same virtual breadcrumbs can be exploited by lawless government busybodies to follow every intimate detail of our lives, and leverage the ill-gotten information as needed.

Those who express opinions online are in effect throwing up a beacon that draws attention to themselves. The more controversial the opinion, whether on Facebook, Instagram, Twitter, YouTube, or even an old-fashioned blog, the more likely it will attract unwanted attention from the cybercriminals in the federal government, who have lately perfected the art of censoring and canceling the more disruptive elements online. Former president Donald Trump learned this firsthand when, in the wake of the January 6 protests, he found himself removed from all social media, joining the likes of Alex Jones and other online "extremists."

The Twitter Follies

The way this is accomplished, as we are all now finding out thanks to ongoing congressional investigations into Twitter and other social media, is that government officials inform executives at online media corporations to censor stories that are darkly hinted to be Russian or other nefarious foreign propaganda, misinformation by shadowy "domestic extremists," or other such pretexts. The unspoken subtext is: "Play ball in suppressing this story or that individual, or we will come at you with new regulations, or unfavorable publicity, or something else that will damage your bottom line." Knowing the ability of Deep State actors in the government and the legacy media to generate propaganda and whip up popular hysteria, such companies are usually happy to comply.

A vivid example of how this is done was revealed in the recent release of the so-called Twitter files by new Twitter CEO Elon Musk. As one of the largest and most influential social-media sites, beloved of politicians, entertainers, and publicity mongers of every type, the microblogging giant played an immensely important role in the rise of Donald Trump and the MAGA movement, in the spread of the "#MeToo" movement, and in many other consequential movements and trends of the last decade. The Twitter files showed the world the degree to which the powerful company had been transformed into a propaganda arm of the anti-Trump, pro-vax Deep State, by maintaining an alliance with the FBI, powerful Democrats on Capitol Hill, and the Biden family. For example, it is now beyond dispute that Twitter closed ranks with the legacy media in suppressing the Hunter Biden laptop story in October 2020 after being warned by a duplicitous FBI that the story was most likely foreign disinformation. Not only that, before Musk released the first batch of Twitter files, which contained the Hunter Biden laptop revelations, they were secretly vetted by Twitter's deputy general counsel Jim Baker — who just happened to have served previously as FBI general counsel and who had been involved in the farcical Trump-Russia investigation.

Twitterpated: Elon Musk's acquisition of Twitter met with fierce resistance from leftists, who understood how valuable a propaganda tool the microblogging behemoth had been. But Musk appears to be making good on his promise to restore Twitter both to profitability and political neutrality. (AP Images)

The long-alleged practice of "shadowbanning," whereby the accounts of prominent conservative and Covid contrarian voices were buried from public view on Twitter without the account holders'

knowledge, was confirmed, despite Twitter officials' longtime lying about the practice and the usual shrill accusations in the left-wing media of "far-right conspiracy theories."

The FBI regularly flagged tweets by Trump and his supporters during the 2020 election campaign as "problematic" — meaning that they contradicted the official narratives of the Deep State. Specifically, FBI Special Agent Elvis Chan stayed in constant touch with Twitter to indicate which tweets the FBI wanted taken down. During that period, Twitter's head of trust and safety Yoel Roth also met weekly with officials from the FBI, the Department of Homeland Security, and the office of the Director of National Intelligence.

Nor was the Twitter partnership with government confined to Trump and his supporters. A lot of influence was exerted to silence the voices of those questioning the Covid-era reign of error. For example, Pfizer board member and former FDA commissioner Scott Gottlieb pressured Twitter to censor those casting doubt on the effectiveness of the Covid vaccines, leading to, among other things, the suspension from Twitter of Alex Berenson, a Substack writer and vocal vaccine skeptic.

One powerful Democrat on Capitol Hill, Representative Adam Schiff (D-Calif.), used his influence to get tweets removed and accounts suspended that were critical of him and his staff. Schiff and several other leading Democrats, including fellow California Senator Dianne Feinstein, also pushed a false narrative to the effect that Russian bots were driving the popularity of a memo by Devin Nunes that cast doubt on the veracity of the Russian collusion hoax.

And it was revealed that Twitter's propaganda reach even extended overseas, at the behest of the Pentagon and the CIA.

The convoluted story of Deep State collusion with Twitter, which led in the end to the banning of Trump himself from the platform along with many of his prominent supporters, is still only known in broad outline; the details of arm-twisting, influence-peddling, and opinion-molding will probably never be known in full — much less similar machinations with the likes of YouTube and Facebook, whose vigorous shadowbanning and account suspension of conservatives and other assorted recalcitrants is well documented.

This is merely the beginning of the emergence of a new high-tech regime of censorship and thought control, courtesy of an unholy alliance between the Deep State and enormously well-funded and influential tech giants. These have together managed to impose their will on much of the once-free internet, the medium that, at its inception in the 1990s, was touted as a grand "information superhighway" where the token of the realm would be unfettered freedom of expression. Yet in the decades since, it has devolved into just another tightly regulated, weaponized tool of Big Government, like print, radio, and television before it, but with far greater power than all of its predecessor media combined to peddle the Big Lie and to mold a compliant, uninformed populace. And with the recent meteoric rise of generative AI, with its almost limitless potential for deception and artificiality, the future of high tech as the ultimate tool of control appears ominous indeed.

All is not lost, however. Elon Musk's takeover of Twitter and its subsequent repurposing as a bona fide arena of free discourse is a positive development. And for all of its faults, the internet remains an extraordinarily powerful tool for research, fact-checking, alternative views, and the overall propagation of truth for those actively seeking it. For all of the propaganda and censorship courtesy of Big Media and the legacy tech giants such as Google, YouTube, and Facebook, there are abundant "little tech"

competitors, such as Rumble, that remain mostly uncompromised and unbiased. Thanks in large measure to the unparalleled reach of the internet, many Americans today are far better informed than ever before.

There are also many steps that informed netizens can take to reduce the ability of Big Government to spy on them (see "Digital Privacy in a World of High-tech Surveillance"). The same technology that has empowered the state has also empowered the individual. And Americans should continue to exert pressure, through their elected representatives, to shine the light of day on government's use of technology to deceive, cover up, and oppress. By exposing such malfeasance in high places, we can yet avoid following the trail blazed by Communist China into a dystopian future out of a Phillip K. Dick cautionary tale.

New American

Written by **Steve Bonta** on May 23, 2023

Published in the June 12, 2023 issue of the New American magazine. Vol. 39, No. 11