

Beware: Our New Online Culture Is a Feast for Mass Surveillance

The [rapid spread of COVID-19](#) has caused network traffic to surge as Internet users resort to video conferencing to work remotely.

For example, last December online meeting provider Zoom hosted roughly 10 million participants. In March this statistic [jumped to 200 million](#). The public's stampede to the cloud is an auspicious development for the intelligence community as sensitive discussions that once occurred in physical office buildings are now channeled through a relatively small number of digital gatekeepers. The implications are unsettling.

From the vantage point of professional spies, the desire to eavesdrop on popular communication channels is all but irresistible. In the United States we've witnessed classified programs [like PRISM](#), where the NSA succeeded in convincing all of the big names in Silicon Valley to participate. [Chatting up tech CEOs](#) on a first name basis. Authoritarian regimes like China are even more eager to tap commercial data streams. Which is particularly salient given that [most of Zoom's engineers work over in China](#) and that Zoom has [unfettered access](#) to the online conferences that it hosts despite marketing claims to the contrary.

Hence, efforts to limit the spread of contagion offer a golden opportunity to [double down](#) on mass surveillance. Data collection tools wielded during an emergency on behalf of public safety –[facial recognition](#), [drones](#), [mobile device apps](#), [smart phone geolocation](#), [payment card records](#)– over time take on a hue of legitimacy. Furthermore the bureaucrats using such tools are loath to give up their newfound access and will

actively identify additional threats to justify it.

China serves as an instructive example. The Communist Party remains in power through an [unspoken agreement](#) with the rest of Chinese society. It's the sort of deal that exists in many repressive nations. The government assures economic growth and in return citizens are expected to stay out of politics and submit to extreme social control measures. The Chinese government asserts that growth will continue at [around 6 percent](#), but keep in mind that it also aggressively [censors bad economic news](#), in the same manner that it [suppressed news](#) about the COVID-19 outbreak.

It's highly unlikely that the Party will be able to keep delivering results forever. The COVID-19 outbreak will simply hasten a looming economic crisis in China, despite the Party's best efforts to maintain control. With China's [towering mountain of debt](#), [zombie factories](#), and conspicuous [industrial overcapacity](#), it's just a matter of time before the average citizen realizes that they're not going to get what they were promised. This raises the specter of military action as the government directs attention outward in search of enemies to mobilize its restive populace. Against this backdrop mass surveillance will be ramped up in a desperate attempt to buttress the status quo.

Common sense dictates that relying on technology that's developed in a police state like China is inherently risky. The instinctive response for many users is to turn to American technology. However, thanks to whistleblowers like Edward Snowden the public record shows that domestic companies are also [cooperating with the intelligence community](#) as well as [monetizing their access](#) to user data. So if you're wondering whether a particular online platform is secure, you're asking the wrong question. The salient question is which group of security services and big data aggregators have access?

Sadly this makes achieving higher levels of communication

security a sort of DIY affair. The key is to prevent the current COVID-19 setting from becoming the new normal by recognizing what's at stake. The more that we rely on Internet platforms to communicate the more power we yield to a narrow set of vested interests. Such that our need to stay in touch with each other during a disaster secretly morphs into a feeding frenzy for spies. Just as it did [in the wake of the 9/11 attacks](#). As always, freedom entails responsibility. This means leaving mainstream channels for sensitive discussions and doing so in a manner that doesn't create baseline anomalies that might alert watchers.

Pervasive monitoring is not the behavior of a confident nation. Mass surveillance isn't the harbinger of stability. It's a dangerous political tremor. A display of anxiety rather than strength. An indicator that leaders have recklessly chosen to dispense with civil liberties behind closed doors under the guise of addressing perceived threats. As citizens we have an obligation to protect the values which actually make America strong. To encourage lawmakers to resist the impulse to trade essential liberty for short-term promises of security and to forge our own paths forward when they fail to do so.

—

This [article](#) has been republished with permission from The American Conservative.

[Image Credit: Pixabay]

Image Credit: [Image Credit: Pixabay]