Domestic Surveillance Has a Chilling Effect on Political Speech

Domestic Surveillance, 2015

John W. Whitehead is an attorney and president of the Rutherford Institute, a nonprofit civil liberties and human rights organization.

The fact that the government can now, at any time, access entire phone conversations, e-mail exchanges, and other communications from months or years past should frighten every American. But it mostly doesn't because the public has come to accept such intrusion into their lives as a byproduct of ensuring public safety in a climate of fear, following such events as September 11, 2001, or the Boston Marathon bombing in 2013. The reality that all digital communications are now monitored is dangerous for free speech, as evidenced by the Massachusetts teen who was jailed on terrorism charges over rap lyrics he posted on Facebook. The government has become a bigger threat to American freedoms than the terrorist groups these security agencies were designed to thwart.

"If you're not a terrorist, if you're not a threat, prove it. This is the price you pay to live in free society right now. It's just the way it is."

Immediately following the devastating 9/11 [2001] attacks, which destroyed the illusion of invulnerability which had defined American society since the end of the Cold War, many Americans willingly ceded their rights and liberties to government officials who promised them that the feeling of absolute safety could be restored.

In the [13] years since, we have been subjected to a series of deceptions, subterfuges and scare tactics by the government, all largely aimed at amassing more power for the federal agencies and extending their control over the populace. Starting with the wars in Afghanistan and Iraq, continuing with the torture of detainees at Abu Ghraib and Guantanamo Bay [military prisons], and coming to a head with the assassination of American citizens abroad, the importing of drones and other weapons of compliance, and the rise in domestic surveillance, we have witnessed the onslaught of a full-blown crisis in government.

Now, in the wake of the Boston Marathon bombing, we are once again being assured that if we only give up a few more liberties and what little remains of our privacy, we will achieve that elusive sense of security we've yet to attain.

Still Americans have gone along with these assaults on their freedoms unquestioningly.
Even with our freedoms in shambles, our country in debt, our so-called "justice" system weighted in favor of corporations and the police state, our government officials dancing to the tune of corporate oligarchs, and a growing intolerance on the part of the government for anyone who challenges the status quo, Americans have yet to say "enough is enough."

Now, in the wake of the Boston Marathon bombing [April 2013], we are once again being assured that if we only give up a few more liberties and what little remains of our privacy, we will achieve that elusive sense of security we've yet to attain. This is the same song and dance that comes after every tragedy, and it's that same song and dance which has left us buying into the illusion that we are a free, safe society.

**All Digital Communications Are Monitored**

The reality of life in America tells a different tale, however. For example, in a May 2013 interview with CNN, former FBI [Federal Bureau of Investigation] counterterrorism agent Tim Clemente disclosed that the federal government is keeping track of all digital communications that occur within the United States, whether or not those communicating are American citizens, and whether or not they have a warrant to do so.

As revelatory as the disclosure was, it caused barely a ripple of dismay among Americans, easily distracted by the torrent of what passes for entertainment news today. Yet it confirms what has become increasingly apparent in the years after 9/11: the federal government is literally tracking any and all communications occurring within the United States, without concern for the legal limitations of such activity, and without informing the American people that they are doing so.

Clemente dropped his bombshell during a CNN interview about authorities' attempts to determine the nature of communications between deceased Boston bombing suspect Tamerlan Tsarnaev and his widow Katherine Russell. In the course of that conversation, Clemente revealed that federal officials will not only be able to access any voicemails that may have been left by either party, but that the entirety of the phone conversations they had will be at federal agents' finger tips.

"We certainly have ways in national security investigations to find out exactly what was said in that conversation," stated Clemente. "All of that stuff [meaning phone conversations occurring in America] is being captured as we speak whether we know it or like it or not." A few days later, Clemente was asked to clarify his comments, at which point he said, "There is a way to look at all digital communications in the past. No digital communication is secure."

Officials in the Obama administration have for some time now been authorizing corporate information sharing and spying in secret through the use of executive orders and other tactics.
In other words, there is no form of digital communication that the government cannot and does not monitor—phone calls, emails, text messages, tweets, Facebook posts, internet video chats, etc., are all accessible, trackable and downloadable by federal agents.

**Privacy Online Is Now Only an Illusion**

At one time, such actions by the government would not only have been viewed as unacceptable, they would also have been considered illegal. However, government officials have been engaged in an ongoing attempt to legitimize these actions by passing laws that make the lives of all Americans an open book for government agents. For example, while the nation was caught up in the drama of the Boston bombing and the ensuing military-style occupation of the city by local and federal police, Congress passed a little-noticed piece of legislation known as the Cyber Intelligence Sharing and Protection Act (CISPA). The legislation, which the House of Representatives approved by an overwhelming margin of 288-127, will allow internet companies to share their users' private data with the federal government and other private companies in order to combat so-called "cyber threats."

In short, the law dismantles any notion of privacy on the internet, opening every action one undertakes online, whether emailing, shopping, banking, or just browsing, to scrutiny by government agents. While CISPA has yet to clear the U.S. Senate Committee on Commerce, Science, and Transportation, the spirit of it is alive and well. In fact, officials in the [Barack] Obama administration have for some time now been authorizing corporate information sharing and spying in secret through the use of executive orders and other tactics.

The Justice Department, for instance, has been issuing so-called "2511 letters" to various internet service providers like AT&T, which immunize them from being prosecuted under federal wiretapping laws for providing the federal government with private information. Despite federal court rulings to the contrary, the Department of Justice continues to assert that it does not require a warrant to access Americans' emails, Facebook chats, and other forms of digital communication.

**How It All Started**

While it may be tempting to lay the full blame for these erosions of our privacy on the Obama administration, they are simply continuing a system of mass surveillance, the seeds of which were planted in the weeks after 9/11, when the National Security Agency (NSA) began illegally tracking the communications of American citizens. According to a Washington Post article published in 2010, the NSA continues to collect 1.7 billion communications, whether telephone, email or otherwise, every single day.
Aside from allowing government agents backdoor access to American communications, corporations are also working on technologies to allow government agents even easier access to Americans' communications.

The NSA and Department of Justice are just two pieces of a vast surveillance network which encompasses and implicates most of the federal government, as well as the majority of technology and telecommunications companies in the United States. For the past two years, the United States Foreign Intelligence Surveillance Court has approved literally every single request by the federal government to spy on people within the United States. There have been some 4,000 applications rubberstamped by the court in the past two years, applications which allow federal officials to monitor the communications of any person in the United States, including American citizens, if they are believed to be in contact with someone overseas.

These government-initiated spying programs depend in large part on the willingness of corporations to hand over personal information about their customers to government officials. Sometimes the government purchases the information outright. At other times, the government issues National Security Letters, which allow the government to force companies to hand over personal information without a warrant or probable cause.

**Tech Companies Get Onboard**

Some web companies, such as Skype, have already altered their products to allow government access to personal information. In fact, government agents can now determine the credit card information and addresses of Skype users under suspicion of criminal activity. Aside from allowing government agents backdoor access to American communications, corporations are also working on technologies to allow government agents even easier access to Americans' communications.

For example, Google has filed a patent for a "Policy Violation Checker," software which would monitor an individual's communications as they type them out, whether in an email, an Excel spreadsheet or some other digital document, then alert the individual, and potentially their employer or a government agent, if they type any "problematic phrases" which "present policy violations, have legal implications, or are otherwise troublesome to a company, business, or individual." The software would work by comparing the text being typed to a pre-defined database of "problematic phrases," which would presumably be defined on a company-by-company basis.

The emergence of this technology fits in well with Google chairman Eric Schmidt's view on privacy, which is that "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." Unfortunately, this is not just the attitude of
corporate benefactors who stand to profit from creating spy technology and software but
government officials as well.

Monitoring Social Media in Real Time

Additionally, police officials throughout the country have become increasingly keen on
monitoring social media websites in real time. Rob D'Ovido, a criminal justice professor at
Drexel University, has noted that, "The danger of this in light of the tragedy in Boston is that
law enforcement is being so risk-averse they are in danger of crossing that line and going
after what courts would ultimately deem as free speech."

Having traded our freedoms for a phantom promise of security, we now find ourselves
imprisoned in a virtual cage of cameras, wiretaps and watchful government eyes.

For example, Cameron Dambrosio, a teenager and self-styled rap artist living in Metheun,
Massachusetts, posted a video of one of his original songs on the internet which included
references to the White House and the Boston bombing. While the song's lyrics may well
have been crude and ill-advised in the wake of the Boston bombing, police officers
exacerbated the situation by arresting Dambrosio [in May 2013] and charging him with
communicating terrorist threats, a felony charge which could land him in prison for twenty
years.

Unfortunately, cases like Dambrosio's may soon become the norm, as the FBI's Next
Generation Cyber Initiative has announced that its "top legislative priority" this year is to get
social media giants like Facebook and Google to comply with requests for access to real-
time updates of social media websites. The proposed method of encouraging compliance is
legal inquiries and hefty fines leveled at these companies. The Obama administration is
expected to support the proposal.

The reality is this: we no longer live in a free society. Having traded our freedoms for a
phantom promise of security, we now find ourselves imprisoned in a virtual cage of
cameras, wiretaps and watchful government eyes. All the while, the world around us is no
safer than when we started on this journey more than a decade ago. Indeed, it well may be
that we are living in a far more dangerous world, not so much because the terrorist threat is
any greater but because the government itself has become the greater threat to our
freedoms.

Further Readings

Books
• Louise Gerdes At Issue: Drones. Farmington Hills, MI: Greenhaven, 2014.

**Periodicals and Internet Sources**

• Alex Abdo "You May Have ‘Nothing to Hide’ but You Still Have Something to Fear," American Civil Liberties Union, August 2, 2013. www.aclu.org.
- Kyle Chayka "Face-Recognition Software: Is This the End of Anonymity for All of Us?," Independent, April 23, 2014.
- Adrian Short "When Does Face Scanning Tip Over into the Full-Time Surveillance Society?," Guardian, November 5, 2013.
• David Von Drehle "The Surveillance Society," Time, August 1, 2013.


Source Citation