8 Bridge Street, Northampton, Massachusetts, 01060 • 413.582.0110 • www.bordc.org • info@bordc.org

Testimony to the

Information, Security and Privacy Advisory Board

From the Defending Dissent Foundation

and

Bill of Rights Defense Committee

Presented by Chip Gibbons, Defending Dissent Legal Fellow

October 23, 2015

The Defending Dissent Foundation and Bill of Rights Defense Committee are national civil liberties organizations that work to realize the rights promised by the U.S. Constitution. The impact of technology on the liberties of all Americans is of great concern to us. Advances in technology have opened up great doors for people the world over.

Technology in the hands of the people has had a democratizing effect: people from all walks of life have access to unprecedented amounts of knowledge and are able to communicate across the globe with rapidity once unimaginable; the Internet has created a public forum for individuals to express their views, while its anonymity has allowed individuals afraid of retaliation for their speech to express potentially unpopular opinions; and the role of technology in organizing and facilitating new movements has been noted across the world—whether it is in the mass protests for democracy in Egypt and Tunisia or in being used to coordinate Occupy Wall Street and Black Lives Matter protests here at home.

But technology, when used by the government, presents serious challenges for civil liberties. First, as law enforcement and intelligence agencies gain new technologies, they often claim that existing legal frameworks do not apply to them. Both the Defending Dissent Foundation and Bill of Rights Defense Committee strongly assert the U.S. Constitution provides the framework for all government surveillance and that new technologies are not exempt from these protections. While the drafters of the Constitution could not have imagined smart phones, twitter, or emails when they wrote about the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" they

nonetheless provided a clear framework for protecting personal communications from unwarranted government intrusion.

Second, as people have sought to use technology to facilitate democratic movements, governments the world over have sought to either restrict the use of technology, or turn technology into a repressive apparatus. The United States is not immune to this; this year marks the 40th Anniversary of the Church Committee, which demonstrated the very real legacy of government encroachment on democratic liberties in the United States. But such encroachments have continued: numerous Congressional reports, agency inspector general reports, and Freedom of Information Act (FOIA) Requests have repeatedly discovered the use of federal and local law enforcement to surveil, infiltrate, and collect information on First Amendment protected activities without any evidence of wrongdoing.

While this pattern of behavior is as old as J. Edgar Hoover, government use of technology has created a new chilling effect on speech. It has been reported that due to revelations concerning the U.S. government's surveillance of the Internet, journalists are now less likely to use e-mail to contact sources.[1] This is a great example of the democratizing power of the people's use of technology running up against the repressive potential of the government's use of technology. E-mail should be enabling journalist to gather more information by being able to contact sources they may not be able to contact in person. Yet, technology here instead of being able

[1] *See* ACLU & Human Rights Watch, *With Liberty to Monitor All: How Large Scale US Surveillance Is Harming Journalism, Law, and American Democracy* (2014) available at https://www.aclu.org/sites/default/files/assets/dem14withlibertytomonitorall07282014.pdf

to fulfill its role in promoting a robust free press is in fact creating new concerns for journalists and a chilling effect on speech.

Of particular concern to the Defending Dissent Foundation and Bill of Rights Defense Committee is the Federal Bureau of Investigation's (FBI) *Going Dark Initiative,* which this board heard about on Thursday. While both the Defending Dissent Foundation and the Bill of Rights Defense Committee inherently value privacy as a fundamental human right, our work highlights the importance of privacy to the right to dissent.

Due partially to consumer demands, private companies like Google and Apple are moving towards encrypting consumer data by default. This encryption protects important personal information, but also empowers people to speak freely and to organize for political change by safeguarding their personal privacy. In the past, the FBI has asked for built-in access to encrypted data saying current encryption policies hamper its ability to pursue terrorism investigations.

Some of the worst abuses of the First Amendment in the last thirty years, however, have been done under the guise of investigating terrorism. It was as part of a terrorism investigation the FBI spied on, infiltrated, and complied information on the Committee in Solidarity of with the People of El Salvador. A 1989 Senate Select Committee on Intelligence report found this investigation to be improper. Six FBI agents were disciplined as a result of the investigation.[2] A 2010 Department of Justice Office of the Inspector General report on FBI investigations of "domestic advocacy groups," such as the Catholic Worker Movement, Thomas Merton Center

---

[2] *See* Select Committee on Intelligence U.S. Sensate *The FBI and CISPES* (1989) available at http://www.intelligence.senate.gov/sites/default/files/publications/10146.pdf

for Peace and Social Justice, Greenpeace, and People for the Ethical Treatment of Animals, showed that such investigations were often "terrorism investigations."[3] A 2012 FOIA request revealed that the FBI monitored the Occupy Wall Street movement as a possible terrorism threat—in spite of the fact that there was no evidence to support this.[4] It is also important to note that a more recent FOIA request has revealed similar improper monitoring of the Black Lives Matter Movement by the Department of Homeland Security.[5]

Even the federal government recognizes that its surveillance is not benign. Both the Supreme Court and the Federal Elections Commission have partially exempted the Socialist Workers Party (SWP) from campaign finance disclosures due to the "long history of threats, violence, and harassment against the SWP and its supporters by Federal and local law enforcement agencies and private parties."[6] While the FBI's counter intelligence actions against the SWP may seem like ancient history, the FEC renewed this exemption in 2013 citing a continuing threat against its members.[7]

When we have discussed encryption we have tackled it from two competing interests—that of individual consumers to secure important personal information from cyber criminals and the fear that bad actors may try to conceal their actions

---

[3] *See* U.S. Department of Justice Office of the Inspector General *A Review of the FBI's Investigations of Certain Domestic Advocacy Groups* (2010) available at https://oig.justice.gov/special/s1009r.pdf
[4] *See* Partnership for Civil Justice *FBI Documents Reveal Secret Nationwide Occupy Monitoring* (2012) available at http://www.justiceonline.org/fbi_files_ows
[5] *See* George Joseph, "Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson," THE INTERCEPT (July 24, 2015 2:50 PM) available at https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/
[6] *See Brown v. Socialist Workers '74 Campaign Committee,* 459 U.S. 87 (1982); Federal Election Committee Advisory Opinion 2012-38 – Socialist Workers Party available at http://www.fec.gov/pages/fecrecord/2013/june/ao2012-38.shtml
[7] *See* Federal Election Committee Advisory Opinion 2012-38 – Socialist Workers Party

from the government. There is, however as the FEC exemption for the SWP shows, a third interest to take into consideration—individuals who want to protect their information from the government not due to their personal bad acts, but to shield themselves from the bad acts of the government.

The Supreme Court has long recognized that privacy is essential to dissent.[8] Knowing that the government may be monitoring their electronic communications activists, muckrakers, whistleblowers, journalists, and others essential to our democracy will think twice about what they type. This is why the Defending Dissent Foundation and Bill of Rights Defense Committee supports the right to encrypt information and strongly opposes any attempts by the government to erode encryption by including built-in access for the government. There is, in addition to this First Amendment concern, an inherent privacy right. On this note we recall the 1974 words of Senator Sam Ervin about the threat posed to our constitution by the government's "technical capacity to store and distribute information:"

> *Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom: the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words.*

---

[8] *See NAACP v. Alabama ex. Rel. Patterson*, 357 U.S. 449 (1958) ("*Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs"*)