JUST SECURITY
A FORUM ON LAW, RIGHTS, AND U.S. NATIONAL SECURITY

NSA Reform — The Consequences of Failure

By Patrick Eddington
November 26, 2014

If you were expecting this to be a detailed post-mortem on the demise of the USA Freedom Act, you will be disappointed. As others have covered that ground, I want to focus on the consequences of the failure to rein in NSA to date, and what a failure to do so in 2015 will mean for this country.

In the absence of real reform, people and institutions at home and abroad are taking matters into their own hands. In America, the NSA's overreach is changing the way we communicate with and relate to each other. In order to evade government surveillance, more and more Americans are employing encryption technology.

The veritable explosion of new secure messaging apps like Surespot, OpenWhisper's collaboration with WhatsApp, the development and deployment of open source anti-surveillance tools like Detekt, the creation of organizationally-sponsored "surveillance self-defense" guides, the push to universalize the https protocol, anti-surveillance book events featuring free encryption workshops— are manifestations of the rise of the personal encryption and pro-privacy digital resistance movement. Its political implications are clear: Americans, along with people around the world, increasingly see the United States government's overreaching surveillance activities as a threat to be blocked.

The federal government's vacuum-cleaner approach to surveillance—manifested in Title II of the PATRIOT Act, the FISA Amendments Act, and EO 12333—has backfired in these respects, and the emergence of this digital resistance movement is one result. Indeed, the existence and proliferation of social networks hold the potential to help this movement spread faster and to more of the general public than would have been possible in decades past. This is evidenced by the growing concern worldwide about governments' ability to access reams of information about people's lives with relative ease. **As one measure, compared to a year ago, 41% of online users in North America now avoid certain Internet sites and applications, 16% change who they communicate with, and 24% censor what they say online.** Those numbers, if anywhere close to accurate, are a major concern for democratic society.

But it's unclear that the privacy technologies offered as solutions will prove effective over the long-term. In the ongoing cat-and-mouse game between digital defenders and surveillance practitioners, it will only be a matter of time before someone finds a way around today's latest defenses, which will prompt the creation of fresh defenses. This very interaction can also chill freedom of expression and association. That is, one can imagine that every turn in this game,

including each launch of a new counter-surveillance technology, will be another reminder to individuals that their digital transactions are potentially being monitored by a government they no longer trust—and why continued efforts to keep the government out are necessary.

Even if commercially available privacy technology proves capable of providing a genuine shield against warrantless or otherwise illegal surveillance by the United States government, it will remain a treatment for the symptom, not a cure for the underlying legal and constitutional malady.

In April 2014, a Harris poll of US adults showed that in response to the Snowden revelations, "Almost half of respondents (47%) said that they have changed their online behavior and think more carefully about where they go, what they say, and what they do online." Set aside for a moment that *just the federal government's collection of the data* of innocent Americans is itself likely a violation of the Fourth Amendment. The Harris poll is just one of numerous studies highlighting the collateral damage to American society and politics from NSA's excesses: segments of our population are now fearful of even *associating* with individuals or organizations executive branch officials deem controversial or suspicious. Nearly half of Americans say they have changed their online behavior out of a fear of what the federal government might do with their personal information. **The Constitution's free association guarantee has been damaged by the Surveillance State's very operation.**

Also at risk is the First Amendment's guarantee of a free press able to investigate potential government abuses of power in the national security arena without reporters fearing that its communications are being monitored and potentially used to unmask sources.

We now live in an age where the federal government is willing to prosecute journalists in an effort to compel them to reveal their sources in national security leak cases. The most recent example is the Justice Department's multi-year legal assault on *New York Times* national security reporter James Risen. Even at the height of the Pentagon Papers case four decades ago, the Nixon administration did not go as far as the Bush 43 and Obama administrations have gone in trying to intimidate journalists into revealing their sources in national security leak cases. Since Snowden's revelations in June 2013, the climate for journalists working issues like the NSA surveillance scandal has only become more hostile.

In the preface to his new book, @War, Shane Harris notes how the executive branch's war on leakers meant that his sources

"…risked criminal prosecution in talking to me. The Obama administration has historically been hostile to government employees who share information with journalists. The Justice Department has prosecuted more people for disclosing classified information than all previous administrations combined. Simply put, it is a dangerous time to talk to journalists. And this risk extends to former government employees and military personnel. Several former intelligence officials have told me that within the past year they were explicitly told by the intelligence agencies where they're still employed as contractors that they should stop talking to journalists if they want to continue doing business with the government."

The failure of the Congress and the courts to end the surveillance state, despite the repeated efforts by a huge range of political and public interest actors to effect that change through the political process, is only fueling the growing resistance movement. Federal officials understand this, which is why they are trying—desperately and in the view of some, underhandedly—to shut down this digital resistance movement. This action/reaction cycle is exactly what it appears to be: an escalating conflict between the American public and its government. Without comprehensive surveillance authority reforms (including a journalist "shield law" and ironclad whistleblower protections for Intelligence Community contractors) that are verifiable and enforceable, that conflict will only continue.

Patrick Eddington was senior policy advisor to Rep. Rush Holt for over 10 years. He is currently a Policy Analyst in Homeland Security and Civil Liberties at the Cato Institute.