The Rest of the Snowden Files Should Be Destroyed

By Thomas Rid | Posted Tuesday, Sept. 10, 2013, at 11:13 AM
| Posted Tuesday, Sept. 10, 2013, at 11:13 AM
Slate.com

The Rest of the Snowden Files Should Be Destroyed

The leaks have done a lot of good. But a lot more damage could be done.

Edward Snowden during an interview in Hong Kong Photo by the Guardian via Getty Images

Privacy is fundamental in an open democracy. Without privacy, there is no democracy. Security is also fundamental. Without security, there is no democracy, either. This creates a dilemma: A crucial public good is pitched against a core individual right. No society can maximize both at the same time. The consequence is that we, as a society, have to agree on a compromise, a balance.

Edward Snowden's leaks revealed that America's and Britain's signal intelligence agencies are capable of intercepting vast amounts of Internet traffic, that they have developed sophisticated data-mining tools, that the agencies cooperate with the private sector in their collection effort, that they spy on allies, that the government's code breakers have cracked encryption that was previously considered safe—and more.

The *New York Times* and the *Guardian* justify this drip-drip of ongoing intelligence revelations with "the value of a public debate." But the public interest reveals itself only through a cost-benefit analysis. So are more leaks in the public interest?

The revelations have had three major benefits. The first is that an overdue debate is seriously taking off. Internet services and mobile phones are now in the hands of billions of people. Humankind has fundamentally changed how it communicates in the past two dozen years. Many are struggling with their new toys, experimenting with gadgets, tricks, and apps as they go along, perhaps picking up addictive behavior along the way. Signal intelligences agencies face similar challenges. Maybe a reform of oversight is required. Certainly 21st-century "sigint," in spy jargon, needs to be discussed by interested parties—which is everyone. This has started to happen. Congressional lawmakers are demanding more oversight of intelligence practices.

The second benefit follows from the first: The public is learning. The Snowden revelations had the unintended side effect of educating citizens as well as companies on security in the digital age. Encryption is now a household expression. Awareness of simple computer hygiene is improving. Nonexperts now know what proxy servers are. Normal users understand that they leave traces online and learn how to control them. Eighty-six percent of Internet users have removed or masked their digital footprints, a new Pew report shows.

Thirdly, tech companies now take security more seriously. Functionality and robustness was the first priority for the Internet's early architects, not security. Many software developers still don't build security in. Now, finally, firms are seriously starting to improve products and services. Google's rush to encrypt

communications between its data centers is a case in point.

So what about the costs and the downsides of the revelations?

There are several items on the list. One is that intelligence capabilities are damaged. There is no doubt that signal intelligence agencies are an essential tool necessary for international statecraft as well as for maintaining the domestic constitutional order. Revealing capabilities and tactics often means they become worthless as a result. Measuring such tactical costs is hard, but the damage is significant.

This means, secondly, that militants, violent extremists, and adversaries—think the Syrian regime—are already racketing up their communication security. In the future it will be harder to detect and foil terrorist attacks. In the future it will be harder to say if some regime possesses or used a specific weapon system. In the future it will be harder to unveil wealth-draining cyberespionage. This is very serious.

Meanwhile, thirdly, authoritarian states get a confidence boost. “Washington ate the dirt this time,” wrote China’s *Global Times*, an outlet sometimes called the Fox News of China. The U.S. administration “has long been trying to play innocent victim of cyberattacks” but now turned out to be “the biggest villain,” said Xinhua, the state-run news agency. This argument, of course, is hypocrisy. The National Security Agency is not spying in order to round up Obama's political opposition, and Government Communications Headquarters is not listening to Internet traffic to help London's banks—both of which stand in sharp contrast to China's own practices. Nevertheless, Snowden's revelations make it easier for the world's authoritarian regimes to crush dissent at home.

A fourth result: Internet governance is creaking. Diminishing America and Britain’s diplomatic and moral standing is threatening the multistakeholder approach, so far a guarantor for a free and open Internet. A patchwork of smaller, sovereign "Internets" is becoming more and more likely. As a result, the Internet could now become more authoritarian, not less.

Finally, and perhaps most significantly, American and British Internet and telecommunication companies are under economic pressure, set to lose disgruntled customers at home and large contracts abroad. This last damage multiplies all previous ones.

The bottom line is sobering: The benefits of the Snowden leaks are abstract, mediated, uncertain, and slow to take shape—the damage is concrete, immediate, certain, and adds up fast.

Some may retort that it was the NSA and its allies who created this damage in the first place, not Snowden and his allies. But this argument is problematic: Spy agencies spy, all of them. Suggesting that all secrecy is bad is plainly naïve. Instead there is a moral case to be made for open democracies to have the most capable intelligence agencies, operating lawfully with robust oversight mechanisms. No liberal mind can want the NSA to sit in Beijing or Moscow.

Yes, NSA and GCHQ may have overstepped their bounds. But that doesn’t mean that all signal intelligence is wrong. The prize question is therefore what they should be able to do and what they should not be able to do—and the answer has to be a conceptual and principled one. Revealing more programs and more details will not bring us any closer to an answer.

The stakes are monumental. Anger and a state of subdued panic prevail at NSA and at GCHQ. Spies cannot drive this debate. Neither will governments, for fear of stoking a fire and provoking even more

revelations. It is therefore the responsibility of intellectuals and public experts to add balance and nuance to a shrill debate.

So far, this is not happening. Bruce Schneier, a widely respected computer security expert, recently wrote in the *Guardian* that the NSA "broke a fundamental social contract," and then implied that revealing intelligence operations, a form of civil disobedience, would be "the moral thing to do."

As usual, the inconvenient truth is more complicated: Gauging if, and how, NSA may have broken the social contract is hard—intelligence successes, after all, are far less visible than intelligence failures. But it is easy to see that revealing more intelligence operations may indeed undermine the social contract. Sometimes protecting secrets is the moral thing to do.

Glenn Greenwald, the American journalist who first published the documents leaked by former NSA contractor Edward Snowden, testifies before a Brazilian congressional committee on NSA's surveillance programs in Brasilia, Brazil, on Aug. 6, 2013. Photo by Ueslei Marcelino/Reuters

Editors and journalists have a huge responsibility in this case. But so far, the newspapers in question have painted the false picture that NSA and GCHQ focused their collection on allies, international organizations, or even their own citizens, not the real threats in the Middle East and beyond. Scandal sells. But responsible journalism means that financially struggling newspapers should resist the temptation to abuse the Snowden files for profiteering. Responsible journalism also means that angry reporters should resist the temptation for revenge.

The *New York Times*, the *Guardian*, the *Washington Post*, and Glenn Greenwald have to make a careful consideration before revealing yet another story: Will the new details do more good than harm? Responsible journalism, in short, means making a hard moral choice: Have we reached the point at which the remaining evidence needs to be returned or destroyed, voluntarily?

It is not for activist journalists and reborn cypherpunks to decide. That decision is for the sovereign, that is, the public—in the United States and in the United Kingdom.

This article arises from Future Tense, a collaboration among Arizona State University, the New America Foundation, and ***Slate****. Future Tense explores the ways emerging technologies affect society, policy, and culture. To read more, visit the* Future Tense blog *and the* Future Tense home page*. You can also* follow us on Twitter.