Surveillance

Why We Published the Decryption Story

by ***Stephen Engelberg*** *and* ***Richard Tofel***
ProPublica, Sep. 5, 2013, 2:54 p.m.

Sept. 6: *This Closer Look has been updated with a response from the Office of the Director of National Intelligence [1].*

ProPublica is today publishing a story [2] in partnership with the Guardian and The New York Times about U.S. and U.K. government efforts to decode enormous amounts of Internet traffic previously thought to have been safe from prying eyes. This story is based on documents provided by Edward Snowden, the former intelligence community employee and contractor. We want to explain why we are taking this step, and why we believe it is in the public interest.

The story, we believe, is an important one. It shows that the expectations of millions of Internet users regarding the privacy of their electronic communications are mistaken. These expectations guide the practices of private individuals and businesses, most of them innocent of any wrongdoing. The potential for abuse of such extraordinary capabilities for surveillance, including for political purposes, is considerable. The government insists it has put in place checks and balances to limit misuses of this technology. But the question of whether they are effective is far from resolved and is an issue that can only be debated by the people and their elected representatives if the basic facts are revealed.

It's certainly true that some number of bad actors (possibly including would-be terrorists) have been exchanging messages through means they assumed to be safe from interception by law enforcement or intelligence agencies. Some of these bad actors may now change their behavior in response to our story.

In weighing this reality, we have not only taken our own counsel and that of our publishing partners, but have also conferred with the government of the United States, a country whose freedoms give us remarkable opportunities as journalists and citizens.

Two possible analogies may help to illuminate our thinking here.

First, a historical event: In 1942, shortly after the World War II Battle of Midway, the Chicago Tribune published an article suggesting, in part, that the U.S. had broken the Japanese naval code (which it had). Nearly all responsible journalists we know would now say that the Tribune's decision to publish this information was a mistake. But today's story bears no resemblance to what the Tribune did. For one thing, the U.S. wartime code-breaking was confined to military communications. It did not involve eavesdropping on civilians.

The second analogy, while admittedly science fiction, seems to us to offer a clearer parallel. Suppose for a moment that the U.S. government had secretly developed and deployed an ability to read individuals' minds. Such a capability would present the greatest possible invasion of personal privacy. And just as surely, it would be an enormously valuable weapon in the fight against terrorism.

Continuing with this analogy, some might say that because of its value as an intelligence tool, the existence of the mind-reading program should never be revealed. We do not agree. In our view, such a capability in the hands of the government would pose an overwhelming threat to civil liberties. The capability would not necessarily have to be banned in all circumstances. But we believe it would need to be discussed, and safeguards developed for its use. For that to happen, it would have to be known.

There are those who, in good faith, believe that we should leave the balance between civil liberty and security entirely to our elected leaders, and to those they place in positions of executive responsibility. Again, we do not agree. The American system, as we understand it, is premised on the idea -- championed by such men as Thomas Jefferson and James Madison -- that government run amok poses the greatest potential threat to the people's liberty, and that an informed citizenry is the necessary check on this threat. The sort of work ProPublica does -- watchdog journalism -- is a key element in helping the public play this role.

American history is replete with examples of the dangers of unchecked power operating in secret. Richard Nixon, for instance, was twice elected president of this country. He tried to subvert law enforcement, intelligence and other agencies for political purposes, and was more than willing to violate laws in the process. Such a person could come to power again. We need a system that can withstand such challenges. That system requires public knowledge of the power the government possesses. Today's story is a step in that direction.

Update (9/6): Statement from the Office of the Director of National Intelligence:

It should hardly be surprising that our intelligence agencies seek ways to counteract our adversaries' use of encryption. Throughout history, nations have used encryption to protect their secrets, and today, terrorists, cybercriminals, human traffickers and others also use code to hide their activities. Our intelligence community would not be doing its job if we did not try to counter that.

While the specifics of how our intelligence agencies carry out this cryptanalytic mission have been kept secret, the fact that NSA's mission

includes deciphering enciphered communications is not a secret, and is not news. Indeed, NSA's public website states that its mission includes leading "the U.S. Government in cryptology … in order to gain a decision advantage for the Nation and our allies."

The stories published yesterday, however, reveal specific and classified details about how we conduct this critical intelligence activity. Anything that yesterday's disclosures add to the ongoing public debate is outweighed by the road map they give to our adversaries about the specific techniques we are using to try to intercept their communications in our attempts to keep America and our allies safe and to provide our leaders with the information they need to make difficult and critical national security decisions.

---

1. #odni-response
2. http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption

---