the Atlantic

How the NSA Threatens National Security

Our choice isn't between a digital world where the agency can eavesdrop and one where it cannot; our choice is between a digital world that is vulnerable to any attacker and one that is secure for all users.

BRUCE SCHNEIER JAN 6 2014, 11:10 AM ET

Powerful systems are too easily abused. A scene from the McCarthy hearings. (Wikimedia Commons)

Secret NSA eavesdropping is still in the news. Details about once secret programs continue to leak. The Director of National Intelligence has recently declassified additional information, and the President's Review Group has just released its report and recommendations.

With all this going on, it's easy to become inured to the breadth and depth of the NSA's activities. But through the disclosures, we've learned an enormous amount about the agency's capabilities, how it is failing to protect us, and what we need to do to regain security in the Information Age.

First and foremost, the surveillance state is robust. It is robust politically, legally, and technically. I can name three different NSA programs [www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html%22] to collect Gmail user data. These programs are based on three different technical eavesdropping capabilities. They rely on three different legal authorities. They involve collaborations with three different companies. And this is just Gmail. The same is true for cell phone call records, Internet chats, cell-phone location [www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html] data.

Second, the NSA continues to lie about its capabilities. It hides behind tortured interpretations of words like "collect," "incidentally," "target," and "directed." It cloaks programs in multiple code names to obscure their full extent and capabilities. Officials testify that a particular surveillance activity is not done under one particular program or authority, conveniently omitting that it is done under some other program or authority.

Third, U.S. government surveillance is not just about the NSA. The Snowden documents have given us extraordinary details [www.tedgioia.com/nsa_facts.html] about the NSA's activities, but we now know that the CIA, NRO, FBI, DEA, and local police all engage in ubiquitous surveillance using the same sorts of eavesdropping tools, and that they regularly share information with each other.

The NSA's collect-everything mentality is largely a hold-over from the Cold War, when a voyeuristic interest in the Soviet Union was the norm. Still, it is unclear how effective targeted surveillance against "enemy" countries really is. Even when we learn actual secrets, as we did regarding Syria's use of chemical weapons earlier this year, we often can't do anything with the information.

Ubiquitous surveillance should have died with the fall of Communism, but it got a new—and even more dangerous—life with the intelligence community's post-9/11 "never again" terrorism mission. This quixotic goal of preventing something from happening forces us to try to know everything that does happen [www.schneier.com/blog/archives/2013/11/dan_geer_explai.html]. This pushes the NSA to eavesdrop on online gaming worlds and on every cell phone in the world. But it's a fool's errand; there are simply too many ways to communicate.

We have no evidence that any of this surveillance makes us safer. NSA Director General Keith Alexander responded to these stories in June by claiming that he disrupted 54 terrorist plots. In October, he revised that number downward to 13, and then to "one or two." At this point, the only "plot" prevented was that of a San Diego man sending $8,500 to support a Somali militant group. We have been repeatedly told that these surveillance programs would have been able to stop 9/11, yet the NSA didn't detect the Boston bombings—even though one of the two terrorists was on the watch list and the other had a sloppy social media trail. Bulk collection of data and metadata is an ineffective counterterrorism tool.

NSA-level surveillance is like the Maginot Line was in the years before World War II: ineffective and wasteful.

Not only is ubiquitous surveillance ineffective, it is extraordinarily costly. I don't mean just the budgets, which will continue to skyrocket. Or the diplomatic costs, as country after country learns of our surveillance programs against their citizens. I'm also talking about the cost to our society. It breaks so much of what our society has built. It breaks our political systems, as Congress is unable to provide any meaningful oversight and citizens are kept in the dark about what government does. It breaks our legal systems, as laws are ignored or reinterpreted, and people are unable to challenge government actions in court. It breaks our commercial systems, as U.S. computer products and services are no longer trusted worldwide. It breaks our technical systems, as the very protocols of the Internet become untrusted. And it breaks our social systems; the loss of privacy, freedom, and liberty is much more damaging to our society than the occasional act of random violence.

NSA-level surveillance is like the Maginot Line was in the years before World War II: ineffective and wasteful.

And finally, these systems are susceptible to abuse. This is not just a hypothetical problem. Recent history illustrates many episodes where this information was, or would have been, abused: Hoover and his FBI spying, McCarthy, Martin Luther King Jr. and the civil rights movement, anti-war Vietnam protesters, and—more recently—the Occupy movement. Outside the U.S., there are even more extreme examples. Building the surveillance state makes it too easy for people and organizations to slip over the line into abuse.

It's not just domestic abuse we have to worry about; it's the rest of the world, too. The more we choose to eavesdrop on the Internet and other communications technologies, the less we are secure from eavesdropping by others. Our choice isn't between a digital world where the NSA can eavesdrop and one where the NSA is prevented from eavesdropping; it's between a digital world that is vulnerable to all attackers, and one that is secure for all users.

Fixing this problem is going to be hard. We are long past the point where simple legal interventions can help. The bill in Congress to limit NSA surveillance won't actually do much to limit NSA surveillance. Maybe the NSA will figure out an interpretation of the law that will allow it to do what it wants anyway. Maybe it'll do it another way, using another justification. Maybe the FBI will do it and give it a copy. And when asked, it'll lie about it.

NSA-level surveillance is like the Maginot Line was in the years before World War II: ineffective and wasteful. We need to openly disclose what surveillance we have been doing, and the known insecurities that make it possible. We need to work toward security, even if other countries like China continue to use the Internet as a giant surveillance platform. We need to build a coalition of free-world nations dedicated to a secure global Internet, and we need to continually push back against bad actors—both state and non-state—that work against that goal.

Securing the Internet requires both laws and technology. It requires Internet technology that secures data wherever it is and however it travels. It requires broad laws that put security ahead of both domestic and international surveillance. It requires additional technology to enforce those

laws, and a worldwide enforcement regime to deal with bad actors. It's not easy, and has all the problems that other international issues have: nuclear, chemical, and biological weapon non-proliferation; small arms trafficking; human trafficking; money laundering; intellectual property. Global information security and anti-surveillance needs to join those difficult global problems, so we can start making progress.

The President's Review Group recommendations are largely positive, but they don't go nearly far enough. We need to recognize that security is more important than surveillance, and work towards that goal.