The NSA Recommendations: Preventing Turnkey Totalitarianism

The White House panel's recommendations for NSA reform are a start, but more needs to be done—and soon.

Ronald Bailey

December 20, 2013

This week President Barack Obama's handpicked review board recommended 46 significant changes to the way the National Security Agency (NSA) and other federal agencies spy on Americans. Many of the panel's proposals would help stop the slide toward the "turnkey totalitarian state," to borrow a phrase from the NSA whistleblower William Binney. But they won't be enough.

Five of the panel's recommendations, or groups of recommendations, are especially important. The first holds that "the government should not be permitted to collect and store mass, undigested, non-public personal information about U.S. persons for the purpose of enabling future queries and data-mining for foreign intelligence purposes." Instead, records of when, from where, to whom, and for how long Americans talk on their phones would be collected and stored by telecommunications companies or by a private consortium. The NSA and other agencies would have to seek separate judicial orders to search those databases instead of authorizing such searches themselves as they do now. Records would be held for just two years. (Some telecom companies currently hold phone records for as long as 10 years. The NSA retains them for five.)

This proposal does not do nearly enough to protect Americans' privacy. As attorney Kurt Opsahl of the Electronic Frontier Foundation points out, "Mass surveillance is still heinous, even if private company servers are holding the data instead of government data centers." Fortunately, two bills have been introduced in Congress, the USA FREEDOM Act and the Intelligence Oversight and Surveillance Reform Act, that would ban the feds from the bulk collection of Americans' phone records altogether.

Besides being unconstitutional, the NSA's dragnet collection of records was, in the review panel's words, "not essential to preventing attacks" anywhere. Americans gave up their liberty but gained no security.

A second set of recommendations involves national security letters. With such a letter, the Federal Bureau of Investigation can order the party holding an American's private communications or financial records to give them to the government; it can also impose a gag order prohibiting that party from

informing anyone that the records have been handed over. Right now, this can be done without any prior court oversight.

Under the panel's proposal, the government could not issue a national security letter unless it first shows a court that it has "reasonable grounds to believe that the particular information sought is relevant to an authorized investigation" involving "international terrorism or clandestine intelligence activities." Gag orders would be issued only "upon a judicial finding that there are reasonable grounds to believe that disclosure would significantly threaten the national security, interfere with an ongoing investigation, endanger the life or physical safety of any person, impair diplomatic relations, or put at risk some other similarly weighty government or foreign intelligence interest." Instead of being essentially perpetual, as they are now, those non-disclosure orders would remain in effect for no longer than 180 days, unless extended by judicial re-approval. Furthermore, the recipients of gag orders would be able to challenge them in court. And federal agencies would have to disclose detailed data to the American people about how much information they are collecting in the name of national security.

All of this would be an improvement on the status quo. But the "reasonable grounds" standard is not stringent enough. Government agencies should be required to obtain a warrant based on probable cause before being permitted to rifle through Americans' private information. Defenders of national security letters claim the lesser standard is needed to "appropriately and efficiently investigate threats to the national security...without alerting the targets that it is doing so." Critics counter, compellingly, that field agents have issued tens of thousands of these letters on the mere assertion that the data they are demanding is "relevant" to an investigation, even if the person whose records are being taken is not suspected of any wrongdoing.

A third group of recommendations would reorganize how the NSA is governed. The panel proposes that the agency's director should be confirmed by the Senate and that civilians should be eligible to hold the position. The panel also suggested that the NSA director should not also head the U.S. Cyber Command.

Obama has already rejected these ideas. That's too bad, because they would be significant improvements. "Even though the overwhelming majority of intelligence activities, personnel, and funding are military, the intelligence process remains an inherently political activity and therefore needs civilian input," Pace University law professor Mark Shulman explained in a 2012 paper. "The nation does not have meaningful civilian control over the military intelligence apparatus," he added, "if its civilian leaders are retired generals." As for Cyber Command, it deploys offensive capabilities, whereas the NSA's intelligence gathering is supposed to be primarily defensive.

The panel's fourth major recommendation is for Congress to create the position of public interest advocate, whose job would be to represent privacy and civil liberties interests in proceedings before the Foreign Intelligence Surveillance Court. The advocate could be housed in a strengthened Civil Liberties and Privacy Protection Board, which would be an authorized recipient for whistleblower complaints related to privacy and civil liberties. (Be that as it may, nearly a quarter of the review panel's recommendations were aimed at making sure that there will be no future Edward Snowdens.)

The fifth salient recommendation is that the NSA be forbidden to engineer vulnerabilities into the encryption algorithms that guard global commerce and that the agency be precluded from demanding changes in any product to ease the clandestine collection of information. Such activities have already undermined trust in the security of telecommunications and data storage around the globe.

At the Cato Institute's conference on NSA surveillance in October, Harvard Berkman Center fellow Bruce Schneier noted that a "secure Internet is in everyone's interests. We are all better off if no one can do this kind of bulk surveillance. Fundamentally, security is more important than surveillance." At the same conference, Matt Blaze, an Internet security professor at the University of Pennsylvania, observed that maintaining vulnerabilities in computer code doesn't just make it easier for the NSA to spy; it makes it easier for the Chinese, Russians, and Iranians to spy, and for Internet criminals to steal data and cause other havoc.

If there is another significant terrorist attack, the report's authors warn, "many Americans, in the fear and heat of the moment, might support new restrictions on civil liberties and privacy." They add, "The powerful existing and potential capabilities of our intelligence and law enforcement agencies might be unleashed without adequate controls. Once unleashed, it could be difficult to roll back these sacrifices of freedom." Turnkey totalitarianism could become a reality. The time to stop that possibility is now.