NationalJournal

Edward Snowden is Completely Wrong

Whether he's a hero or traitor, Americans are already so acclimated to the loss of privacy that his revelations won't unnerve them much.

By Michael Hirsh & Sara Sorcher – June 14, 2013

Is he a hero—the most important whistle-blower in U.S. history, as Pentagon Papers leaker Daniel Ellsberg called him? Or is Edward Snowden a flat-out traitor and a very deluded young man? The 29-year-old contractor at the center of the biggest national security scandal in years is eloquent and impressively intelligent, having risen from high school dropout and security guard at the National Security Agency to uber systems administrator at the CIA. Snowden also appears to have acted genuinely out of conscience, because it's clear he could have sold what he knows for quite a lot of money, taken down "the surveillance structure in an afternoon" (as he declared in an interview), or revealed undercover assets that might "have cost lives. Instead, Snowden, a product of the federal government ecosystem who grew up in the D.C. suburbs, says he has sacrificed his own "very comfortable" life to expose what he calls Washington's "architecture of oppression."

What's not clear is why Snowden thought that revealing the NSA's surveillance methods would change very much in our government or society, except to make it much harder for the NSA, the CIA, and defense and intelligence contractors to hire anyone like him in the future.

That process, if little else, must now change. Snowden will likely be charged with espionage, or worse. Washington will massively revamp its vetting procedures, especially for giant contractors such as Booz Allen Hamilton, which has grown fat on a diet of government work and appeared to hire Snowden in Hawaii at a generous salary of $120,000 almost as an afterthought. Contracts like the one he worked on—to help the government analyze an overwhelming stream of data—represented 99 percent of its revenue, most of them related to the NSA.

Other than tightened security clearances, though, the startling revelations of the past several days will probably alter very little in the lives of Americans or the way the government works in a data-driven world. That's not just because, apart from a few outraged senators—Democrats Ron Wyden of Oregon and Mark Udall of Colorado and libertarian Republican Rand Paul of Kentucky—almost the entire U.S. government, from the White House to Congress to the judiciary, has come out in support of the NSA program of collecting troves of telephone data and personal Internet information, using the servers and telecommunications systems of America's biggest companies. If the mandarins of official Washington don't amend their conduct, it's because Americans aren't asking them to.

A NEW CONCEPT OF PRIVACY

The reason may not be entirely obvious at first. In the past decade, our very concept of privacy has changed to the point that we're less likely to see information-sharing as a violation of our personal liberty. In an era when our daily lives are already networked, we have E-ZPasses that give us access to the fast lane in exchange for keeping the government informed about where we drive. We shop online despite knowing that the commercial world will track our buying preferences. We share our personal reflections and habits not only with Facebook and Google but also (albeit sometimes inadvertently) with thousands of online marketers who want our information. All of this means Americans are less likely to erupt in outrage today over one more eye on their behavior. "One thing I find amusing is the absolute terror of Big Brother, when we've all already gone and said, 'Cuff me,' to Little Brother," jokes John Arquilla, an intelligence expert at the Naval Postgraduate School in Monterey, Calif.

The latest Allstate/National Journal Heartland Monitor Poll bears this out. Americans are vaguely aware of these slowly eroding walls of privacy, and 55 percent say they are worried about the overall accumulation of personal information about them "by businesses, law enforcement, government, individuals, and other groups." The survey also found that an overwhelming majority of Americans believe that business, government, social-media sites, and other groups are accessing their most personal information without their consent. Even so, for the most part, they accept it as an unavoidable modern phenomenon. Most younger and college-educated people—in contrast to Snowden—take a benign view of these changes.

Despite the press treatment of the NSA story, which judging from editorial opinion has come out largely on Snowden's side, most Americans appear relatively unperturbed. A Pew Research Center/Washington Post poll conducted last weekend found that 56 percent of Americans believe NSA access to the call records of millions of Americans is an "acceptable" way for the federal government to investigate terrorism. An even bigger majority, 62 percent, said it was more important for the government to investigate terrorist threats than it was to safeguard personal privacy. That explains why soft queasiness has not congealed into hard political outrage.

Another problem for the alarmists: No evidence suggests that the worst fears of people like Snowden have ever been realized. In his interview with The Guardian, which broke the story along with The Washington Post, Snowden warned that the NSA's accumulation of personal data "increases every year consistently by orders of magnitude to where it's getting to the point where you don't have to have done anything wrong. You simply have to eventually fall under suspicion from somebody."

In a state with no checks and balances, that is a possibility. But even the American Civil Liberties Union, which has called NSA surveillance "a stone's throw away from an Orwellian state," admits it knows of no cases where anything even remotely Orwellian has happened. Nor can any opponent of NSA surveillance point to a Kafkaesque Joseph K. who has appeared in an American courtroom on mysterious charges trumped up from government surveillance. Several civil-liberties advocates, asked to cite a single case of abuse of information, all paused for long seconds and could not cite any.

There is also great misunderstanding about how the NSA system works and whether such abuse could even happen in the future. It's unclear if the government will be capable of accessing and misusing the vast array of personal data it is accumulating, as Snowden predicts. The NSA appears primarily to use computer algorithms to sift through its database for patterns that may be possible clues to terrorist plots. The government says it is not eavesdropping on our phone calls or voyeuristically reading our e-mails. Instead, it tracks the "metadata" of phone calls—

whom we call and when, the duration of those conversations—and uses computer algorithms to trawl its databases for phone patterns or e-mail and search keywords that may be clues to terrorist plots. It can also map networks by linking known operatives with potential new suspects. If something stands out as suspicious, agents are still required by law to obtain a court order to look into the data they have in their storehouses. Officials must show "probable cause" and adhere to the principle of "minimization," by which the government commits to reducing as much as possible the inadvertent vacuuming up of information on citizens instead of foreigners—the real target of the NSA's PRISM program. The program, according to Director of National Intelligence James Clapper, has had success. He told NBC that tracking a suspicious communication from Pakistan to a person in Colorado allowed officials to identify a terrorist cell in New York City that wanted to bomb its subway system in the fall of 2009.

Indeed, the scandal is perhaps narrower in scope than it's made out to be. "The only novel legal development that I see in that area is the government says, 'We know there's relevant information in there—if we don't get it now it will be gone; we won't be able to find it when we need it. So we'll gather it now and then we'll search it only when we have a good basis for the search to be done,' " says Stewart Baker, who was the first assistant secretary for policy at the Homeland Security Department and is a former NSA general counsel. "The courts are still involved. They say, 'You put it in a safe place, lock it up, come to me when you want to search it.' If you're serious about ways to make [counterterrorism] work and still protect privacy, it seems like a pretty good compromise."

Baker says the government built in as many controls and oversights as it could think of. "Two different presidents from two different parties with very different perspectives. Two different Intelligence committees led by two different parties. A dozen judges chosen from among the life-appointed judiciary. None of them thought this was legally problematic," Baker says. "And one guy says, 'Yeah, I disagree, so I'm going to blow it up.' If the insistence is, 'It only satisfies me if it's out in public,' then we're not talking about intelligence-gathering. We're not even talking about law enforcement. We're talking about research. And I'm not sure you can run a large country in a dangerous world just by doing open-source research."

Other advocates of the NSA operation say the sheer vastness of the program is what helps shield citizens. "Individuals are protected by the anonymity granted by the quantity of information," says Eric Posner, a University of Chicago law professor. "It's just too difficult to spy on such a vast number of people in a way that's meaningful."

THE CULTURE OF INTRUSION

Behavioral research shows that, like the proverbial frog in the pot of water who doesn't notice the rising temperature, Americans have grown inured to the "culture of intrusion" in today's world of continuous data exchange. "There are undeniable changes in behavior we have been observing in the past 10 years or so, with the birth and rise of social media," says Alessandro Acquisti, an economist at Carnegie Mellon University who has studied the effects. "There is evidence that people will give away personal data for very small rewards, such as the psychological benefit of sharing with others, or even for a discount coupon," he says. "For instance, on social media, people quite openly talk, without containing their audience only to their Facebook friends, about dating, eating, going out, success, and failures—something that 10 years ago you would have disclosed only to your direct friends."

The Michigan-based Ponemon Institute, which conducts independent research on privacy and data collection, has found that a relatively small number of Americans, only about 14 percent,

care enough about their privacy on a consistent basis to change their behavior to preserve it. These are the people who will not buy a book on Amazon because they would have to surrender information about themselves, or don't go to certain websites if they fear they're going to be behaviorally profiled, or won't contribute to political campaigns for the same reason. By contrast, a substantial majority of Americans, about 63 percent, say they care about their privacy, but "there's no evidence to suggest they're going to do anything different to preserve it," says Larry Ponemon, who runs the institute. (Some 23 percent care so little about the issue they are known as "privacy complacent," Ponemon says.)

People are blithe even as they discover how much their online behavior can hurt them personally, on everything from job and college applications to terrorist investigations. "People are losing jobs because of things they posted on their Facebook page," says Loren Thompson, chief operating officer of the Lexington Institute, who refuses to use Facebook or Twitter or even conduct potentially controversial searches on Google. "I just had a feeling all along that by the time people realized how vulnerable they were, it would be too late. There would be too much information about them online."

There is a difference, to be sure, between government and private-sector abuses of privacy. "Even I recognize that it's one thing for Google to know too much, because they aren't putting me in jail. It's another thing for government, because they can coerce me," says Michael Hayden, who as director of the NSA from 1999 to 2006 was a primary mover behind the agency's transformation from Cold War dinosaur to a post-9/11 terror-detection leviathan with sometimes frightening technical and legal powers. "But if we weren't doing this, there would be holy hell to raise."

That is likely true, too. Defenders of the program say, as Hayden does, that the government had no choice. "This is about taping foreign telecommunications transmissions that just happen to pass through the United States because of the way the Internet architecture is designed," Thompson says. "It really doesn't have anything to do with spying on Americans; it's about spying on foreigners the easy way." At first this meant finding the right communications hardware. The USS Jimmy Carter, a Seawolf-class submarine, was modified to tap into the trunk lines, but there are really only a handful of major Internet conduits to the Middle East, Thompson says. Eventually, someone probably said, "Jeepers, most of this traffic passes through the U.S. anyway. Why don't we just talk to Verizon?"

Hayden admitted this, surprisingly, in an open session of the House Intelligence Committee way back in 2000, telling the members that this monitoring was needed to enable the NSA to get in front of the data. No one listened right way, but after 9/11 and the passage of the USA Patriot Act, the mood shifted dramatically in favor of more aggressive surveillance. "This agency grew up in the Cold War. We came from the world of Enigma [the Nazi encryption device whose code was broken by the Allies], for God's sake. There were no privacy concerns in intercepting German communications to their submarines, or Russian microwave transmissions to missile bases," Hayden says today. Now, "all the data you want to go for is coexisting with your stuff. And the trick then, the only way the NSA succeeds, is to get enough power to be able to reach that new data but with enough trust to know enough not to grab your stuff even though it's whizzing right by." The demonization of the NSA now is ironic, he says, considering that in late 2002 the Senate Intelligence Committee (which included Wyden), in its joint 9/11 report with the House, criticized the agency for its "failure to address modern communications technology aggressively" and its "cautious approach to any collection of intelligence relating to activities in the United States."

Most Americans, based on the polls, seem willing to make the trade-off between what President Obama called "modest encroachments on privacy" and safety from terrorists. "There is a lot of authoritarian overreach in American society, both from the drug war and the war on terror," David Simon, the writer and producer of the hit HBO shows The Wire and Treme, wrote in his blog this week, in a scathing blast at Snowden and the pundits who have lionized him. "But those planes really did hit those buildings. And that bomb did indeed blow up at the finish line of the Boston Marathon. And we really are in a continuing, low-intensity, high-risk conflict with a diffuse, committed, and ideologically motivated enemy. And for a moment, just imagine how much bloviating would be wafting across our political spectrum if, in the wake of an incident of domestic terrorism, an American president and his administration had failed to take full advantage of the existing telephonic data to do what is possible to find those needles in the haystacks."

HOW WE SURRENDER PRIVACY

Every time you go online, you're a target. Advertisers are searching for you—maybe not by name, but through your interests and your assessed income and even your health symptoms, all based on your search-engine terms and the cookies deposited on your computer to watch you surf the Internet and report back on your habits. Sites may have an agreement with advertisers, which can target their messages to you. And they likely sell this information to third-party brokers who can do what they want with it.

A sweeping Wall Street Journal investigation in 2010 found that the biggest U.S. websites have technologies tracking people who visit their pages, sometimes upwards of 100 tools per site. One intrusive string of code even recorded users' keystrokes and transmitted them to a data-gathering firm for analysis. "A digital dossier over time is built up about you by that site or third-party service or data brokers," says Adam Thierer, senior research fellow at the Mercatus Center's Technology Policy Program at George Mason University. "They collect these data profiles and utilize them to sell you or market you better services or goods." This is what powers the free Internet we know and love; users pay nothing or next to nothing for services—and give up pieces of personal information for advertisers in exchange. If you search for a Mini Cooper on one website, you're likely to see ads elsewhere for lightweight, fuel-efficient cars. Companies robotically categorize users with descriptions such as "urban upscale" to "rural NASCAR" to tailor the advertising experience, says Jim Harper of the libertarian Cato Institute. "They'll use ZIP codes and census data to figure out what their lifestyle profile is."

As a result of these changes, the government's very concept of privacy has grown ever narrower and more technical. "Too often, privacy has been equated with anonymity; and it's an idea that is deeply rooted in American culture," Donald Kerr, the principal deputy director of national intelligence, said in 2007 as Congress was busy debating new rules for government eavesdropping. That's quickly fading into history, Kerr said. The new version of privacy is defined by enough rules affecting the use of data that Americans' constitutionally enumerated rights (privacy not among them) will be safe. "Protecting anonymity isn't a fight that can be won. Anyone that's typed in their name on Google understands that." We've already given up so much privacy to the government, Kerr said back then, that it can be protected only by "inspectors general, oversight committees, and privacy boards" that have become staples of the intelligence community.

Clapper seems to be relying on a similar concept. The United States, he said in an interview with NBC, can put all the communications traffic that passes through the country in a massive metaphorical library. Presumably, the "shelves" contain the phone numbers of Americans, the

duration of their calls, and their e-mail correspondence. “To me, collection of U.S. persons’ data would mean taking the book off the shelf, opening it up, and reading it,” Clapper said. Instead, the government is “very precise” about which “books” it borrows from the library. “If it is one that belongs or was put in there by an American citizen or a U.S. person, we are under strict court supervision, and have to get permission to actually look at that. So the notion that we’re trolling through everyone’s e-mails and voyeuristically reading them, or listening to everyone’s phone calls, is on its face absurd. We couldn’t do it even if we wanted to, and I assure you, we don’t want to.”

Critics say the Constitution’s Fourth Amendment, designed to guard against unreasonable searches and seizures, should impede the government’s access to personal data—even if that information is available in the commercial sphere. “If Google has it, that says nothing about whether the government should have it,” says Cato’s Harper. “It’s not reasonable to collect information without probable cause or reasonable suspicion.”

For most Americans, the reassurance that the government won’t gratuitously pursue them may well be enough. For Snowden and his defenders, it clearly is not. In explaining his daring act, he said he hoped to provoke a national debate about surveillance and secrecy, and added: “The greatest fear that I have regarding the outcome for America of these disclosures is that nothing will change.”

That fear is likely to be realized. Snowden offered a valuable window into a top-secret world The Washington Post wrote about in great detail three years ago, when it published a series on a clandestine intelligence-industrial complex that “has become so large, so unwieldy, and so secretive that no one knows how much money it costs, how many people it employs, how many programs exist within it, or exactly how many agencies do the same work.” Perhaps the country should thank Snowden for reopening that issue, even as it prosecutes him for what is plainly a violation of his oath of secrecy. But after the thanks are offered, we will probably just get back to business.