theguardian

Snowden showed us just how big the panopticon really was. Now it's up to us

By: Julian Sanchez
June 5, 2014

The scale of the surveillance industrial complex turned out to be so vast that even the NSA couldn't comprehend all the rules it was breaking. One year later, we can finally examine not just the code-named programs but the future of information itself

America's first real debate about the 21st century surveillance state began one year ago. There had, of course, been no previous shortage of hearings, op-eds and panels mulling the appropriate "balance between privacy and security" in the post-9/11 era. But for the masses who lacked a security clearance, these had the character of a middle school playground conversation about sex – a largely speculative discussion among participants who'd learned a few of the key terms, but with only the vaguest sense of the reality they described. Secrecy meant abstraction, and in a conflict between abstract fears and the all-too-visible horror of a burning skyscraper, there could be little question which would prevail. The panoptic infrastructure of surveillance developed well out of public view.

A more meaningfully informed public debate finally became possible via a series of unprecedented disclosures about the global surveillance apparatus operated by the National Security Agency – disclosures for which the word "leak" seems almost preposterously inadequate. It was a torrent of information, and it gave even the most dedicated newshounds a glimmer of what intelligence officials mean when they complain about "drinking from the fire hose" of planet-spanning communications networks.

The fountainhead of this stream of revelations, a young former contractor named Edward Snowden, declared himself to be motivated by a "reasonable fear of omniscient State powers kept in check by nothing more than policy documents." It is a telling formulation, because it concedes at the outset the point on which intelligence officials invariably insist: that there are rules and procedures, safeguards and oversight mechanisms, meant to guarantee that the vast quantities of information ingested by the NSA and its global partners are used only for good purposes. The question remains whether, once the astonishing scope of the spy machine is comprehended, those fetters begin to seem somewhat decorative – and if so, what we can do about it.

'Everything changed'

Above the doorway to the CIA's Counterterrorism Center hangs a sign meant to remind Langley's employees of the urgency of their mission – a sign that reads: "Today's date is September 12, 2001." In one respect, for all the hearings and blue-ribbon panels, the fresh dumps of documents and the legislative proposals, the date remains June 6, 2013 – and our public debate (at least within the United States) remains fixated on the very first program revealed by the Guardian using Snowden's trove of documents: the NSA's bulk collection of telephone metadata.

Though USA Today had reported on an earlier version of the program in a single 2006 article, it is not hard to see why the Guardian story was so explosive. There, in black and white, was something vanishingly few people had ever laid eyes on:a classified order from the Foreign Intelligence Surveillance Court (FISC) requiring a single telecommunications provider, Verizon, to provide "all call detail records" on a continuous basis, whether they concerned international calls or those "wholly within the United States, including local telephone calls." Other major carriers, we soon learned, had been receiving similar orders for years.

It had the ideal mix of ingredients to ignite public controversy. Beyond providing that first tantalizing glimpse of forbidden texts, it was unambiguous confirmation of privacy advocates' worst fears: the NSA, traditionally barred from deploying its unparalleled signals intelligence capabilities domestically, had been vacuuming up sensitive data about millions of ordinary citizens with no known connection to terrorism or espionage, in a program institutionalized with the blessing of the FISC. Unlike many later Snowden stories, this one involved technology familiar to all but the most dedicated Luddites.

Moreover, it gave the first hint of that Court's extraordinary secret interpretation of the government’s authority under section 215 of the Patriot Act – one that stunned and outraged even the law's co-author, Rep James Sensenbrenner. Language permitting the FBI to obtain documents "relevant to an investigation" – a phrase used in several related authorities – could be used to acquire entire databases of information in order to sift through them for the tiny fraction of records pertaining to investigative targets and their associates. To many, it seemed like the dictionary definition of an impermissible "fishing expedition". At least one federal judge would ultimately conclude that the NSA program was not just statutorily but constitutionally suspect – too vast and potentially intrusive in scale to fall within the scope of a 1979 Supreme Court opinion that had blessed far more limited collection of phone records without a Fourth Amendment search warrant.

The 215 telephony program is also the one about which we have learned, by far, the most additional details since its initial exposure – through a combination of disclosures from the government itself, both voluntary and legally compelled, as well two thorough investigative reports produced by two independent expert panels: a handpicked review group appointed by President Obama and the long quiescent Privacy and Civil Liberties Oversight Board (PCLOB) established by federal statute.

Initial assurances from the government that the telephony program was both strictly supervised and vital to security fared poorly in light of these subsequent disclosures – continuing a disturbing pattern that has emerged over the past decade. The fact that a 29-year-old contractor had been able to walk out with tens of thousands of the NSA's most highly classified secrets should already, of course, have raised questions about the efficacy of internal controls. But a 2009 opinion from the FISC also made clear that the agency’s official overseers had little independent ability to monitor whether the rules were being followed. Three full years after the telephony program began, officials acknowledged that it had never actually operated as it had been described to the court. The rules the FISC had imposed to limit access to this vast trove of sensitive records, as the understandably irate opinion put it, "have been so frequently and systematically violated that it can fairly be said that this critical element of the overall regime has never functioned effectively."

Dramatic defenses of the program’s value soon began to collapse as well. A thorough inquiry by the PCLOB determined that the program had “shown only limited value,” and in the dozen or so cases where it had played some role in a successful investigation, “simply mirrored information about telephone connections that the FBI developed independently using other authorities.” Far from being instrumental in foiling multiple terrorist plots, as some defenders originally suggested, the NSA program had served as a “catalyst” in exactly *one* investigation, involving not bombs but the transfer of funds to the Somali terror group Al Shabaab. Even in that lone case—the “strongest success story” produced by the program after seven years—the PCLOB concluded that neither the NSA’s vast compendium of records nor its analytic speed were essential to the discovery of the suspect. The FBI, in other words, could have gotten their man by traditional, targeted means.

One of Snowden's great fears one year ago was that nothing would change as a result of his disclosures – that the public would greet them with a shrug, or at any rate, with insufficient outrage to overcome the inertia of a Congress where the NSA’s allies controlled the intelligence committees. With respect to this one program, that fear has been at least partly dispelled. President Obama has ordered the NSA to seek specific judicial orders before querying its existing database, and the USA Freedom Act, legislation requiring the use of "specific identifiers" in government demands for information under a range of intelligence authorities, has already passed the House of Representatives. Already, then, we have powerful confirmation that surveillance*secretly* approved by "all three branches of government", as its defenders never tired of reminding us, will not necessarily pass muster with the public.

Yet it is hard to believe that an end to completely indiscriminate bulk collection – under certain authorities, at least – is all the change Snowden hoped to achieve, and the reforms approved by the House thus far have fallen well short of the hopes of privacy advocates.

Slouching toward reform

When the USA Freedom Act was unveiled at a Cato Institute conference in October 2013, it set civil libertarian hearts aflutter with its ambition. It not only required that demands for records show at least an indirect connection to a suspected foreign agent, but it also implemented an array of procedural changes designed to check the secret expansion of surveillance authorities. Critically, it imposed new limits on large-scale collection of international communications under section 702 of the Fisa Amendments Act. But by the time the bill made its way to a floor vote, it had been so thoroughly compromised that many civil liberties groups and technology companies pulled their support.

Though some of the procedural and transparency reforms in the original bill survive in a severely diluted form, the current version jettisoned changes to other surveillance powers in order to focus squarely on barring indiscriminate collection of records. And where the original bill accomplished this by putting teeth into the requirement of "relevance to an investigation", the current version leaves the FISC’s broad understanding of that phrase untouched, instead requiring the use of vaguely defined "specific identifiers". With sufficient chutzpah, the government might simply hand the court a stack of telephone directories – or, more plausibly, use extremely broad "identifiers" such as domain names or ranges of internet protocol addresses to enable “targeted” collection of records about communications to or from entire websites or corporate entities, such as the few remaining major internet service providers.

The bill even includes a novel authority designed to recreate the NSA's telephony program in a more limited and judicially supervised form, with the compelled "technical assistance" of telephone carriers. This does at least mean that records will generally be left in private hands pending a specific request approved by the FISC. But it also opens the door to demands that carriers redesign their own systems to enable more sophisticated types of searches, utilizing a broader array of personal information than the NSA was previously obtaining. Where the FISC had stopped short of permitting the NSA to acquire the increasingly precise location information that can be derived from cell phone logs, for instance, it remains unclear whether this new authority could be used to compel the production of people "linked" to a suspect by physical proximity rather than direct contact.

However optimistic we choose to be about the likely effects of legislation like USA Freedom, however, it was not any one legally dubious program that Snowden cites as his motive for abandoning his life and career, a decision that landed him in exile in Russia. It was a total architecture of monitoring – divided for legal and clerical convenience into discrete code-worded programs, but functionally operating as an integrated apparatus of surveillance whose true capabilities are more than the sum of its subsystems, and which may be flexible enough to simply route around the disruption of any individual data source.

If we care about seriously assessing the warning Snowden purports to offer, we need to scrutinize the full range of capabilities we've learned about, not only as freestanding programs, but as nodes in a network of information gathering and analysis. We're then in a position to ask whether the design and aims of the system as a whole are compatible with a free society.

Collect it all

Two elementary facts – one strategic, one technological – have driven the design of all the programs that the journalists with access to the Snowden documents have disclosed.

The first is that, as Sen Lindsey Graham put it, "people are trying to come to our nation and kill us, and we need to find out what they're up to before they do it. They have to be right only one time. We have to be right all the time." Foreign intelligence has always been about anticipating the actions of adversaries – but with the attacks on the World Trade Center and the Pentagon, it became imperative to anticipate the identity of the adversary as well, with no margin of error considered small enough to tolerate. It was not enough to monitor known threats; the intelligence community was ordered to foresee unknown threats, from individuals and small groups no less than states, and these threats could materialize nearly anywhere.

The second basic fact is that modern communications networks obliterate many of the assumptions about the importance of geography that had long structured surveillance law. A "domestic" internet communication between a user in Manhattan and a server in Palo Alto might, at midday in the United States, be routed through nocturnal Asia's less congested pipes, or to a mirror in Ireland, while a "foreign" e-mail service operated from Egypt may be hosted in San Antonio. "What we really need to do is all the bad guys need to be on this section of the internet," former NSA director Keith Alexander likes to joke. "And they only operate over here. All good people operate over here. All bad guys over here." It's never been quite that easy – but General Alexander's dream scenario used to be closer to the truth. State adversaries communicated primarily over dedicated circuits that could be intercepted wholesale without much worry about bumping into innocent Americans, whereas a communication entering the United States could generally be presumed to be *with* someone in the United States. The traditional division of intelligence powers by physical geography – particularized warrants on this side of the border, an interception free-for-all on the other – no longer tracks the reality of global information flows.

What NSA documents themselves describe as a "collect it all" approach to signals intelligence is an understandable reaction to these two facts. If a national security threat could come from anyone, it's necessary to track everyone. If their communications can flow anywhere, you want to be able to collect everywhere. Thus "Alexander's strategy is the same as Google's," as a former colleague told Foreign Policy's Shane Harris: "I need to get all of the data. If he becomes the repository for all that data, he thinks the resources and authorities will follow."

This broad perception of the intelligence mission has natural consequences for the security and privacy of all users. It's no longer sufficient to focus on cracking the bespoke cryptographic systems used by foreign states, because now everyone relies on encryption, whether they know it or not. Thus the aggressive Bullrun program which seeks to "insert vulnerabilities into commercial encryption systems, IT systems, networks and endpoint communications devices used by targets," and "covertly influence" the design of widely used software to ensure in advance there’s no communication the NSA can’t read.

In a very literal sense, then, network infrastructures themselves have become the agency's primary targets. When they"re abroad, that might mean "hunting sysadmins", who hold the "keys to the kingdom" on foreign networks, or implanting back-doors on tens of thousands of routers designed to handle an entire network’s traffic. Domestically, it might mean using the relationships developed with major technology companies under the Prism program, authorized under the Fisa Amendments Act of 2008, not only to rapidly collect on specific foreign users, but to influence the design of online services to render them tappable – which is to say, insecure – by default.

Though the "collect it all" approach may have been motivated chiefly by the desire to identify and anticipate terrorists, wholesale collection capabilities will clearly not remain confined to that purpose once they have been created. An astonishing program known as Somalget, for instance, reportedly records *nearly every cell phone call* in … the Bahamas. The rationale for this mindboggling universal wiretap? Not to catch beachcombing jihadis, but to aid in the war on drugs.

One of the most disturbing manifestations of the imperative to control infrastructure is the system known as Turbine, an industrial scale delivery system for targeted exploitation that now appears to live right on the internet backbone itself. Scanning the vast stream of Internet traffic, a suspicious user's web browsing session can be automatically hijacked to install malware that allows the NSA to log every action a user takes on their device, or even activate cameras and microphones, transforming smartphones and laptops into remotely operated bugs on a massive scale.

The government's ability to compel the assistance of domestic companies aids subsequent collection on foreign networks, whether under the general warrants provided for by the Fisa Amendments Act or the still broader authority of Executive Order 12333. Likewise, the agency's relatively free hand when collecting data abroad can enable de facto bulk collection at home under nominally targeted authorities designed for domestic use.

The government has insisted, for example, that the companies with which the NSA partners under the Prism program don't simply permit intelligence agencies to troll through their systems and servers hunting for malefactors: they provide the government with user data only in response to targeted requests that use a specific "hard selector" like an e-mail address or user ID. But those "hard" selectors may be derived from analysis of far vaster interception acquired *from the very same companies* without their knowledge, under programs like Muscular, at overseas data links. Alternatively, the NSA might feed bulk-collected foreign web traffic through a tool like XKeyscore, which allows the agency to filter communications using more abstract characteristics, or "soft selectors”"such as language, location, or software configuration. What looks like targeted collection under a program like Prism may simply be the final step in a process that, considered as a whole, employs specific target identifiers as an intermediary step in what is functionally algorithmic or pattern-based surveillance.

As has become all too clear from the programs that have received the greatest scrutiny to date, the scale and complexity of these interdependent mechanisms for collection an analysis make them opaque even to the spy agencies themselves – and so, a fortiori, to their assigned overseers. It appears that violations of the rules are discovered only when the NSA itself deigns to report them – sometimes years after the fact.

That's especially disturbing given the vastly increased scale and speed with which surveillance capabilities could be turned to inappropriate ends. Technologies to enable the most intrusive forms of wholesale monitoring, once directed exclusively overseas, are now installed at the heart of our domestic communications infrastructure. And the massive troves of metadata collected under a wide variety of authorities – with varying degrees of oversight – give the intelligence community enormous flexibility in targeting those surveillance technologies.

The result is that we've achieved an unprecedented kind of economy of scale in surveillance. Just as a song can now be sent to a single user or to thousands at essentially the same cost, surveillance systems can be tasked with thousands of new targets – or categories of targets – almost instantaneously.

It is a stroke of historical good fortune that J Edgar Hoover's seemingly unbounded willingness to deploy his surveillance powers against domestic political dissidents at least faced technical constraints. Having bugged the offices of the Southern Christian Leadership Congress did not render it any cheaper or easier to bug the next hotel room Dr Martin Luther King Jr checked into: time and resources had to be invested on each occasion.

Infrastructural surveillance is another matter. If a system is technically capable of rapidly collecting the Gmail inboxes of foreigners who frequent jihadist websites, then it is apt to be technically capable of doing the same for Americans who are active on Tea Party or Occupy forums. Tweaking a few lines of code will transform one system into the other.

If we care above all about avoiding that scenario, then perhaps the most significant change wrought by the Snowden disclosures to date has not been the policy proposals it has inspired – which, however vital, tend to focus on rules rather than architectures – but in the way it has transformed the incentives of the technology companies that maintain those architectures. Under cover of secrecy, the few within those companies who understood what was happening had little motive to draw attention to it, to do anything other than quietly comply – even if they had legally been permitted to do so. Exposure has inverted those incentives: Silicon Valley now stands to lose tens of billions in revenue unless it acts to regain the dwindling trust of its global user base.

Thus, America's largest tech companies quickly banded together to demand greater transparency about the scope of surveillance – an essential safeguard against any abrupt and major expansion of collection. They also began making individual changes to their systems, encrypting the links between their data centers to forestall wholesale interception. As a Snowdenversary present, Google even announced that it will introduce strong, user-friendly end-to-end encryption for its wildly popular Gmail service – a design choice that would render them incapable of handing over the keys needed to read user messages. None of these changes are likely to stop the NSA if it is determined to spy on particular targets, but they do help raise the cost of the indiscriminate mass surveillance that poses the greatest threat to democracy.

We cannot, however, rely on Silicon Valley to avoid hard policy choices: the security they now enhance, they can ultimately be ordered to help undermine. Armed at last with a fuller understanding of the surveillance systems our intelligence agencies have been building, it falls to us to assess whether they are truly so necessary to our security that they justify their inherent risks. And the question we should ask about such systems is the question we should ask about, say, biological weapons: not whether we are satisfied with how (as far as we know) they are currently being used, but whether the consequences of their misuse are so great that, if and when it occurs, it will be too late to do much about it.

-Julian Sanchez is a senior fellow at the Cato Institute who studies issues at the busy intersection of technology, privacy, and civil liberties, with a particular focus on national security and intelligence surveillance.