Forbes

Why We're 'Shocked, Shocked' At NSA Surveillance Revelations

By: Larry Downes- June 10, 2013

It was, to paraphrase Yogi Berra, déjà vu all over again. Fielding calls last week from journalists about reports the NSA had been engaged in massive and secret data mining of phone records and Internet traffic, I couldn't help but wonder why anyone was surprised by the so-called revelations.

Not only had the surveillance been going on for years, the activity had been reported all along—at least outside the mainstream media. The programs involved have been the subject of longstanding concern and vocal criticism by advocacy groups on both the right and the left.

For those of us who had been following the story for a decade, this was no "bombshell." No "leak" was required. There was no need for an "expose" of what had long since been exposed.

As the Cato Institute's Julian Sanchez and others reminded us, the NSA's surveillance activities, and many of the details breathlessly reported last week, weren't even secret. They come up regularly in Congress, during hearings, for example, about renewal of the USA Patriot Act and the Foreign Intelligence Surveillance Act, the principal laws that govern the activity.

In those hearings, civil libertarians (Republicans and Democrats) show up to complain about the scope of the law and its secret enforcement, and are shot down as being soft on terrorism. The laws are renewed and even extended, and the story goes back to sleep.

But for whatever reason, the mainstream media, like the corrupt Captain Renault in "Casablanca," collectively found itself last week "shocked, shocked" to discover widespread, warrantless electronic surveillance by the U.S. government. Surveillance they've known about for years.

Let me be clear. As one of the long-standing critics of these programs, and especially their lack of oversight and transparency, I have no objection to renewed interest in the story, even if the drama with which it is being reported smells more than a little sensational with a healthy whiff of opportunism.

In a week in which the media did little to distinguish itself, for example, ***The Washington Post*** stood out, and not in a good way. As Ed Bott detailed in a withering post for ***ZDNet*** on Saturday, the ***Post*** substantially revised its most incendiary article, a Thursday piece that originally claimed nine major technology companies had provided direct access to their servers as part of the Prism program.

That "scoop" generated more froth than the original "revelation" that Verizon had been complying with government demands for customer call records.

Except that the ***Post's*** sole source for its claims turned out to a PowerPoint presentation of "dubious provenance." A day later, the editors had removed the most thrilling but unsubstantiated revelations about Prism from the article. Yet in an unfortunate and baffling Orwellian twist, the paper made absolutely no mention of the "correction." As Bott points out, that violated not only common journalistic practice but the paper's own revision and correction policy.

All this and much more, however, would have been in the service of a good cause–if, that is, it led to an actual debate about electronic surveillance we've needed for over a decade.

Unfortunately, it won't. The mainstream media will move on to the next story soon enough, whether some natural or man-made disaster.

And outside the Fourth Estate, few people will care or even notice when the scandal dies. However they feel this week, most Americans simply aren't informed or bothered enough about wholesale electronic surveillance to force any real accountability, let alone reform. Those who are up in arms today might ask themselves where they were for the last decade or so, and whether their righteous indignation now is anything more than just that.

As ***Politico***'s James Hohmann noted on Saturday, "Government snooping gets civil libertarians from both parties exercised, but this week's revelations are likely to elicit a collective yawn from voters if past polling is any sign."

Why so pessimistic? I looked over what I've written on this topic in the past, and found the following essay, written in 2008, which appeared in slightly different form in my 2009 book, "The Laws of Disruption." It puts the NSA's programs in historical context, and tries to present both the costs and benefits of how they've been implemented. It points out why at least some aspects of these government activities are likely illegal, and what should be done to rein them in.

What I describe is just as scandalous, if not moreso, than anything that came out last week.

Yet I present it below with the sad realization that if I were writing it today–five years later–I wouldn't need to change a single word. Except maybe the last sentence. And then, just maybe.

Searching Bits, Seizing Information

U.S. citizens are protected from unreasonable search and seizure of their property by their government. In the Constitution, that right is enshrined in the Fourth Amendment, which was enacted in response to warrantless searches by British agents in the run-up to the Revolutionary War. Over the past century, the Supreme Court has increasingly seen the Fourth Amendment as a source of protection for personal space—the right to a "zone of privacy" that governments can invade only with probable cause that evidence of a crime will be revealed.

Under U.S. law, Americans have little in the way of protection of their privacy from businesses or from each other. The Fourth Amendment is an exception, albeit one that applies only to government.

But digital life has introduced new and thorny problems for Fourth Amendment law. Since the early part of the twentieth century, courts have struggled to extend the "zone of privacy" to intangible interests—a right to privacy, in other words, in one's information. But to "search" and "seize" implies real world actions. People and places can be searched; property can be seized.

Information, on the other hand, need not take physical form, and can be reproduced infinitely without damaging the original. Since copies of data may exist, however temporarily, on thousands of random computers, in what sense do netizens have "property" rights to their information? Does intercepting data constitute a search or a seizure or neither?

The law of electronic surveillance avoids these abstract questions by focusing instead on a suspect's expectations. Courts reviewing challenged investigations ask simply if the suspect believed the information acquired by the government was private data and whether his expectation of privacy was reasonable.

It is not the actual search and seizure that the Fourth Amendment forbids, after all, but *unreasonable* search and seizure. So the legal analysis asks what, under the circumstances, is reasonable. If you are holding a loud conversation in a public place, it isn't reasonable for you to expect privacy, and the police can take advantage of whatever information they overhear. Most people assume, on the other hand, that data files stored on the hard drive of a home computer are private and cannot be copied without a warrant.

One problem with the "reasonable expectation" test is that as technology changes, so do user expectations. The faster the Law of Disruption accelerates, the more difficult it is for courts to keep pace. Once private telephones became common, for example, the Supreme Court required law enforcement agencies to follow special procedures for the search and seizure of conversations—that is, for wiretaps. Congress passed the first wiretap law, known as Title III, in 1968. As information technology has revolutionized communications and as user expectations have evolved, the courts and Congress have been forced to revise Title III repeatedly to keep it up to date.

In 1986, the Electronic Communications Privacy Act amended Title III to include new protection for electronic communications, including e-mail and communications over cellular and other wireless technologies. A model of reasonable lawmaking, the ECPA ensured these new forms of communication were generally protected while closing a loophole for criminals who were using them to evade the police. (By 2005, 92 percent of wiretaps targeted cell phones.)

As telephone service providers multiplied and networks moved from analog to digital, a 1994 revision required carriers to build in special access for investigators to get around new features such as call forwarding. Once a Title III warrant is issued, law enforcement agents can now simply log in to the suspect's network provider and receive real-time streams of network traffic.

Since 1968, Title III has maintained an uneasy truce between the rights of citizens to keep their communications private and the ability of law enforcement to maintain technological parity with criminals. As the digital age progresses, this balance is harder to maintain. With each cycle of Moore's Law, criminals discover new ways to use digital technology to improve the efficiency and secrecy of their operations, including encryption, anonymous e-mail resenders, and private telephone networks. During the 2008 terrorist attacks in Mumbai, for example, co-conspirators used television reports of police activity to keep the gunmen at various sites informed, using Internet telephones that were hard to trace.

As criminals adopt new technologies, law enforcement agencies predictably call for new surveillance powers. China alone employs more than 30,000 "Internet police" to monitor online traffic, what is sometimes known as the "Great Firewall of China." The government apparently intercepts all Chinese-bound text messages and scans them for restricted words including *democracy*, *earthquake*, and *milk powder*.

The words are removed from the messages, and a copy of the original along with identifying information is stored on the government's system. When Canadian human rights activists recently hacked into Chinese government networks they discovered a cluster of message-logging computers that had recorded more than a million censored messages.

Netizens, increasingly fearful that the arms race between law enforcement and criminals will claim their privacy rights as unintended victims, are caught in the middle. Those fears became palpable after the September 11, 2001, terrorist attacks and those that followed in Indonesia, London, and Madrid. The world is now engaged in a war with no measurable objectives for winning, fought against an anonymous and technologically savvy enemy who recruits, trains, and plans assaults largely through international communication networks. Security and surveillance of all varieties are now global priorities, eroding privacy interests significantly.

The emphasis on security over privacy is likely to be felt for decades to come. Some of the loss has already been felt in the real world. To protect ourselves from future attacks, everyone can now expect more invasive surveillance of their activities, whether through massive networks of closed-circuit TV cameras in large cities or increased screening of people and luggage during air travel.

The erosion of privacy is even more severe online. Intelligence is seen as the most effective weapon in a war against terrorists. With or without authorization, law enforcement agencies around the world have been monitoring large quantities of the world's Internet data traffic. Title III has been extended to private networks and Internet phone companies, who must now insert government access points into their networks. (The FCC has proposed adding other providers of phone service, including universities and large corporations.)

Because of difficulties in isolating electronic communications associated with a single IP address, investigators now demand the complete traffic of large segments of addresses, that is, of many users. Data mining technology is applied after the fact to search the intercepted information for the relevant evidence.

Passed soon after 9/11, the USA Patriot Act went much further. The Patriot Act abandoned many of the hard-fought controls on electronic surveillance built into Title III. New "enhanced surveillance procedures" allow any judge to authorize electronic surveillance and lower the standard for warrants to seize voice mails.

The FBI was given the power to conduct wiretaps without warrants and to issue so-called national security letters to gag network operators from revealing their forced cooperation. Under a 2006 extension, FBI officials were given the power to issue NSLs that silenced the recipient *forever*, backed up with a penalty of up to five years in prison.

Gone is even a hint of the Supreme Court's long-standing admonitions that search and seizure of information should be the investigatory tool of last resort.

Despite the relaxed rules, or perhaps inspired by them, the FBI acknowledged in 2007 that it had violated Title III and the Patriot Act repeatedly, illegally searching the telephone, Internet, and financial records of an unknown number of Americans. A Justice Department investigation found that from 2002 to 2005 the bureau had issued nearly 150,000 NSLs, a number the bureau had grossly under-reported to Congress.

Many of these letters violated even the relaxed requirements of the Patriot Act. The FBI habitually requested not only a suspect's data but also those of people with whom he maintained regular contact—his "community of interest," as the agency called it. "How could this happen?" FBI director Robert Mueller asked himself at the 2007 Senate hearings on the report. Mueller didn't offer an answer.

Ultimately, a federal judge declared the FBI's use of NSLs unconstitutional on free-speech grounds, a decision that is still on appeal. The National Security Agency, which gathers foreign intelligence, undertook an even more disturbing expansion of its electronic surveillance powers.

Since the Constitution applies only within the U.S., foreign intelligence agencies are not required to operate within the limits of Title III. Instead, their information- gathering practices are held to a much more relaxed standard specified in the Foreign Intelligence Surveillance Act. FISA allows warrantless wiretaps anytime that intercepted communications do not include a U.S. citizen and when the communications are not conducted through U.S. networks. (The latter restriction was removed in 2008.)

Even these minimal requirements proved too restrictive for the agency. Concerned that U.S. operatives were organizing terrorist attacks electronically with overseas collaborators, President Bush authorized the NSA to bypass FISA and conduct warrantless electronic surveillance at will as long as one of the parties to the information exchange was believed to be outside the United States.

Some of the president's staunchest allies found the NSA's plan, dubbed the Terrorist Surveillance Program, of dubious legality. Just before the program became public in 2005, senior officials in the Justice Department refused to reauthorize it.

In a bizarre real-world game of cloak-and-dagger, presidential aides, including future attorney general Alberto Gonzales, rushed to the hospital room of then-attorney general John Ashcroft, who was seriously ill, in hopes of getting him to overrule his staff. Justice Department officials got wind of the end run and managed to get to Ashcroft first. Ashcroft, who was barely able to speak from painkillers, sided with his staff.

Many top officials, including Ashcroft and FBI director Mueller, threatened to resign over the incident. President Bush agreed to stop bypassing the FISA procedure and seek a change in the law to allow the NSA more flexibility. Congress eventually granted his request.

The NSA's machinations were both clumsy and dangerous. Still, I confess to having considerable sympathy for those trying to obtain actionable intelligence from online activity. Post-9/11 assessments revealed embarrassing holes in the technological capabilities of most intelligence agencies worldwide. (Admittedly, it also revealed repeated failures to act on intelligence that was already collected.) Initially at least, the public demanded tougher measures to avoid future attacks.

Keeping pace with international terror organizations and still following national laws, however, is increasingly difficult. For one thing, communications of all kinds are quickly migrating to the cheaper and more open architecture of the Internet. An unintended consequence of this change is that the nationalities of those involved in intercepted communications are increasingly difficult to determine.

E-mail addresses and instant-message IDs don't tell you the citizenship or even the location of the sender or receiver. Even telephone numbers don't necessarily reveal a physical location. Internet telephone services such as Skype give their customers U.S. phone numbers regardless of their actual location. Without knowing the nationality of a suspect, it is hard to know what rights she is entitled to.

The architecture of the Internet raises even more obstacles against effective surveillance. Traditional telephone calls take place over a dedicated circuit connecting the caller and the person being called, making wiretaps relatively easy to establish. Only the cooperation of the suspect's local exchange is required.

The Internet, however, operates as a single global exchange. E-mails, voice, video, and data files—whatever is being sent is broken into small packets of data. Each packet follows its own path between connected computers, largely determined by data traffic patterns present at the time of the communication.

Data may travel around the world even if its destination is local, crossing dozens of national borders along the way. It is only on the receiving end that the packets are reassembled.

This design, the genius of the Internet, improves network efficiency. It also provides a significant advantage to anyone trying to hide his activities. On the other hand, NSLs and warrantless wiretapping on the scale apparently conducted by the NSA move us frighteningly close to the "general warrant" American colonists rejected in the Fourth Amendment. They were right to revolt over the unchecked power of an executive to do what it wants, whether in the name of orderly government, tax collection, or antiterrorism.

In trying to protect its citizens against future terror attacks, the secret operations of the U.S. government abandoned core principles of the Constitution. Even with the best intentions, governments that operate in secrecy and without judicial oversight quickly descend into totalitarianism. Only the intervention of corporate whistle-blowers, conscientious government officials, courts, and a free press brought the United States back from the brink of a different kind of terrorism.

Internet businesses may be entirely supportive of government efforts to improve the technology of policing. A society governed by laws is efficient, and efficiency is good for business. At the same time, no one is immune from the pressures of anxious customers who worry that the information they provide will be quietly delivered to whichever regulator asks for it. Secret surveillance raises the level of customer paranoia, leading rational businesses to avoid countries whose practices are not transparent.

Partly in response to the NSA program, companies and network operators are increasingly routing information flow around U.S. networks, fearing that even transient communications might be subject to large-scale collection and mining operations by law enforcement agencies.

But aside from using private networks and storing data offshore, routing transmissions to avoid some locations is as hard to do as forcing them through a particular network or node.

The real guarantor of privacy in our digital lives may not be the rule of law. The Fourth Amendment and its counterparts work in the physical world, after all, because tangible property cannot be searched and seized in secret. Information, however, can be intercepted and copied without anyone knowing it. You may never know when or by whom your privacy has been invaded. That is what makes electronic surveillance more dangerous than traditional investigations, as the Supreme Court realized as early as 1967.

In the uneasy balance between the right to privacy and the needs of law enforcement, the scales are increasingly held by the Law of Disruption. More devices, more users, more computing power: the sheer volume of information and the rapid evolution of how it can be exchanged have created an ocean of data. Much of it can be captured, deciphered, and analyzed only with great (that is, expensive) effort. Moore's Law lowers the costs to communicate, raising the costs for governments interested in the content of those communications.

The kind of electronic surveillance performed by the Chinese government is outrageous in its scope, but only the clumsiness of its technical implementation exposed it. Even if governments want to know everything that happens in our digital lives, and even if the law allows them or is currently powerless to stop them, there isn't enough technology at their disposal to do it, or at least to do it secretly.

So far.