Through the PRISM Darkly

Hal Berghel
University of Nevada, Las Vegas

The Foreign Intelligence Surveillance Court has an approval rate of 99.93 percent of all surveillance requests. While this might not meet the strict definition of a kangaroo court, it seems to fall within the marsupial family.

Last month, the National Security Agency found itself exposed to public ridicule for a variety of privacy-abusing activities. Once the mainstream media and political operatives got hold of the story, the signal-to-noise ratio decreased precipitously. Perhaps this column can add some clarity.

THE EVENTS OF INTEREST

June 2013 is a month that will live in NSA infamy. On 5 June, Glenn Greenwald of the UK's *Guardian* newspaper posted a redaction of an order from the Foreign Intelligence Surveillance Court signed by Judge Roger Vinson that required cell phone giant Verizon to provide "all call detail records [aka CDRs] or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls … and that no person shall disclose to any other [unauthorized] person that the FBI or NSA has sought or obtained tangible things under this Order." This order, still in effect at this writing, covered the period 25 April to 19 July 2013 (www.guardian.co.uk/world/interactive/2013/jun/06/verizon-telephone-data-court-order). Needless to say, this had a chilling effect on the public and launched a firestorm of criticism.

But the story didn't end there. It appears that on 16 May 2013 the source of the *Guardian* story, an employee of government contractor Booz Allen Hamilton by the name of Edward Snowden, informed *Washington Post* reporter Barton Gellman of a secret NSA program to intercept and collect metadata from collaborating tech companies (www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html?tid=pm_pop). This effort, subsumed under the cover term PRISM, began after passage of the 2008 Foreign Intelligence Surveillance Act (FISA) amendment in response to the disclosure that the George W. Bush administration had authorized warrantless wiretaps of civilians. The *Post* broke the story two weeks later. Snowden shared the information with Greenwald at the *Guardian*, which also ran the story. Both the *Post* and the *Guardian* stories released a few nontechnical, NSA-internal and confidential PowerPoint briefing slides that demonstrated some of the intent of PRISM surveillance and the involvement with high-tech companies. Of the 41 briefing slides that Snowden provided the *Guardian* and *Post*, only five—one of them being Figure 1—have been made public at this time.

Published by the IEEE Computer Society

Particularly noteworthy is the template header listing the cooperating high-tech companies. Immediately following the disclosure, some of the larger companies went into denial, thereby causing the *Post* to speculate that the NSA might have had a "back door" in situ that was fed data from the host server clusters but not directly connected. This would bring the observations and the carefully crafted corporate statements into consistency. By everyone's account, the relationship between the NSA and the high-tech companies is willingly cooperative, leading some to describe the NSA technology as a "data-ingestion API" (http://mashable.com/2013/06/08/prism-nsa-direct-access.)

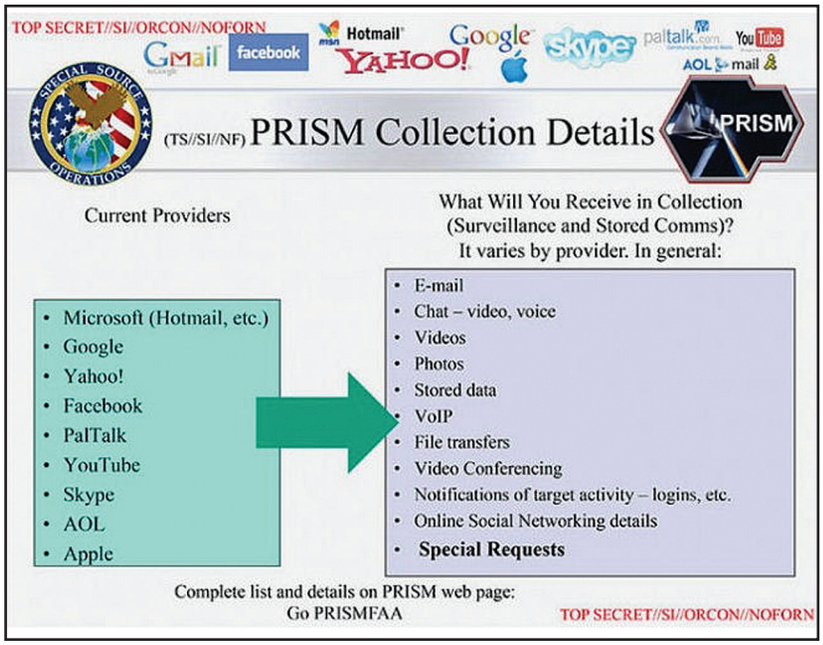

Figure 1. The PRISM corporate partners hall of shame. Who were the corporate officers who agreed to this relationship with the NSA? Why did Apple hold out until after Steve Jobs' death? Inquiring minds want to know.

THE "TRUST ME" DEFENSE, FALSE DILEMMAS, AND RED HERRINGS

As I write this, Snowden is being labeled as both saint and sinner (depending on political persuasion), the NSA and its sympathizers are claiming that the world is far less safe than it was before the leaks, the overzealous "big data" politicians call for a full measure of hurt for Snowden, and the three-letter agency leaderships single him out, alone, for their wrath. If this sounds familiar, it's the same security theater that we've gone through over the past few years with Bradley Manning (see the March 2012 installment of this column). As I pointed out at that time, the real security story addresses the question, "By what/whose authority was Manning (now Snowden) given access to sensitive, classified documents?" Once again, a security clearance isn't supposed to be a hunting permit for curiosity seekers. Based on the description of Snowden's job title, his access to this sensitive information failed any reasonable "need to know" standard.

Once the hubris and hyperbole die down, it will become clear that the revelations weren't earth-shaking, very little if any security was compromised, the only real damage was to the continuous erosion of the credibility of the NSA and the government, and, most importantly, that the "system" that produced PRISM and the Verizon court order isn't transparent, is overly clandestine, and only works efficiently in the imagination of its supporters.

The first two weeks of June seem to have produced two main defenses of the surveillance programs. The simpler of the two is the "trust me" defense that seems to be in vogue by the political leadership. While the "trust me" defense has been a staple of totalitarian governments worldwide, it hasn't been effective with the educated electorate in the US at least since Watergate—it has become a "throw away" concept. However, when strange bedfellows like John Boehner, Harry Reid, Lindsey Graham, and Dianne Feinstein all say there's nothing to worry about. …

The second defense is a false dilemma: the choice is to either endorse government surveillance as it is or run the risk of increased terrorist attacks, death, and disorder. Of course, this begs the question whether there might be other, more constitutionally sympathetic, effective means of accomplishing the same objective. The false dilemma tactic is currently popular with President Barack Obama and NSA director Keith Alexander, at this writing the latter of whom promises the congressional leadership imminent objective proof by enumeration.

Concurrently, most of the media emphasize the extent of the US government's electronic surveillance programs, the leaker and his motivations, and the political reaction to both, all of which are red herrings.

IN CONTEXT

The NSA's PRISM project and its access of Verizon's phone logs aren't isolated 4th Amendment assaults. Open source information that confirms the breadth and depth of

government surveillance has been widely and publicly available for many decades. The US government's passion for surveillance and stealth is anything but new in signals intelligence—only the circuits and frequencies have changed:

- 1950s-1970s: Baby boomers will recall that the major crises of confidence over government surveillance exposed by the Senate Judiciary Subcommittee on the Constitution, Civil Rights, and Human Rights under chairs Sam Ervin and Frank Church, including the CIA "family jewels"-like disclosure by Christopher Pyle that the US Army had 1,500 undercover agents infiltrating antiwar demonstrations in the 1960s; disclosure of the 1950s "mail covers" mail opening programs; disclosure of surveillance of journalists; and disclosure of the White House enemies list, the Watergate break-in, and that of Daniel Ellsberg's psychiatrist.
- 1970s: Echelon, the NSA's "global system for intercepting private and commercial communications," is deployed by the US and some of its allies.
- 1996-1997: Carnivore (aka DCS1000), the FBI's packet-sniffing system for mass surveillance of Windows computer users, is deployed.
- 1997: NarusInsight, a commercial, supercomputer successor to the Carnivore effort, is put on the Internet backbone and related to the AT&T's infamous secret room in San Francisco. Note that PRISM's "back door" approach to digital surveillance follows in the NarusInsight lineage.
- Late 1990s: Magic Lantern, the FBI's keystroke logger, is spawned by an email Trojan horse activated when target uses email encryption.
- Early 2000s: The Trailblazer project, an inelegant and costly NSA program that was part of the George W. Bush administration's warrantless surveillance efforts, analyzes traffic over communications networks. Costly and ineffective, it was chosen over the less expensive, finely grained, and privacy-protective effort, ThinThread. The DoD inspector general's office criticized the Trailblazer effort as "poorly executed and overly expensive" (http://upload.wikimedia.org/wikipedia/commons/3/33/Redacted-dod-oig-audit-requirements-for-the.pdf). Trailblazer was shut down in 2006, having overspent its budget by hundreds of millions of dollars.
- 2001: Stellar Wind (now called Ragtime), the NSA's bulk data collection program, is initiated after 9/11 and will feed the NSA's Utah Data Center when it is completed.
- 2013: Tailored Access Operations (TAO) is the NSA's "offensive OPS" group that compromises adversaries' computer systems and networks, the US equivalent to the offensive Chinese cyberwarfare units on Hainan Island and in Shanghai. Rumor has it that TAO was instrumental in outing China's recent industrial espionage efforts against US corporations (www.scmp.com/news/china/article/1259175/inside-nsas-ultra-secret-china-hacking-group).

The playwright William Archer once said that "drama is anticipation mingled with uncertainty." This holds for security theater as well.

So, PRISM (aka US-984XN) is far from a new development. It's merely one of the more recent programs that have been revealed. Think of it as a supplement to preexisting intelligence-gathering activities. This toothpaste is out of this tube.

CYBURBAN MYTHS

As the timeline shows, the government, through various three-letter agencies, willingly accosted if not assaulted 4th Amendment protections long before 9/11. The claim that all of this surveillance was necessitated by 9/11 and the subsequent global war on terror is a myth.

A December 2000 NSA memo shows that a case was even then being made for pushing the boundaries of constitutional limits on surveillance (www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB24/nsa25.pdf). Particularly notable are the references to "major policy issues" on pages 31-32. To wit, here are some relevant quotations:

- "The volumes and routing of data make finding and processing nuggets of intelligence information more difficult. To perform both its offensive and defensive missions, NSA must 'live on the network.'"
- "because of the [sophisticated] communications environment …, availability of critical foreign intelligence information will mean gaining access in new places and in new ways." Interestingly, the presumably clarifying next sentence was redacted.
- "The Fourth Amendment is as applicable to eSIGINT as it is to the SIGINT of yesterday and today. The Information Age will however cause us to rethink and reapply the procedures,

policies and authorities born in an earlier electronic surveillance environment."

- "Make no mistake, NSA can and will perform its missions consistent with the Fourth Amendment and all applicable laws. But senior leadership must understand that today's and tomorrow's mission will demand a powerful, permanent presence on a global telecommunications network that will host the 'protected' communications of Americans as well as the targeted communications of adversaries."

URL PEARLS

The specific details on Snowden's discussions with the two reporters are under some dispute (www.wired.com/threatlevel/2013/06/snowden-powerpoint/#slideid-57991).

For the historians among you, the redacted CIA "family jewels" are now available online on the George Washington University NSA Archive site at www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB222/index.htm. Former CIA Director William Colby's revelations were extremely unpopular with conservatives and strong government types, and his testimony contributed to the "Halloween Massacre" that reorganized President Gerald Ford's cabinet in 1975. Colby was replaced as director of the CIA by George H.W. Bush, Secretary of Defense James Schlesinger was replaced by Donald Rumsfeld, Dick Cheney replaced Rumsfeld as chief of staff, Henry Kissinger was fired as national security advisor, and Vice President Nelson Rockefeller was encouraged not to seek reelection. PRISM is part of the new millennium "family jewels."

A second myth is that rigorous oversight of surveillance activities is present. Token, yes; rigorous, not so much. When Director of National Intelligence James Clapper refers to the FISA court as one component of an "extensive oversight regime, incorporating reviews by the Executive, Legislative and Judicial Branches" (www.wired.com/images_blogs/threatlevel/2013/06/PRISM-FAQ.pdf), that should be understood in the limited sense that there is minimal congressional awareness restricted to a few committees and one element of the judiciary. The latter, the FISA court, is worthy of elaboration.

Clandestine surveillance and intelligence activities are statute-driven in the sense that they're enabled, and sometimes motivated, by changes in federal statutes and executive orders. When agency activities are determined to be outside the law, both the laws and activities are thus brought into agreement. The classic illustration is the 2008 modification motivated by the 2005 discovery that the George W. Bush administration had authorized warrantless wiretaps that included US citizens, which produced a flurry of lawsuits. To forestall further litigation and 4th Amendment challenges, FISA was amended to ensure that federal surveillance objectives, basically as practiced, would be legal. In this way, federal law seamlessly integrated itself with the interests of investigative and intelligence-gathering agencies. So when a government official reports that agency activities comply with the law, this is true a priori. Of course, the more interesting question is whether the laws are both constitutional and consistent with the public's expectations from participatory democracy.

Since the expiration of the Protect America Act in 2008, FISA became the centerpiece of agency oversight efforts. To my knowledge, the only people who claim that the FISA court is proactive in its oversight are the people who benefit from its minimalism.

Mother Jones recently ran a story that suggests the FISA court is of the "rubber stamp" ilk (www.motherjones.com/mojo/2013/06/fisa-court-nsa-spying-opinion-reject-request). According to the magazine, FISA has approved 99.93 percent of all government surveillance requests (11 of 33,900 denied since FISA's inception in 1978, and none in the past year). Given this approval rate (the 11 denials must have been whoppers!), it might seem simpler and less expensive to abolish the court and turn the approval process over to a clerk. The numbers speak for themselves. Although FISA might not meet the strict definition of a kangaroo court, it falls somewhere within the marsupial family.

Also worthy of mention is the obvious political bias of the FISA court. Of the 11 federal judges that make up the current court, nine were appointed to the federal bench by Republican presidents (Reagan 3, George H.W. Bush 1, George W. Bush 5, Clinton 1, Obama 1), and all FISA justices are appointed by the Chief Justice of the Supreme Court, himself a Republican appointee to the federal judiciary. If the intention of the legislation that created the FISA court was to give the appearance of nonpartisanship, it didn't happen.

WHERE ARE WE HEADED?

It has been fashionable for much of the past century to criticize "big government." Fiscal conservatives and neoliberals speak of "big government" in the sense of scope and size of budget. However, there's another, important sense of "big government"—one that refers to the degree of control that a government exercises over its citizens. This is the sense of big government that produces the dystopia of which George Orwell and Aldous Huxley wrote. The recent Verizon/PRISM expose is the most recent wake-up call that this latter dimension is worthy of

our sustained attention. I find it ironic that the opponents of big government in the former sense seem inattentive to big government in the latter. I'll make some predictions.

What we will see in the near future:

- This next year, the Utah Data Center will be complete. With a planned capacity of 5 exabytes (10^{18} bytes), it's unlikely that the NSA intends to limit itself to CDRs. And at 650 WPSF (65 megawatt/100,000 square feet of datacenter), there will surely be a lot of data mining. Absent new, effective oversight legislation, the UDC will function like a multimedia digital vacuum.
- The government will continue to outsource surveillance and intelligence-gathering activities (and perhaps even cyberwarfare) to cyber-mercenary companies like HBGary Federal/ManTech, Gamma Group, STRATFOR, and so on, which are even less subject to congressional and judicial oversight.
- Congress will continue to add, delete, and modify FISA and other appurtenant statutes to assure the appearance of propriety and the illusion of transparency.
- Occasional insights into the inner operation of the agencies through whistle-blowers and the occasional lapses of judgment during congressional hearings will continue.
- A revolving door between senior agency leadership, government cybercontractors, and the military will ensure that all stay on the same page.
- Politicians will seize the opportunity for media coverage of their opinions.
- The government will continue its aggressive prosecution of whistle-blowers, leakers, and journalists to strike fear in the hearts of contrarians of any stripe.
- Stakeholder journalism and media will continue to be distracted from the important issues.

What we would like to see:

- Constitution and Bill of Rights awareness training for three-letter agency recruits or world-class constitutional law specialists or ethicists involved in oversight.
- High-tech companies and corporate America filing friends-of-the court briefs on behalf of 4th amendment protections.
- Agency leadership accepting blame for information security policies of their design that fail to enforce reasonable standards for security clearances.
- Technology-aware members of Congress and the FISA court, and laws that make the latter more accountable to the electorate.
- Civilian (versus military or political) oversight of three-letter agencies.
- Enforcement of sunset provisions of oversight statutes.
- "Trust me" banned from political discourse.

Harvard evolutionary biologist Stephen Jay Gould introduced the theory of punctuated equilibrium, whereby evolution is seen as long periods of stability interrupted by brief periods of rapid change. In our present context, the "steady state" is the subtle but continuous erosion of personal privacy and liberty by big government, punctuated by occasional restraint in the form of Ervin committees, Church Commissions, Iran-Contra hearings, and occasional unauthorized disclosures. The playwright William Archer once said that "drama is anticipation mingled with uncertainty." This holds for security theater as well.

Hal Berghel, *Out of Band column editor, is a professor of computer science at the University of Nevada, Las Vegas, where he is the director of the Identity Theft and Financial Fraud Research and Operations Center (itffroc.org). Contact him at hlb@computer.org.*