The NSA and the BIG SUCK at Defcon

by Elinor Mills via zuis - CNET *Saturday, Jul 28 2012, 2:22am*
international / prose / post

Elite Uber Hackers are not amused

> *The director of the known criminal (illegal surveillance) National Security Agency (NSA) Gen. Keith Alexander, admits that Defcon hackers constitute the "world's best cybersecurity community;" he then, not entirely unexpectedly, begged for their help BUT elite Uber hackers are not buying the bullshit nor do they intent to give away their edge to the criminal enemy!*

NSA Director Keith Alexander

LAS VEGAS -- Over the past two decades, hackers at Defcon and the feds have been circling each other suspiciously. The nation's top "spook" -- National Security Agency Director Gen. Keith Alexander -- giving a keynote at the hacker confab, shows just how much tensions have mellowed.

"I've spent 20 years trying to get someone from the NSA" to speak at Defcon, said Defcon founder Jeff Moss, who serves on the U.S. Homeland Security Advisory Council and is chief security officer for ICANN. "It's eye-opening to see the world from their view," he said. "On the NSA's 60th anniversary and our 20th anniversary this has all come together."

Against a backdrop of relentless cyber-espionage on U.S. companies and government agencies and vulnerabilities and exploits affecting critical infrastructure providers, Gen. Alexander, who also is commander of the U.S. Cyber Command, asked the hackers for help. "In this room right here is the talent we need to secure cyberspace," he said. "You know we can protect the networks and have civil liberties and privacy and you can help us get there."

Long a staple at Defcon, the "Spot the Fed" contest served as a playful detente between the hackers and the agents who chased them for phone phreaking, distributed denial-of-service attacks, Web site defacements, and basically using the Internet as their personal playground and social experiment.

Now, Defcon is "the world's best cybersecurity community," Alexander said. "This community, better than anyone, understand(s) what we need to do" to address these problems.

The country also needs better sharing between private companies and the government, something that proposed cybersecurity legislation can help fix, he said, noting that Congress is debating the legislation this week. "We can sit on the sidelines and let others who don't understand this space tell

us what they're gonna do or...help them develop strategy. That's there real reason I came here. To solicit your support. You have the talent. You have the expertise."

The U.S. needs to do more to train and educate people in cybersecurity to increase the numbers of hackers who can work on the problems, he said, praising Defcon Kids for doing just that. He congratulated a preteen hacker, CyFi, for winning the Defcon Kids Zero-Day contest by finding a vulnerability that was previously unknown.

"Sometimes you guys get a bad rap," Alexander said. "From my perspective, what you're doing to figure out vulnerabilities in systems" is great.

Asked during the question-and-answer session whether the NSA keeps a file on every U.S. citizen, Alexander said that notion was "absolute nonsense," partly because managing 260 million or so individual citizen files would be impossible for the department to handle.

"No we don't. Absolutely not," he said. "Our job is foreign intelligence. We get oversight by Congress...everything we do is auditable by them, by the FISA (Foreign Intelligence Surveillance Act)...and by the (Obama) Administration."

He acknowledged that occasionally there are slip ups. "We may, incidentally in targeting a bad guy, hit on a good guy," he said. "We have requirements from (the FISA) court and the attorney general to minimize that."

[A note from the Uber elite kiddies; hang in there, maintain ur integrity and improve ur skills until such time u r able to enter our realm. we are the only effective force for justice on the planet ... the NSA is a known and proven criminal organization that serves the ruling mass murdering elites. hold fast to ur principles and join us one day in the right fight against the evil forces that plague our world. Be aware and beware!]

See:
http://jungledrum.hopto.org/news/story-15.html

http://cleaves.zapto.org/news/story-516.html

> **NSA Spying: 'If We Tell You, We'll Have to Kill You'**
> by Tom Burghardt - Antifascist Calling
>
> When Congress passed the FISA Amendments Act (FAA) in 2008, a privacy-killing law that gutted First, Fourth and Fifth Amendment protections for Americans while granting immunity to giant telecoms that assisted the National Security Agency's (NSA) warrantless wiretapping programs, we were assured that the government "does not spy" on our communications.
>
> Yet scarcely a year after FAA was signed into law by President Bush, The New York Times revealed that under Hope and ChangeTM huckster Barack Obama, NSA continued the previous regime's illegal practices, intercepting "private e-mail messages and phone calls of Americans in recent months on a scale that went beyond the broad legal limits established by Congress last year."

The wholesale vacuuming-up of private communications by the sprawling Pentagon bureaucracy were described by unnamed "senior officials" as the "'overcollection' of domestic communications of Americans;" in other words, a mere technical "glitch" in an otherwise "balanced" program.

But what most Americans are blissfully unaware of is the fact that they carry in their pockets what have been described as near-perfect spy devices: their cellphones.

Earlier this week, The New York Times disclosed that "cellphone carriers reported that they responded to a startling 1.3 million demands for subscriber information last year from law enforcement agencies seeking text messages, caller locations and other information in the course of investigations."

The report by carriers, made in response to congressional inquiries "document an explosion in cellphone surveillance in the last five years, with the companies turning over records thousands of times a day in response to police emergencies, court orders, law enforcement subpoenas and other requests."

"I never expected it to be this massive," said Rep. Edward J. Markey (D-MA), the co-chair of the Bipartisan Congressional Privacy Caucus, "who requested the reports from nine carriers, including AT&T, Sprint, T-Mobile and Verizon."

Markey told the Times that the prevalence of cellphone surveillance by law enforcement agencies raised the specter of "digital dragnets" that threaten the privacy of most customers.

While the sheer volume of requests by local, state and federal police for user data may have startled Congress, which by-and-large has turned a blind eye when it comes to privacy depredations at all levels of government, it is hardly a complete picture of the pervasive nature of the problem.

In 2009 security watchdog Christopher Soghoian reported on his Slight Paranoia web site that just one firm, Sprint Nextel, "provided law enforcement agencies with its customers' (GPS) location information over 8 million times between September 2008 and October 2009. This massive disclosure of sensitive customer information was made possible due to the roll-out by Sprint of a new, special web portal for law enforcement officers." (emphasis added)

According to Soghoian, "Internet service providers and telecommunications companies play a significant, yet little known role in law enforcement and intelligence gathering."

"Government agents routinely obtain customer records from these firms," Soghoian averred, "detailing the telephone numbers dialed, text messages, emails and instant messages sent, web pages browsed, the queries submitted to search engines, and of course, huge amounts of geolocation data, detailing exactly where an individual was located at a particular date and time."

While there are indeed "exigent circumstances" which may require law enforcement to demand instant access to GPS data or other customer records--a kidnapping or child abduction in progress--in the main however, it appears that most warrant-free requests fall under a more sinister category: fishing expedition.

Commenting on congressional revelations, ACLU legislative counsel Christopher Calabrese informed us that data supplied to the Times represents "a vast undercount of the number of Americans who have been affected by this tracking. Sprint disclosed that it received approximately 500,000 subpoenas in 2011 (a subpoena is a written request for information from law enforcement that isn't reviewed by a judge) and that 'each subpoena typically requested subscriber information on multiple subscribers.' In addition, several carriers disclosed that they sometimes provide all the information from a particular cell tower or particular area."

Although several geolocation privacy bills that require warrants to obtain records are pending in Congress, it should be clear there is no consensus among ruling class elites for protecting the privacy rights of Americans or reining-in overly-intrusive police agencies.

In fact, the opposite is the case.

Under Obama, illegal surveillance programs once hidden behind code-named black projects such as STELLAR WIND and PINWALE have been greatly expanded. Indeed, the bipartisan consensus which encourages and permits the secret state to carry out warrantless wiretapping and data mining have been "regularized" to such a degree (under the rubric of "keeping us safe") they're no longer even regarded as controversial.

More than three years ago, Obama promised to "fix" illegal policies which surfaced under the previous Bush government. However, an anonymous "senior official" told the Times there were certain "technical problems" that led the agency "to inadvertently 'target' groups of Americans and collect their domestic communications without proper court authority. Officials are still trying to determine how many violations may have occurred."

It was further revealed that some of the groups "inadvertently" targeted by NSA and other spy satrapies (CIA, DHS, FBI, et. al.) included Muslim Americans, anarchist and socialist groups, libertarians, civil liberties organizations, antiwar activists as well as individual supporters of the secrecy-spilling web site WikiLeaks.

Just last week the Bradley Manning Support Network disclosed that "A letter dated May 18, 2012, which purports to originate from the US Army Criminal Investigative Division (CID), rejects a Freedom of Information Act (FOIA) request submitted for data the government has collected on the Bradley Manning Support Network. The letter states that 'an active investigation is in progress with an undetermined completion date'."

As readers recall, Manning is the Army private accused by the government of releasing hundreds of thousands of secret files to WikiLeaks. He currently faces charges that could lead to decades of incarceration.

"At this time," Network supporters wrote, "it is unclear whether the investigation cited in the FOIA denial simply refers to the government's ongoing legal retaliation against Bradley Manning, or whether there is actually some other separate investigation targeting the Support Network."

It's a sure bet, given the administration's ongoing war against whistleblowers, that the Army as well the Justice Department has the Manning Support Network--along with

WikiLeaks--in their gun sights.

And with the construction of NSA's giant $2 billion Utah Data Center nearing completion, as James Bamford reported in Wired Magazine in March, the agency's ability "to intercept, decipher, analyze, and store vast swaths of the world's communications as they zap down from satellites and zip through the underground and undersea cables of international, foreign, and domestic networks" will soon take a qualitative leap forward--at our expense.

With FAA currently up for renewal, and with congressional grifters on both sides of the aisle pushing for a five-year, amendment-free extension as demanded by the administration, the secret state is refusing to provide privacy advocates--both in and outside government--with any information whatsoever on how just many violations have occurred on a regular basis under the law's admittedly loose guidelines.

In May, senators Ron Wyden (D-OR) and Mark Udall (D-CO), members of the Senate Select Committee on Intelligence asked NSA to divulge information about how many Americans communications have been spied upon by the agency.

The Office of the Director of National Intelligence responded by saying that it was "not reasonably possible to identify the number of people located in the United States whose communications may have been reviewed under the authority of the FAA."

Both senators oppose FAA's extension on civil liberties grounds and in the face of the government's stonewall, Wyden placed a "hold" on the legislation.

In a statement published on his web site Wyden explained why he was blocking unanimous consent requests to pass FAA's five-year extension.

"The purpose of this 2008 legislation was to give the government new authorities to collect the communications of people who are believed to be foreigners outside the United States, while still preserving the privacy of people inside the United States," Wyden wrote.

"Before Congress votes to renew these authorities it is important to understand how they are working in practice. In particular, it is important for Congress to better understand how many people inside the United States have had their communications collected or reviewed under the authorities granted by the FISA Amendments Act."

"I am concerned, of course, that if no one has even estimated how many Americans have had their communications collected under the FISA Amendments Act," Wyden averred, "it is possible that this number could be quite large. Since all of the communications collected by the government under section 702 are collected without individual warrants, I believe that there should be clear rules prohibiting the government from searching through these communications in an effort to find the phone calls or emails of a particular American, unless the government has obtained a warrant or emergency authorization permitting surveillance of that American."

Ludicrously enough, in response to the senator's requests I. Charles McCullough, the Inspector General of the Office of the Director of National Intelligence wrote that the NSA Inspector General "and NSA leadership agreed that an IG review of the sort

suggested would itself violate the privacy of U.S. persons." (emphasis added)

McCullough's irony-rich obfuscation, published by Wired, argued that even providing an estimate on how many Americans were spied upon would be "beyond the capacity" of the NSA's in-house watchdog. "I defer to [the NSA inspector general's] conclusion that obtaining such an estimate was beyond the capacity of his office and dedicating sufficient additional resources would likely impede the NSA's mission."

Just as the Bush administration scotched citizen lawsuits that demanded accountability from the nation's telecommunication providers over their collaboration with NSA's illegal programs, so too has the Obama regime sought to derail government accountability by invoking an alleged "state secrets privilege."

Recently, the Electronic Frontier Foundation reported that "Three whistleblowers--all former employees of the National Security Agency (NSA)--have come forward to give evidence in ... EFF's lawsuit against the government's illegal mass surveillance program, Jewel v. NSA."

In a July 2 motion filed in U.S. District Court in San Francisco, "the three former intelligence analysts confirm that the NSA has, or is in the process of obtaining, the capability to seize and store most electronic communications passing through its U.S. intercept centers, such as the 'secret room' at the AT&T facility in San Francisco first disclosed by retired AT&T technician Mark Klein in early 2006."

Those three former NSA officials--William E. Binney, Thomas A. Drake and J. Kirk Wiebe--were themselves targets of government persecution over allegations that they provided information to The New York Times in their 2005 revelation of illegal domestic spying by the Agency.

Drake, who pled guilty last year to a misdemeanor after the Justice Department's Espionage Act charges collapsed, was initially prosecuted by the administration--as a spy no less--for providing evidence to The Baltimore Sun of massive waste, fraud and corruption in NSA's Trailblazer program.

The $1.2 billion corporate boondoggle, overseen by the Science Applications International Corporation (SAIC) and project partners Boeing, Computer Sciences Corporation and Booz Allen Hamilton was eventually shut down in 2006.

In the wake of initial reporting by the Times, USA Today disclosed that NSA "has been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon and BellSouth."

In fact, the same firms who assisted the Agency in creating "'a database of every call ever made' within the nation's borders," are busy as proverbial bees providing geolocational information to law enforcement and secret state agencies.

As EFF averred, "Jewel v. NSA is back in district court after the 9th U.S. Circuit Court of Appeals reinstated it in late 2011. In the motion for partial summary judgment filed today, EFF asked the court to reject the stale state secrets arguments that the government has been using in its attempts to sidetrack this important litigation and instead apply the processes in the Foreign Intelligence Surveillance Act that require the

court to determine whether electronic surveillance was conducted legally."

While EFF should be commended for their efforts, prospects for a full accounting of serious state constitutional violations of Americans' right face an uphill battle.

As the World Socialist Web Site pointed out Monday, "The latest revelations about cell phone monitoring, when added to the long record of antidemocratic attacks carried out since the declaration of the 'war on terror'--from the establishment of the Guantanamo Bay prison camp to the Obama administration's assertion of the right to summarily execute anyone, including US citizens, anywhere in the world—provide chilling evidence of the real and growing threat of an American police state."

Efforts in that direction by the Obama administration are gathering steam.

The Electronic Privacy Information Center (EPIC) also reported Monday that "The White House has released a new Executive Order seeking to ensure the continuity of government communications during a national emergency."

That Executive Order, issued July 6 by the White House, grants new powers to the Department of Homeland Security, "including the ability to collect certain public communications information," EPIC averred.

But it does far more than that. "Under the Executive Order the White House has also granted the Department the authority to seize private facilities when necessary, effectively shutting down or limiting civilian communications."

As researcher Peter Dale Scott disclosed in numerous analyses on so-called "Continuity of Government" planning, COG is code for the suspension of constitutional guarantees and the imposition of martial law by the National Security State.

In 2010, Scott pointed out in Japan Focus: "Clearly 9/11 met the conditions for the implementation of COG measures, and we know for certain that COG plans were implemented on that day in 2001, before the last plane had crashed in Pennsylvania. The 9/11 Report confirms this twice, on pages 38 and 326. It was under the auspices of COG that Bush stayed out of Washington on that day, and other government leaders like Paul Wolfowitz were swiftly evacuated to Site R, inside a hollowed out mountain near Camp David."

In fact, the first ninety days after 9/11 "saw the swift implementation of the key features attributed to COG planning ... in the 1980s: warrantless detentions, warrantless deportations, and the warrantless eavesdropping that is their logical counterpart. The clearest example was the administration's Project Endgame--a ten-year plan, initiated in September 2001, to expand detention camps, at a cost of $400 million in Fiscal Year 2007 alone. This implemented the central feature of the massive detention exercise, Rex 84, conducted by Louis Giuffrida and Oliver North in 1984."

The proposed five-year extension of the FISA Amendments Act, coupled with indefinite detention provisions of the 2012 National Defense Authorization Act (NDAA), the president's "kill list" and now, a new Executive Order granting DHS the power to "seize" private communications' facilities in the wake of a "national emergency" have accelerated these dictatorial trends.

Author retains copyright.

The Kill List, Drone President -- she 'didn't see it coming' - Artwork, Mr Fish

http://news.cnet.com/8301-1009_3-57481689-83/nsa-director-finally-greets-defcon-hackers/

Jungle Drum Prose/Poetry. http://jungledrum.lingama.net/news/story-20.html