GlobalResearch
Center for Research on Globalization

FBI Wiretapping of Internet Users. “All Your Data Belongs to Us”

A Seamless Global Surveillance Web

By Tom Burghardt
Global Research, November 21, 2010
Antifascist Calling... 21 November 2010
Region: USA
Theme: Police State & Civil Rights

*In a further sign that Barack Obama’s faux “progressive” regime will soon seek broad new Executive Branch power, **The New York Times** disclosed last week that FBI chief and **cover-up specialist extraordinaire**, Robert S. Mueller III, “traveled to Silicon Valley on Tuesday to meet with top executives of several technology firms about a proposal to make it easier to wiretap Internet users.”*

Times’ journalist Charlie Savage reported that Mueller and the Bureau’s chief counsel, Valerie Caproni, “were scheduled to meet with senior managers of several major companies, including Google and Facebook, according to several people familiar with the discussions.”

Facebook’s public policy manager Andrew Noyes confirmed that Mueller “is visiting Facebook during his trip to Silicon Valley;” Google, on the other hand, “declined to comment.”

*Last month, **Antifascist Calling** reported that the U.S. secret state, in a reprise of the crypto wars of the 1990s, is seeking new legislation from Congress that would “fix” the Communications Assistance to Law Enforcement Act (**CALEA**) and further curtail our civil- and privacy rights.*

*When the administration floated the proposal in September, **The New York Times** revealed that among the “fixes” sought by the FBI and other intrusive spy satrapies, were demands that communications’ providers build backdoors into their applications and networks that will give spooks trolling “encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct ‘peer to peer’ messaging like Skype” the means “to intercept and unscramble encrypted messages.”*

And with a new “security-minded” Congress set to convene in January, chock-a-block with Tea Partying “conservatives” and ultra-nationalist know-nothings, the chances that the administration will get everything they want, and then some, is a sure bet.

“All Your Data Belongs to Us”

Caproni and her cohorts, always up to the challenge when it comes to grabbing our personal data, much like pigs snuffling about a dank forest in search of truffles or those rarer, more elusive delicacies christened “actionable intelligence” by our minders, avowed that said legislative tweaks are “reasonable” and “necessary” requirements that will “prevent the erosion” of the Bureau’s “investigative powers.”

Never mind that the FBI, as ***Wired Magazine*** revealed three years ago, "has quietly built a sophisticated, point-and-click surveillance system that performs instant wiretaps on almost any communications device."

Security journalist Ryan Singel reported that the Bureau's Digital Collection System Network or DCS-3000, a newer iteration of the Carnivore system of the 1990s, "connects FBI wiretapping rooms to switches controlled by traditional land-line operators, internet-telephony providers and cellular companies."

Documents obtained by the Electronic Frontier Foundation through a Freedom of Information Act lawsuit revealed that the system was created to "intercept personal communications services delivered via emerging digital technologies used by wireless carriers." A second system, Red Hook, collects "voice and data calls and then process and display the intercepted information."

And never mind, as ***Wired*** also informed us, that the Bureau's "computer and internet protocol address verifier," or CIPAV, once called Magic Lantern, is a malicious piece of software, a virtual keystroke reader, that "gathers a wide range of information, including the computer's IP address; MAC address; open ports; the operating system type, version and serial number; preferred internet browser and version; the computer's registered owner and registered company name; the current logged-in user name and the last-visited URL."

Insidiously, the U.S. Ninth Circuit Court of Appeals ruled at the time, since the Bureau's malware doesn't capture the content of communications, it can be conducted without a wiretap warrant, because, as our judicial guardians opined, users have "no reasonable expectation of privacy" when using the internet.

And with the secret state clamoring for the broadest possible access to our data, its become a lucrative business for greedy, I mean patriotic, ISPs who charge premium prices for services rendered in the endless "War on Terror."

Security Is Patriotic, and Profitable Too!

Last week, ***The Register*** informed us that privacy and security researcher Christopher Soghoian revealed that although "Microsoft does not charge for government surveillance of its users," Google, on the other hand "charges $25 per user."

This information was revealed in a **document** obtained by the intrepid activist under the Freedom of Information Act.

Soghoian, whose ***Slight Paranoia*** web site has broken any number of stories on the collusive, and patently illegal, collaboration amongst grifting telecoms, niche spy firms and the secret state, revealed in March that the Secure Socket Layer (SSL) system has already been compromised by U.S. and other intelligence agencies. (SSL is the tiny lock that appears in your browser when you log-on to an allegedly "secure" web site for banking or other online transactions.)

In a paper co-authored with researcher Sid Stamm, ***Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL***, Soghoian revealed that a "new attack" against online privacy, "*the compelled certificate creation attack*, in which government agencies compel a certificate authority to issue false SSL certificates that are then used by intelligence agencies to covertly intercept and hijack individuals' secure Web-

based communications … is in active use."

The latest disclosure by Soghoian uncovered evidence that the U.S. Drug Enforcement Administration (DEA), shelled out some $6.7 million for pen registers and $6.5 million for wiretaps. While a wiretap provides law enforcers with "actual telephone or internet conversations," a pen register "merely grabs numbers and addresses that show who's doing the communicating," *The Register* averred.

While Microsoft doesn't charge the government for spying on their users, conveniently doing away with a messy paper trail in the process, Google receives $25 and Yahoo $29 from taxpayers for the privilege of being surveilled. Soghoian points out that "Google and Yahoo! may make more money from surveillance than they get directly from their email users. Basic Google and Yahoo! email accounts are free. Department of Justice **documents** show that telcos may charge as much as $2,000 for a pen register."

That 2006 report from the DoJ's Office of the Inspector General reported that to facilitate CALEA compliance, "Congress appropriated $500 million to reimburse carriers for the direct costs of modifying systems installed or deployed on or before January 1, 1995."

Ten years on, and $450 million later, the Bureau estimates that "only 10 to 20 percent of the wireline switches, and approximately 50 percent of the pre-1995 and 90 percent of the post-1995 wireless switches, respectively, have CALEA software activated and thus are considered CALEA-compliant."

Sounds like a serious crisis, right? Well, *not exactly*. OIG auditors averred that "we could not provide assurance on the accuracy of these estimates;" a subtle way of saying that the FBI could be ginning-up the numbers–and alleged "threats" to the *heimat* posed by an open internet and wireless networks.

As it turns out, this too is a proverbial red herring.

Whether or not the switches themselves are "CALEA-compliant" is a moot point since the vast majority of ISPs retain search data "in the cloud" indefinitely, just as wireless carriers cache cell phone geolocation and dialed-number data in huge data warehouses seemingly until the end of time, all readily accessible to law enforcement agencies–for a price.

Bringing the Hammer Down

The weakest link in the battle to preserve privacy rights, as ***Washington Technology*** revealed, are the corporate grifters feeding at the federal trough. What with the "cybersecurity" market the newest growth center for enterprising capitalist pirates, why bite the hand that feeds.

Couple this with the brisk private market in grabbing online users' data and selling it to the highest bidder, as *The Wall Street Journal* uncovered in their excellent **"What They Know"** series on web- and cell phone tracking, it becomes clear that profit *always* trumps democratic control and privacy rights.

In light of these disturbing trends, **CNET News** reported that "Democratic politicians are proposing a novel approach to cybersecurity: fine technology companies $100,000 a day unless they comply with directives imposed by the U.S. Department of Homeland Security."

Investigative journalist Declan McCullagh informs us that legislation introduced last week by the lame duck Congress "would allow DHS Secretary Janet Napolitano to levy those and other civil penalties on noncompliant companies that the government deems 'critical,' a broad term that could sweep in Web firms, broadband providers, and even software companies and search engines."

Congressional grifter Rep. Bennie Thompson (D-MS), the outgoing chairman of the House Homeland Security Committee, claimed that the bill "will make our nation more secure and better positions DHS–the 'focal point for the security of cyberspace'–to fulfill its critical homeland security mission," right alongside the National Security Agency as ***Antifascist Calling*** reported last month.

Jim Harper, a policy analyst with the right-wing Cato Institute told CNET that "Congress is stepping forward to regulate something it has no idea how to regulate. It's a level of bureaucracy that actually adds nothing at all."

While Harper's assertion is accurate up to a point, he's missing the boat insofar as demands for expanded–and unregulated–authority by our political minders to access anything and everything even remotely connected to "national security," from email to web searches and from financial transactions to travel plans, is *precisely* the point of an electronic police state.

The bill, the Homeland Security Cyber and Physical Infrastructure Protection Act (HSCPIPA), has "other high-profile backers," including Rep. Jane Harman (D-CA) and Yvette Clarke (D-NY), the outgoing chair of the Cybersecurity Subcommittee.

Last week, ***Antifascist Calling*** reported that Clarke **proclaimed** that "the likelihood of a cyberattack that could bring down our [electrical] grid is … 100%. Our networks are already being penetrated as we stand here. We are already under attack."

Clarke, who raised some $267,938 in campaign contributions during the current election cycle, according to **OpenSecrets.org**, including tens of thousands of dollars from defense and security grifters such as Honeywell International, Dell, AT&T, Raytheon, Verizon, Boeing and General Dynamics, not to mention that sterling citizen and beacon of financial transparency, Goldman Sachs.

With a straight face, she asserted: "We must stop asking ourselves 'could this happen to us' and move to a default posture that acknowledges this fact and instead asks 'what can we do to protect ourselves'?"

With the introduction of HSCPIPA, we now have our answer!

Hardly slouches themselves when it comes to feeding at the corporate security trough, Harman **raked in** $654,787 from firms such as Northrop Grumman, Boeing, Raytheon and Science Applications International Corporation (SAIC), while Thompson **grabbed** $584,938 from firms like SAIC, Boeing, General Dynamics, Raytheon and Lockheed Martin, all of whom do yeoman's work, as readers are well aware, to "keep us safe."

While no Republicans have signed onto the bill, the incoming chairman of the House Homeland Security Committee, ultra-rightist crazy, Rep. Peter King (R-NY), **pulled down** some $664,657 from his loyal constituents: General Dynamics, Goldman Sachs, AT&T, Lockheed Martin and Raytheon, OpenSecrets told us.

King, an apologist for Bush-Obama "War on Terror" policies, told ***Politico*** earlier this month that the practice of torturing terrorism suspects "saved many, many lives." And, like his Democratic Party colleague Clarke, King **avers** that "cyber-spies from foreign countries have already penetrated our electrical system, mapped it and left behind software that caused disruptions and disabled our electrical system."

While neither representative has provided a shred of evidence to back their wild claims, both scrupulously avoid addressing the question of who the most egregious planetary perpetrators of "cyber espionage" actually are.

A Seamless Global Surveillance Web

In a sign that the collapsing American Empire will make new wiretap rules a cost of doing business with the greatest country that ever was, foreign governments and firms that do business in the U.S. were warned that overseas internet service providers "would have to route communications through a server on United States soil where they could be wiretapped," the *Times* reported.

That would certainly give our corporate grifters a leg up on the competition!

Considering that the National Security Agency's ECHELON surveillance platform, accused by the European Parliament in their 2001 **report** of filching communications from EU businesses and passing them on to corporate "friends," I'm sure they'll just smile and suck it up.

According to the report, the NSA routinely used the program for corporate and industrial espionage and that information was turned over to American firms for their financial advantage.

For example, EU investigators discovered that ECHELON spies had "lifted…all the faxes and phone calls" between the European aircraft manufacturer Airbus and Saudi Arabian Airlines. The information gleaned was then used by two American companies, Boeing and McDonnell Douglas, to outflank their Airbus rivals and win a $6 billion contract. Investigators also found that the French company Thomson-CSF lost a $1.3 billion satellite deal to Raytheon the same way.

Similarly, the new communications spying regime proposed by the FBI also has a long and sordid history. In January, investigative journalist Nicky Hager **reported** that under terms of New Zealand's 2004 Telecommunications (Interception Capability) Act, "a basic interception warrant … allows them access to all your emails, internet browsing, online shopping or dating, calls, texts and location for mobile phones, and much more–all delivered almost instantaneously to the surveillance agencies."

Sound familiar? It should, since the template for global driftnet spying originated deep in the bowels of the **UKUSA Security Agreement** and the National Security Agency, the dark Pentagon entity that created ECHELON.

Hager, the author of ***Secret Power***, first blew the lid off ECHELON in a 1996 piece for ***Covert Action Quarterly***. He revealed that the origins of New Zealand's new system "can be traced back 10 years to when British researchers uncovered European Union police documents planning exactly the same sort of surveillance system in Europe."

That secret plan Hager reports, "known as Enfopol 98 … aimed to create 'a seamless web of telecommunications surveillance' across Europe, and involved EU nations adopting 'International User Requirements for Interception', to standardise surveillance capabilities."

Who, pray tell, was in the thick of this nasty business? According to Hager, European researchers discovered "that the moves followed 'a five-year lobbying exercise by American agencies such as the FBI'."

Hager tells us, that similar to moves inside the United States, the island nation's Secret Intelligence Service (SIS) forced through legislation that empowered spooks "to catch … communications, including people using overseas-based email or other services, all the local communications networks are wired up as well, to monitor messages en route overseas."

The origin of these intrusive measures, Hager reports, are the series of conferences, first hosted by the FBI-run International Law Enforcement Telecommunications Seminar (**ILETS**) beginning in the mid-1990s.

According to the document posted by the secrecy-shredding web site **Cryptome**, international snoops averred that "Law enforcement agencies require access to all interception subjects operating temporarily or permanently within a telecommunications system," and that "Law enforcement agencies require a real-time, full-time monitoring capability for the interception of telecommunications. Call associated data should also be provided in real-time."

Fast forward a decade and we learn, Hager writes, that alongside the United States "New Zealand is integrated into the 'seamless web of telecommunications surveillance' around the globe–a system which from the start had primarily been about US agencies wanting surveillance capabilities beyond their borders."

Thus the secret state's desire, as *The New York Times* reported, for legislative authority demanding that foreign citizens and firms route their overseas communications through U.S. servers "where they could be wiretapped."

And with the latest push for "total information awareness"–data retention–looming ever-larger on the horizon, ISPs and wireless carriers "are forced by government to store all their customers' emails, texts, internet use and phone data…making them available to police and spy agencies to trawl for people's past correspondence and activities."

"These developments" Hager writes, "have been introduced quietly. Neither the government nor the phone and internet companies are keen to advertise their Big Brotherish activities."

Now the repressive American domestic intelligence agency that brought us **COINTELPRO**, targets the antiwar movement for "special handling" and gives "aid and comfort" to international terrorists like al-Qaeda triple agent, the false-flag specialist **Ali Mohamed**, is lobbying internet firms Facebook and Google in a bid to expand their onerous surveillance powers.

As the American Civil Liberties Union pointed out last week in their **denunciation** of the FBI's sought-after legislation, "this proposal isn't simply applying the same sort of wiretap system we have for phones to the Internet; it would require reconfiguring and changing the nature of the Internet."

Laura W. Murphy, the Director of the ACLU's Washington Legislative Office said they "remain very concerned that this proposal is a clear recipe for abuse and will make it that much easier for the government to gain access to our most personal information."

"Americans," Murphy averred, "should not simply surrender their privacy and other fundamental values in the name of national security."

And with a growing revolt over egregious sexual assaults and virtual strip searches by Transportation Security Agency goons threatening to break out amongst air travelers, including calls to **resist** being bombarded with ionizing radiation and humiliating TSA "pat-downs," are we on the cusp of a more generalized rebellion against the capitalist surveillance state?

*Tom Burghardt is a researcher and activist based in the San Francisco Bay Area. In addition to publishing in Covert Action Quarterly and **Global Research**, an his articles can be read on **Dissident Voice**, **The Intelligence Daily**, **Pacific Free Press**, **Uncommon Thought Journal**, and the whistleblowing website **WikiLeaks**. He is the editor of Police State America: U.S. Military "Civil Disturbance" Planning, distributed by **AK Press** and has contributed to the new book from **Global Research**, The Global Economic Crisis: The Great Depression of the XXI Century.*

Articles by: Tom Burghardt
http://antifascist-calling.blogspot.com/