GlobalResearch
Center for Research on Globalization

SPYING ON AMERICANS: Obama's Backdoor "Cybersecurity" Wiretap Bill Threatens Political and Private Rights

Spying on Social Media

By Tom Burghardt
Global Research, April 10, 2012
Antifascist Calling... 10 April 2012

Region: USA
Theme: Police State & Civil Rights

Under the guise of "cybersecurity," the new all-purpose bogeyman to increase the secret state's already-formidable reach, the Obama administration and their congressional allies are crafting legislation that will open new backdoors for even more intrusive government surveillance: portals into our lives that will never be shut.

As Antifascist Calling has frequently warned, with the endless "War on Terror" as a backdrop the federal government, most notably the 16 agencies that comprise the so-called "Intelligence Community" (IC), have been constructing vast centralized databases that scoop-up and store all things digital–from financial and medical records to the totality of our electronic communications online–and do so without benefit of a warrant or probable cause.

The shredding of constitutional protections afforded by the Fourth Amendment, granted to the Executive Branch by congressional passage of the Authorization for Use of Military Force (AUMF) after the 9/11 attacks, followed shortly thereafter by the oxymoronic USA Patriot Act set the stage for today's depredations.

Under provisions of multiple bills under consideration by the House and Senate, federal officials will be given broad authority over private networks that will almost certainly hand security officials wide latitude over what is euphemistically called "information-sharing" amongst corporate and government securocrats.

As *The Washington Post* reported in February, the National Security Agency "has pushed repeatedly over the past year to expand its role in protecting private-sector computer networks from cyberattacks" but has allegedly "been rebuffed by the White House, largely because of privacy concerns."

"The most contentious issue," *Post* reporter Ellen Nakashima wrote, "was a legislative proposal last year that would have required hundreds of companies that provide such critical services as electricity generation to allow their Internet traffic to be continuously scanned using computer threat data provided by the spy agency. The companies would have been expected to turn over evidence of potential cyberattacks to the government."

Both the White House and Justice Department have argued, according to the *Post*, that the "proposal would permit unprecedented government monitoring of routine civilian Internet activity."

National Security Agency chief General Keith Alexander, the dual-hatted commander of NSA and U.S. Cyber Command (USCYBERCOM), the Pentagon satrapy that wages offensive cyberwar, was warned to "restrain his public comments after speeches in which he argued that more expansive legal authority was necessary to defend the nation against cyberattacks."

While we can take White House "objections" with a proverbial grain of salt, they do reveal however that NSA, the largest and most well-funded of the secret state's intel shops will use their formidable surveillance assets to increase their power while undermining civilian control over the military in cahoots with shadowy security corporations who do their bidding. (Readers are well-advised to peruse The Surveillance Catalog posted by *The Wall Street Journal* as part of their excellent What They Know series for insight into the burgeoning Surveillance-Industrial Complex).

As investigative journalist James Bamford pointed out recently in *Wired Magazine*, "the exponential growth in the amount of intelligence data being produced every day by the eavesdropping sensors of the NSA and other intelligence agencies" is "truly staggering."

In a follow-up piece for *Wired*, Bamford informed us that when questioned by Congress, Alexander stonewalled a congressional subcommittee when asked whether NSA "has the capability of monitoring the communications of Americans, he never denies it–he simply says, time and again, that NSA can't do it 'in the United States.' In other words it can monitor those communications from satellites in space, undersea cables, or from one of its partner countries, such as Canada or Britain, all of which it has done in the past."

Call it Echelon on steroids, the massive, secret surveillance program first exposed by journalists Duncan Campbell and Nicky Hager.

And with the eavesdropping agency angling for increased authority to monitor the electronic communications of Americans, the latest front in the secret state's ongoing war against privacy is "cybersecurity" and "infrastructure protection."

'Information Sharing' or Blanket Surveillance?

Among the four bills currently competing for attention, the most egregious threat to civil liberties is the Cyber Intelligence Sharing and Protection Act of 2011 (CISPA, H.R. 3523).

Introduced by Mike Rogers (R-MI) and Dutch Ruppersberger (D-MD), the bill amends the National Security Act of 1947, adding language concerning so-called "cyber threat intelligence and information sharing."

"Cyber threat intelligence" is described as "information in the possession of an element of the intelligence community directly pertaining to a vulnerability of, or threat to, a system or network of a government or private entity, including information pertaining to the protection of a system or network from: (1) efforts to degrade, disrupt, or destroy such system or network; or (2) theft or misappropriation of private or government information, intellectual property, or personally identifiable information."

In keeping with other "openness" mandates of our Transparency Administration™ the Rogers bill will require the Director of National Intelligence (DNI) to establish procedures that permit IC elements to "share cyber threat intelligence with private-sector entities, and (2) encourage the sharing of such intelligence."

These measures however, will *not* protect the public at large from attacks by groups of organized cyber criminals since such intelligence is only "shared with certified entities or a person with an appropriate security clearance," gatekeepers empowered by the state who ensure that access to information is "consistent with the need to protect U.S. national security, and used in a manner that protects such intelligence from unauthorized disclosure."

In other words, should "cleared" cyber spooks be directed by their corporate or government masters to install state-approved malware on private networks as we discovered last year as a result of the HBGary hack by Anonymous, it would be a crime punishable by years in a federal gulag if official lawbreaking were disclosed.

The bill authorizes "a cybersecurity provider (a non-governmental entity that provides goods or services intended to be used for cybersecurity purposes)," i.e., an outsourced contractor from any one of thousands of spooky "cybersecurity" firms, to use "cybersecurity systems to identify and obtain cyber threat information in order to protect the rights and property of the protected entity; and share cyber threat information with any other entity designated by the protected entity, including the federal government."

Furthermore, the legislation aims to regulate "the use and protection of shared information, including prohibiting the use of such information to gain a competitive advantage and, if shared with the federal government, exempts such information from public disclosure."

And should the public object to the government or private entities trolling through their personal data in the interest of "keeping us safe" well, there's an app for that too! The bill "prohibits a civil or criminal cause of action against a protected entity, a self-protected entity (an entity that provides goods or services for cybersecurity purposes to itself), or a cybersecurity provider acting in good faith under the above circumstances."

One no longer need wait until constitutional violations are uncovered, the Rogers bill comes with a get-out-of-jail-free card already in place for state-approved scofflaws.

Additionally, the bill also "preempts any state statute that restricts or otherwise regulates an activity authorized by the Act." In other words, in states like California where residents have "an inalienable right to privacy" under Article 1, Section 1 of the State Constitution, the Rogers bill would be abolish that right and effectively "legalize" unaccountable snooping by the federal government or other "self-protected," i.e., private entities deputized to do so by the secret state.

Social Media Spying

How would this play out in the real world? As *Government Computer News* reported, hyped-up threats of an impending "cyber-armageddon" have spawned a host of new actors constellating America's Surveillance-Industrial Complex: the social media analyst.

> "Companies and government agencies alike are using tools to sweep the Internet–blogs, websites, and social media such as Facebook and Twitter feeds–to find out what people are saying about, well, just about anything."

Indeed, as researchers Jerry Brito and Tate Watkins pointed out last year in *Loving the Cyber*

Bomb?, "An industrial complex reminiscent of the Cold War's may be emerging in cybersecurity today."

Brito and Watkins averred that "the military-industrial complex was born out of exaggerated Soviet threats, a defense industry closely allied with the military and Department of Defense, and politicians striving to bring pork and jobs home to constituents. A similar cyber-industrial complex may be emerging today, and its players call for government involvement that may be superfluous and definitely allows for rent seeking and pork barreling."

Enter social media analysis and the private firms out to make a buck–at our expense.

> "Not surprisingly," GCN's Patrick Marshall wrote, "intelligence agencies have already been looking at social media as a source of information. The Homeland Security Department has been analyzing traffic on social networks for at least the past three years."

While DHS claims it does not routinely monitor Facebook or Twitter, and only responds when it receives a "tip," such assertions are demonstrably false.

Ginger McCall, the director of the Electronic Electronic Privacy Information Center's Open Government Program told *GCN* that the department is "explicitly monitoring for criticism of the government, for reports that reflect adversely on the agency, for public reaction to policy proposals."

But DHS isn't the only agency monitoring social media sites such as Facebook and Google+.

As *Antifascist Calling* reported back in 2009, according to *New Scientist* the National Security Agency "is funding research into the mass harvesting of the information that people post about themselves on social networks."

Not to be outdone, the CIA's venture capital investment arm, In-Q-Tel, has poured millions of dollars into Visible Technologies, a Bellevue, Washington-based firm specializing in "integrated marketing, social servicing, digital experience management, and consumer intelligence."

According to In-Q-Tel "Visible Technologies has developed TruCast®, which takes an innovative and holistic approach to social media management. TruCast has been architected as an enterprise-level solution that provides the ability to track, analyze, and respond to social media from a single, Web-based platform."

Along similar lines, the CIA has heavily invested in Recorded Future, a firm which "extracts time and event information from the web. The company offers users new ways to analyze the past, present, and the predicted future."

The firm's defense and intelligence analytics division promises to "help analysts understand trends in big data, and foresee what may happen in the future. Groundbreaking algorithms extract temporal and predictive signals from unstructured text. Recorded Future organizes this information, delineates results over interactive timelines, visualizes past trends, and maps future events–all while providing traceability back to sources. From OSINT to classified data, Recorded Future offers innovative, massively scalable solutions."

As *Government Computer News* pointed out, in January the FBI "put out a request for vendors to provide information about available technologies for monitoring and analyzing social media." Accordingly, the Bureau is seeking the ability to:

> • Detect specific, credible threats or monitor adversarial situations.
>
> • Geospatially locate bad actors or groups and analyze their movements, vulnerabilities, limitations, and possible adverse actions.
>
> • Predict likely developments in the situation or future actions taken by bad actors (by conducting trend, pattern, association, and timeline analysis).
>
> • Detect instances of deception in intent or action by bad actors for the explicit purpose of misleading law enforcement.
>
> • Develop domain assessments for the area of interest (more so for routine scenarios and special events).
>
> So much for privacy in our Orwellian New World Order!

Backdoor Official Secrets Act

Social media "harvesting" by private firms hot-wired into the state's Surveillance-Industrial Complex will be protected from challenges under provisions of CISPA.

As the Electronic Frontier Foundation (EFF) pointed out, "a company that protects itself or other companies against 'cybersecurity threats' can 'use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property' of the company under threat. But because 'us[ing] cybersecurity systems' is incredibly vague, it could be interpreted to mean monitoring email, filtering content, or even blocking access to sites. A company acting on a 'cybersecurity threat' would be able to bypass all existing laws, including laws prohibiting telcos from routinely monitoring communications, so long as it acted in 'good faith'."

And as EFF's Rainey Reitman and Lee Tien aver, the "broad language" concerning what constitutes a cybersecurity "threat," is an invitation for the secret state and their private "partners" to include "theft or misappropriation of private or government information, intellectual property, or personally identifiable information."

"Yes," Reitman and Tien wrote, "intellectual property. It's a little piece of SOPA wrapped up in a bill that's supposedly designed to facilitate detection of and defense against cybersecurity threats. The language is so vague that an ISP could use it to monitor communications of subscribers for potential infringement of intellectual property. An ISP could even interpret this bill as allowing them to block accounts believed to be infringing, block access to websites like The Pirate Bay believed to carry infringing content, or take other measures provided they claimed it was motivated by cybersecurity concerns."

More troubling, "the government and Internet companies could use this language to block sites like WikiLeaks and NewYorkTimes.com, both of which have published classified information."

Should CISPA pass muster it could serve as the basis for establishing an American "Official

Secrets Act." In the United Kingdom, the Act has been used against whistleblowers to prohibit disclosure of government crimes. But it does more than that. The state can also issue restrictive "D-Notices" that "advise" editors not to publish material on subjects deemed sensitive to the "national security."

EFF warns that "online publishers like WikiLeaks are currently afforded protection under the First Amendment; receiving and publishing classified documents from a whistleblower is a common journalistic practice. While there's uncertainty about whether the Espionage Act could be brought to bear against WikiLeaks, it is difficult to imagine a situation where the Espionage Act would apply to WikiLeaks without equally applying to the New York Times, the Washington Post, and in fact everyone who reads about the cablegate releases."

And with the Obama regime's crusade to prosecute and punish whistleblowers, as the recent indictment of former CIA officer John Kiriakou for alleged violations of the Espionage Act and the Intelligence Identities Protection Act for disclosing information on the CIA's torture programs, we have yet another sterling example of administration "transparency"! While Kiriakou faces 30 years in prison, the former head of the CIA's Directorate of Operations, Jose A. Rodriguez Jr., who was responsible for the destruction of 92 torture videotapes held by the Agency, was not charged by the government and was given a free pass by the Justice Department.

As the *World Socialist Web Site* points out: "More fundamentally, the prosecution of Kiriakou is part of a policy of state secrecy and repression that pervades the US government under Obama, who came into office promising 'the most transparent administration in history.'"

Critic Bill Van Auken observed that Kiriakou's prosecution "marks the sixth government whistleblower to be charged by the Obama administration under the Espionage Act, twice as many such prosecutions as have been brought by all preceding administrations combined. Prominent among them is Private Bradley Manning, who is alleged to have leaked documents exposing US war crimes to WikiLeaks. He has been held under conditions tantamount to torture and faces a possible death penalty."

"In all of these cases," the *World Socialist Web Site* noted, "the World War I-era Espionage Act is being used to punish not spying on behalf of a foreign government, but exposing the US government's own crimes to the American people. The utter lawlessness of US foreign policy goes hand in hand with the collapse of democracy at home."

The current crop of "cybersecurity" bills are sure to hasten that collapse.

Under Rogers' legislation, "the government would have new, powerful tools to go after WikiLeaks," or anyone else who challenges the lies of the U.S. government by publishing classified information that contradicts the dominant narrative.

"By claiming that WikiLeaks constituted 'cyber threat intelligence' (aka 'theft or misappropriation of private or government information')," EFF avers, "the government may be empowering itself and other companies to monitor and block the site. This means that the previous tactics used to silence WikiLeaks–including a financial blockade and shutting down their accounts with online service providers–could be supplemented by very direct means. The government could proclaim that WikiLeaks constitutes a cybersecurity threat and have new, broad powers to filter and block communication with the journalistic website."

Since January, Obama has signed legislation (NDAA) granting the Executive Branch authority to condemn alleged “enemy combatants,” including U.S. citizens detained in America, indefinite military detention without charges or trials, and with U.S. Attorney General Eric Holder asserting that the president has the “right” to assassinate American citizens anywhere on earth, its clear to anyone who hasn’t drunk the Hope and Change™ Kool-Aid, that the architecture of an American police state is now in place.

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, he is a Contributing Editor with Cyrano’s Journal Today. His articles can be read on Dissident Voice, 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/