GlobalResearch
Center for Research on Globalization

CYBER INTELLIGENCE AND INTERNET SPYING: House Passes Draconian Internet Spying Bill

By Tom Burghardt
Global Research, April 29, 2012
Antifascist Calling... 29 April 2012

Region: USA
Theme: Police State & Civil Rights

On April 26, 2012, the U.S. House of Representatives passed the draconian Cyber Intelligence Sharing and Protection Act (H.R. 3523 or CISPA) by a vote of 248-168, with 206 Republicans and 42 Democrats voting in favor.

If the legislation passes muster in the Senate and is signed by President Obama (who has threatened a veto, but don't hold your breath), it would allow private firms–internet service providers (ISPs), telecoms and wireless providers–to hand over personal information about users to law enforcement and security agencies.

This unprecedented power-grab by a cabal of giant corporations and the federal government would take place under the guise of "cybersecurity," the latest front in the secret state's assault on Americans' civil liberties and privacy rights.

While the bill's sponsors and supporters claim that any "information-sharing" of personal data would be "voluntary," it would occur without benefit of a warrant or a court order and automatically "exempts such information from public disclosure."

Denouncing the bill, the ACLU's Michelle Richardson said that CISPA's "biggest and most fundamental flaw" is that it empowers "the military, including agencies like the NSA, to collect the internet records of Americans' everyday internet use."

CISPA is the latest in a series of repressive measures that have incrementally rolled-back the Bill of Rights since 1995's Oklahoma City bombing and the 9/11 terrorist provocations. Under successive Democratic and Republican administrations fundamental constitutional protections, specifically those guaranteed by the First, Fourth and Fifth Amendments, have been gutted.

Beginning with the Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA), which severely limited the rights of prisoners to obtain habeas corpus relief from federal courts, 2001's Authorization for Use of Military Force (AUMF) which handed the Executive Branch carte blanche to wage endless, undeclared wars, and now the National Defense Authorization Act of 2012 (NDAA), which empowers the President to order the military to pick up and indefinitely imprison anyone, anywhere in the world declared a "terrorist," including American citizens detained on U.S. soil, without charge or trial, the architecture of a police state is firmly in place.

> "In the past decade," the Electronic Frontier Foundation's (EFF) Trevor Timm averred, "the amorphous phrase 'national security' has invaded many arenas of government action, and has been used to justify much activity that did not

> involve legitimate terrorist threats. The most obvious (and odious) example is the unfortunately named USA-PATRIOT Act, a law that was sold to the American public as essential to combating terrorism, but which has overwhelmingly been applied to ordinary American citizens never even suspected of terrorism."

Citing the example of the FBI, Timm pointed out that under the rubric of "stopping terrorism" the Bureau "issued more than 192,000 National Security Letters to get Americans' business, phone or Internet records without a warrant. These invasive letters–which come with a gag order on the recipient so they can't even admit they received one–have been used to gather information about untold number of ordinary citizens, including journalists."

Indeed, "'Information sharing'–CISPA's mantra–has also created privacy nightmares for everyday Americans in the name of national security. The federal government routinely shares its massive national security databases with local law enforcement agencies with predictable results."

Amongst CISPA's controversial provisions, the Director of National Intelligence (DNI), the *Obergruppenführer* of America's 16-agency Intelligence Community, "shall issue guidelines providing that the head of an element of the intelligence community may, as the head of such element considers necessary to carry out this subsection: (A) grant a security clearance on a temporary or permanent basis to an employee or officer of a certified entity; (B) grant a security clearance on a temporary or permanent basis to a certified entity and approval to use appropriate facilities; and (C) expedite the security clearance process for a person or entity as the head of such element considers necessary, consistent with the need to protect the national security of the United States."

Under "Definitions," (1) a "certified entity" is described as a "protected entity, self-protected entity, or cybersecurity provider that–(A) possesses or is eligible to obtain a security clearance, as determined by the Director of National Intelligence; and (B) is able to demonstrate to the Director of National Intelligence that such provider or such entity can appropriately protect classified cyber threat intelligence."

> "(2) The term 'cyber threat information' means information 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–(A) efforts to degrade, disrupt, or destroy such system or network; or (B) theft or misappropriation of private or government information, intellectual property, or personally identifiable information. (3) Cyber threat intelligence.–The term 'cyber threat intelligence' means 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–(A) efforts to degrade, disrupt, or destroy such system or network; or (B) theft or misappropriation of private or government information, intellectual property, or personally identifiable information."

According to this reading, a "certified entity" is any one of the thousands of über-secretive "cybersecurity firms" with their stable of "cleared" employees who hold top secret and above security clearances who rely upon and do the bidding of their masters–corporate shareholders and the federal government.

The bill's draconian language would in essence transform investigative journalism and whistleblowing into a crime since "the theft or misappropriation of private or government information, intellectual property, or personally identifiable information" is *precisely* the meat and potatoes used by journalists and outraged citizens to uncover corporate and government lawbreaking.

Indeed under CISPA, the employees of firms such as the ultra-spooky Endgame Systems, SAIC, Lockheed Martin, or General Dynamics, the designers of "boutique cyber weapons" for the government as *BusinessWeek* disclosed last summer, would ply their dirty trade in destructive algorithmic weapons with more than a wink-and-a-nod: they would be empowered to do so and earn big bucks (courtesy of U.S. taxpayers) in the process!

To get a sense of some of the surveillance "products" which have transformed private data into weaponized kit for the secret state, readers are well-advised to peruse The Spyfiles published last December by the whistleblowing web site WikiLeaks.

> "In the last ten years," WikiLeaks informed us, "systems for indiscriminate, mass surveillance have become the norm. Intelligence companies such as VASTech secretly sell equipment to permanently record the phone calls of entire nations. Others record the location of every mobile phone in a city, down to 50 meters. Systems to infect every Facebook user, or smart-phone owner of an entire population group are on the intelligence market."

To cite but one example culled from The Spyfiles, NICE Systems, founded by "retired" members of Israel's equivalent of the National Security Agency, Unit 8200, has become a key player in the global Surveillance-Industrial Complex.

With decades of experience surveilling, tracking and repressing Palestinian and left-wing activists at home and abroad, the NiceTrack Mass Detection Center is a perfect tool that provides "nationwide interception, monitoring and analysis" to enterprising securocrats who need a leg-up on home-grown "subversive elements."

Accordingly, the Mass Detection Center "helps intelligence organizations and national security agencies fight terrorism and reduce national threat levels. It supports both mass and target monitoring workflows and helps operators and analysts find new suspects, generate new leads and monitor existing targets." Indeed, the software suite "stores and analyzes all types of telephony and Internet content." We're informed that "collecting and storing nationwide data enables broadening the scope of target information and performing on-going and post-event investigations."

NiceTrack Target 360° according to brochures published by WikiLeaks "is the leading communication intercept system for tracking, monitoring, and investigating targets' activities, securing 1.5 billion people worldwide." Indeed, "the system is designed to provide Law Enforcement Agencies (LEAs), intelligence organizations and SIGINT agencies with hermetic 360° target monitoring by collecting, processing, retaining and analyzing any type of communication activity."

Amongst the product's "Key Benefits" we learn that Target 360° can "help" law enforcement "reduce crime, prevent terrorism" and "identify other security threats" by providing "persistent situation awareness" of a "target" through "advanced IP monitoring," "open source intelligence" and "lawful hacking."

Additionally, Target 360° can "manage and efficiently structure millions of internet activities and unstructured data into a simple and meaningful intelligence picture." Target 360° "is designed to handle all types of Web 2.0 internet applications, including Facebook, Twitter and other social networks, forums, chats, and e-mails, and is scalable to support new services" and can "be integrated with legacy systems for telephony and mobile interception and provide a comprehensive solution for all types of communication interception."

As numerous critics and journalists have pointed out, the privatization of the government's intelligence and security functions, theoretically transparent under provisions of the Freedom of Information Act (FOIA), would, under CISPA, fall under the purview of the Department of Homeland Security (DHS) and the National Security Agency (NSA) where "disclosure" is little more than a euphemism for "down the memory hole."

In all likelihood, privatized spooks would be exempt from revealing the state's blanket surveillance of its citizens under any number of provisions built into the Freedom of Information Act.

For example under section (b)(1), the secret state can prevent "disclosure [of] national security information concerning the national defense or foreign policy, provided that it has been properly classified in accordance with the substantive and procedural requirements of an executive order."

Can you say "state secrets privilege," Sibel Edmonds or Thomas Drake?

Since, an "an employee or officer of a certified entity," i.e., a private contractor, telecom or ISP will be empowered by Congress to share user information with NSA and other departments of the federal government, such information "shall be considered proprietary information and shall not be disclosed to an entity outside of the Federal Government except as authorized by the entity sharing such information."

Under CISPA it will be virtually impossible for the average citizen to learn whether they have been spied upon since Section (b)(4) of FOIA specifically protects "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential. This exemption is intended to protect the interest of both the government and submitter of information."

And once an "employee or officer of a certified entity" has been "read into" a CIA, FBI, DHS or NSA black program, they are automatically exempt from disclosing such information to a lawful court since CISPA "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."

With CISPA, official lawbreaking is automatically precluded from review by a lawful court and the average citizen, who may have lost their job because of malicious or flawed data collected by a "certified entity" will be stripped of their ability to obtain compensation from deputized cyber snoops "acting in good faith."

Most controversially perhaps, the statute reads: "notwithstanding any other provision of law," companies can share information "with any other entity, including the federal government."

As CNET News analyst Declan McCullagh pointed out, "By including the word 'notwithstanding,' House Intelligence Committee Chairman Mike Rogers (R-Mich.) and ranking member Dutch Ruppersberger (D-Md.) intended to make CISPA trump all existing federal and state civil and criminal laws."

Indeed, by inserting the word "notwithstanding" into the legislation, it "would trump wiretap laws, Web companies' privacy policies, gun laws, educational record laws, census data, medical records, and other statutes that protect information," McCullagh wrote.

As noted above, "CISPA's authorization for information sharing extends far beyond Web companies and social networks. It would also apply to Internet service providers, including ones that already have an intimate relationship with Washington officialdom," CNET reported.

> "Large companies including AT&T and Verizon handed billions of customer records to the NSA; only Qwest refused to participate," McCullagh reminded us. "Verizon turned over customer data to the FBI without court orders. An AT&T whistleblower accused the company of illegally opening its network to the NSA, a practice that the U.S. Congress retroactively made legal in 2008."

What's to prevent firms such as Google, Facebook or Twitter from turning over our private data to the government, after all, they have their customers' best interests at heart as part of their business model, right? Better think again!

The New York Times reported Sunday that that "Google's harvesting of e-mails, passwords and other sensitive personal information from unsuspecting households in the United States and around the world was neither a mistake nor the work of a rogue engineer, as the company long maintained, but a program that supervisors knew about, according to new details from the full text of a regulatory report."

That report, prepared by the Federal Communications Commission "draws a portrait of a company where an engineer can easily embark on a project to gather personal e-mails and Web searches of potentially hundreds of millions of people as part of his or her unscheduled work time, and where privacy concerns are shrugged off."

> "As early as 2007," the Times disclosed, "Street View engineers had 'wide access' to the plan to collect payload data. Five engineers tested the Street View code, a sixth reviewed it line by line, and a seventh also worked on it, the report says."
>
> "Google's rogue engineer scenario collapses in light of the fact that others were aware of the project and did not object," Marc Rotenberg, the executive director of the Electronic Privacy Information Center told the Times. "This is what happens in the absence of enforcement and the absence of regulation."

Such practices will be infinitely worse under CISPA. Google's harvesting of their customers' private data or Facebook's routine cooperation with law enforcement "requests" for users' information could in fact be turned over whenever an intelligence agency declares that doing so is in the interest of national- or cybersecurity and we would have no way of ever learning about it since harvested emails, web searches and stored profiles could be deemed "proprietary information."

With a ginned-up panic over “cybersecurity” taking its place alongside imperialism’s other “wars” on “terror,” “drugs” and “crime,” the secret state’s “unprecedented attacks on democratic rights, in which the entire political establishment and both Democrats and Republicans are participating,” as the *World Socialist Web Site* warned, “must be understood as preemptive preparations by the political establishment to meet the coming social upheavals with police state measures.”

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/