GlobalResearch
Center for Research on Globalization

Crypto Wars! Obama Wants New Law to Wiretap the Internet

By Tom Burghardt
Global Research, October 04, 2010
Antifascist Calling... 3 October 2010

Region: USA
Theme: Intelligence, Law and Justice

In a reprise of the crypto wars of the 1990s, the U.S. secret state is mounting an offensive that would force telecommunication companies to redesign their systems and information networks to more easily facilitate internet spying.

Touted as a simple technical "fix" that would "modernize" existing legislation for wiretaps, government security officials will demand that telecommunication firms and internet service providers provide law enforcement with backdoors that would enable them to bypass built-in encryption and security features of electronic communications.

With the Obama administration rivaling, even surpassing antidemocratic moves by the Bush regime to monitor and surveil the private communications of the American people, The New York Times reported last week that "federal law enforcement and national security officials are preparing to seek sweeping new regulations for the Internet."

Following closely on the heels of FBI raids on antiwar and international solidarity activists, the "change" administration now wants Congress to require all providers who enable communications "to be technically capable of complying if served with a wiretap order."

Times' reporter Charlie Savage informs us that the administration will demand that software and communication providers build backdoors accessible to law enforcement and intelligence agencies, thus enabling 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."

Calling new legislative strictures a "reasonable" and "necessary" tool for law enforcement that will "prevent the erosion of their investigative powers," FBI mouthpiece, general counsel Valerie E. Caproni, told the Times, "We're talking about lawfully authorized intercepts."

Really?

Caproni's assertion that the Bureau and spy shops such as the National Security Agency are not interested in "expanding authority" but rather "preserving our ability to execute our existing authority in order to protect the public safety and national security," is a thin tissue of lies lacking credibility.

In fact, the state's "existing authority" to spy upon private communications under the USA Patriot Act and assorted National Security- and Homeland Security Presidential Directives

(NSPD/HSPD) in areas as such as “continuity of government” (NSPD 51/HSPD 20), “cybersecurity” (NSPD 54/HSPD 23) and “biometrics” (NSPD 59/HSPD 24), have led to the creation of overly broad and highly classified programs regarded as “state secrets” under Obama.

As I have written many times, most recently in August (see: “Obama Demands Access to Internet Records, in Secret, and Without Court Review,” Antifascist Calling, August 12, 2010), since his 2009 inauguration President Obama has done nothing to reverse this trend. Indeed, he has taken further steps through the Comprehensive National Cybersecurity Initiative (CNCI), a highly-sanitized version of NSPD 54/HSPD 23, to ensure that the “President’s Surveillance Program” (PSP) launched by Bush remains a permanent feature of daily life in the United States.

In a widely circulated report last year, the inspectors general from five federal agencies, including the Justice Department, the Defense Department, the Central Intelligence Agency, the National Security Agency and the Office of the Director of National Intelligence, noted that following advice from the Office of Legal Counsel under torture-enablers Jay Bybee and John C. Yoo, “the President authorized the NSA to undertake a number of new, highly classified intelligence activities” that went far beyond warrantless wiretapping in their scope, encompassing additional unspecified “activities” that have never been disclosed to the public.

What were once regarded by Democrats and their ever-shrinking base of acolytes, cheerleaders and toadies as unspeakable crimes when carried out by Republican knuckle-draggers, are now regarded as “forward thinking,” even “visionary” policies when floated by the faux “progressive” occupying the Oval Office.

And with “homegrown terrorism” and “cybersecurity” high priorities on the administration’s to-do list, White House changelings and their friends from the previous regime are pulling out all the stops.

Last week, speaking at a Washington, D.C. “Ideas Forum,” former Director of National Intelligence Mike McConnell, currently a top executive with the spooky Booz Allen Hamilton private security corp, said that cybersecurity is the “wolf at the door” and that a “large-scale” cyberattack “could impact the global economy ‘an order of magnitude surpassing’ the attacks of September 11,”The Atlantic reported.

McConnell and former Bushist Homeland Security Adviser, Frances Fragos Townsend, the current chairwoman of the Intelligence and National Security Alliance (INSA), a D.C. lobby shop catering to security and intelligence grifters, urged the Obama administration to transform “how it defends against cyberattacks,” claiming that the secret state “lack[s] the organizational ability and authorization to prevent and respond to cybersecurity threats.”

Their prescription? Let NSA pit bulls off the leash, of course! Townsend said that “the real capability in this government is in the National Security Agency.”

True enough as far as it goes, however Townsend mendaciously asserted that NSA is legally forbidden from domestic spying, not that it prevented her former boss from standing up NSA’s internal surveillance apparatus through programs such as STELLAR WIND and PINWALE, the agency’s domestic email interception program.

Both Townsend and McConnell claim that the "laws haven't kept up" with the alleged threat posed by a cyberattack and urged the administration to give the NSA even more authority to operate domestically.

No mention was made by liberal interventionist-friendly Atlanticreporter Max Fisher that McConnell's firm has reaped multiyear contracts worth billions for their classified cybersecurity work for the secret state.

Hardly slouches themselves when it comes to electronic eavesdropping, the FBI is seeking to expand their already-formidable capabilities through their "Going Dark" program.

As Antifascist Calling previously reported (see: "FBI 'Going Dark.' Budget Request for High-Tech Surveillance Capabilities Soar," May 17, 2009), the Bureau sought–and received–$233.9 billion in FY 2010 for the development of a new advanced electronic surveillance program.

ABC News first disclosed the program last year, and reported that "the term 'Going Dark' does not refer to a specific capability, but is a program name for the part of the FBI, Operational Technology Division's (OTD) lawful interception program which is shared with other law enforcement agencies."

According to ABC, "the term applies to the research and development of new tools, technical support and training initiatives."

The New York Times reported last week that OTD spent $9.75 million last year "helping communications companies" develop "interception capabilities" for the Bureau.

Administration Hypocrisy

The administration's push for more control is all the more ironic considering that the U.S. State Department according toReuters, said in August it was "disappointed" that "the United Arab Emirates planned to cut off key BlackBerry services, noting the Gulf nation was setting a dangerous precedent in limiting freedom of information."

As The Washington Post told us at the time, UAE securocrats claimed that "it will block key features on BlackBerry smartphones because the devices operate beyond the government's ability to monitor."

Citing–what else!–"national security concerns," the measure "could" be motivated "in part" by state fears that "the messaging system might be exploited by"–wait!–"terrorists or other criminals who cannot be monitored by local authorities."

That regional beacon of democracy, Saudi Arabia, said it would follow suit. In response, State Department shill P.J. Crowley said that the United States is "committed to promoting the free flow of information. We think it's integral to an innovative economy."

With a straight face, Crowley told a State Department news briefing, "It's about what we think is an important element of democracy, human rights and freedom of information and the flow of information in the 21st century."

"We think it sets a dangerous precedent," he said. "You should be opening up societies to

these new technologies that have the opportunity to empower people rather than looking to see how you can restrict certain technologies."

Pointing out the Obama regime's hypocrisy, Yousef Otaiba, the UAE Ambassador to the United States counteracted and said it was Crowley's comments that were "disappointing" and that they "contradict the U.S. government's own approach to telecommunication regulation."

"Importantly," Otaiba said, "the UAE requires the same compliance as the U.S. for the very same reasons: to protect national security and to assist in law enforcement."

The BBC informed us in July that Emirate officials are concerned that the encrypted software and networks used by Research in Motion, BlackBerry's parent company, "make it difficult for governments to monitor communications."

Although this is precisely the autocratic mindset that rules the roost here in the heimat, corporate media report identicalmoves by the U.S. government with nary a critical word, failing to point out the disconnect between administration rhetoric and ubiquitous "facts on the ground."

Among the proposals being considered by the administration, the Times reports that officials "are coalescing" around several "likely requirements" that include the following: "Communications services that encrypt messages must have a way to unscramble them." U.S. law will apply to overseas businesses, not just domestic firms. The Times avers that "Foreign-based providers that do business inside the United States must install a domestic office capable of performing intercepts." And finally, a kiss of death for privacy rights, "Developers of software that enables peer-to-peer communication must redesign their service to allow interception."

Firms that fail to comply "would face fines or some other penalty." The Times neglected to tell us however, what penalties await software developers or individual users who have the temerity to design–or avail themselves–of systems that bypass backdoors mandated by the secret state.

An Electronic Police State

Far from being an "enhanced security feature," the administration's proposal for peer-to-peer snooping would be a boon to hackers, thieves and other miscreants who routinely breech and exploit whatever "firewall" grifting firms and their political allies devise to "keep us safe."

In fact, as computer security and privacy researchers Christopher Soghoian and Sid Stamm revealed in their paper,Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL, secret state agencies havealready compromised the Secure Socket Layer certification process (SSL, the tiny lock that appears during supposedly "secure," encrypted online transactions), and do so routinely.

In March, Soghoian and Stamm introduced the public to "a new attack, 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."

The intrepid researchers provided “alarming evidence” suggesting “this attack is in active use,” and that a niche security firm, Packet Forensics, is already marketing “extremely small, covert surveillance devices for networks” to government agencies.

It now appears that the Obama administration will soon be seeking legislative authority from Congress that legalizes surreptitious snooping by security officials and a coterie of outsourced contractors who grow fat subverting our privacy rights.

Commenting on the administration’s proposal in a recent post, Soghoian points out that when wiretap reporting requirements were amended in 2000, similar arguments were made that strong encryption would “harm national security.”

Congress inserted language that compelled secret state agencies like the FBI to “include statistics on the number of intercept orders in which encryption was encountered and whether such encryption prevented law enforcement from obtaining the plain text of communications intercepted pursuant to such order.”

It didn’t.

However in a replay of the crypto wars of the 1990s, FBI general counsel Caproni brushed off breech of privacy concerns and told the Times that service providers “can promise strong encryption. They just need to figure out how they can provide us plain text.”

Senator Patrick Leahy (D-VT) argued a decade ago that “compiling the statistics would be a ‘far more reliable basis than anecdotal evidence on which to assess law enforcement needs and make sensible policy in this area’.”

“Since then,” Soghoian writes, “the Administrative Office of the US Courts has compiled an annual wiretap report, which reveals that encryption is simply not frequently encountered during wiretaps, and when it is, it never stops the government from collecting the evidence they need.”

In light of statistical evidence provided by the government itself, demands that communications’ providers cough-up their customers’ private data to unaccountable government snoops is quintessentially a political decision, and not, as mendaciously claimed, a “law enforcement” let alone a “national security” problem.

In fact, while police and intelligence agencies “look through thousands of individuals’ email communications, search engine requests or private, online photo albums each year,” they don’t “obtain wiretap orders to intercept that data in real time. Instead,” Soghoian tells us “[they] simply wait a few minutes, and then obtain what they want after the fact as a stored communication under 18 USC 2703,” the Stored Communications Act.

“Unfortunately,” Soghoian avers, “while we have a pretty good idea about how many wiretaps law enforcement agencies obtain each year, we have no idea how many times they go to email, search engine and cloud computing providers to compel them to disclose their customers’ communications and other private data.”

Therefore, “we find ourselves in the same situation as 12 years ago, where law enforcement officials were making anecdotal claims for which no evidence existed to prove, or disprove them.”

As security expert Bruce Schneier pointed out, while the "proposal may seem extreme ... it's not unique." Averring that sinister snooping laws were "formerly reserved for totalitarian countries," Schneier writes "this wholesale surveillance of citizens has moved into the democratic world as well."

Citing moves by Sweden, Canada and Britain to hand "their police new powers of internet surveillance" compelling "communications system providers to redesign products and services they sell," securocrats, as is their wont, are lusting after the capacity to transform all aspects of daily life into "actionable intelligence."

On top of this, as Schneier and others such as Cryptohippie andQuintessenz have revealed, so-called democratic states, not just usual suspects like China (whose "Golden Shield" was designed by Western firms, after all) "are passing data retention laws, forcing companies to retain customer data in case they might need to be investigated later."

In their 2010 report, The Electronic Police State, Cryptohippieinformed us that data retention "is criminal evidence, ready for use in a trial, and that "it is gathered universally ('preventively') and only later organized for use in prosecutions."

How does such a system work? What are the essential characteristics that differentiate an Electronic Police State from previous forms of oppressive governance? Cryptohippie avers:

"In an Electronic Police State, every surveillance camera recording, every email sent, every Internet site surfed, every post made, every check written, every credit card swipe, every cell phone ping... are all criminal evidence, and all are held in searchable databases. The individual can be prosecuted whenever the government wishes."

As the World Socialist Web Site points out, the proposal by the Obama regime "goes far beyond anything envisioned by the Bush administration."

While the White House claims that new legislation is needed to combat "crime" and "terrorism," socialist critic Patrick Martin writes that "the Obama administration has defined 'terrorism' so widely that the term now covers a vast array of constitutionally protected forms of political opposition to the policies of the US government, including speaking, writing, political demonstrations, even the filing of legal briefs."

Just ask activists raided last month by FBI bully-boys in Minneapolis and Chicago!

The American Civil Liberties Union denounced the proposal and called on Congress to reject calls "to make the Internet wiretap ready."

ACLU Legislative Counsel Christopher Calabrese derided the move, saying: "Under the guise of a technical fix, the government looks to be taking one more step toward conducting easy dragnet collection of Americans' most private communications."

Clamping Down on the Freedom of Information Act

Entreaties by civil libertarians however, are likely to fall on deaf ears in the Democratic-controlled Congress.

In a clear sign that the Obama administration is moving to clamp down further on the free flow of information even as they seek access to all of ours', Politico reported that the Office

of the Director of National Intelligence (ODNI) “appears to be on the verge of prevailing in an attempt to put some information it receives from other intelligence agencies beyond the reach of Freedom of Information Act requests.”

National Counterterrorism Center Director Michael Leiter pushed through an onerous section to Intelligence Authorization Act legislation that exempts so-called “operational files” from four secret state agencies–the CIA, NSA, National Reconnaissance Office and the National Geospatial-Intelligence Agency–from FOIA requests.

Apparently the American people, long the targets of illegal driftnet spying by the intelligence and security apparatus, will soon find another door slammed shut, even as the administration claims sweeping new powers, including the right to assassinate American citizens deemed “terrorists,” in secret and without due process, anywhere on the planet.

And they call this transparency…

The original source of this article is Antifascist Calling...

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