Broad Email Spying in America

Senate Bill Sets the Stage?

By Tom Burghardt
Global Research, December 01, 2012
Antifascist Calling...

Region: USA
Theme: Intelligence, Law and Justice, Police State & Civil Rights

A Senate proposal claiming to "protect" Americans' email privacy from unwarranted secret state intrusions "has been quietly rewritten, giving government agencies more surveillance power than they possess under current law," CNET revealed.

As provisions of the 1986 Electronic Communications Privacy Act (ECPA) are "updated" to better reflect the insatiable needs of our police state minders, law enforcement groups and corporate lobbyists are clamoring for greater access to our electronic communications.

While doe-eyed "progressives" claim that the reelection of war criminal Barack Obama portends an imminent "2.0 reset" by his administration, actions speak louder than words, parti 

cularly as they pertain to Americans' constitutional rights.

Most recently the Hope and Change™ fraudster signaled his intentions by giving Israel a green light to murder Palestinians in the open air prison of Gaza. The silence from "progressive" quarters was worse than deafening as writers Chris Floyd and Arthur Silber pointed out.

What about other "liberal icons," stalwart champions of civil liberties; what have *they* been up to since the election?

CNET investigative reporter Declan McCullagh informed us that "Patrick Leahy, the influential Democratic chairman of the Senate Judiciary Committee, has dramatically reshaped his legislation in response to law enforcement concerns," and that a "vote on his bill, which now authorizes warrantless access to Americans' e-mail, is scheduled for next week."

Among the proposals found in the Leahy revisions are the following:

> • Grants warrantless access to Americans' electronic correspondence to over 22 federal agencies. Only a subpoena is required, not a search warrant signed by a judge based on probable cause.

• Permits state and local law enforcement to warrantlessly access Americans' correspondence stored on systems not offered "to the public," including university networks.

• Authorizes any law enforcement agency to access accounts without a warrant–or subsequent court review–if they claim "emergency" situations exist.

• Delays notification of customers whose accounts have been accessed from 3 days to "10 business days." This notification can be postponed by up to 360 days.

Although a follow-up CNET article reported that Leahy, reacting to widespread opposition, has now "abandoned his controversial proposal that would grant government agencies more surveillance power–including warrantless access to Americans' e-mail accounts," given Congress's near universal embrace of the "Total Information Awareness" paradigm, it is a near certainty these measures will return in some form.

"It's an abrupt departure from Leahy's earlier approach," McCullough noted, one "which required police to obtain a search warrant backed by probable cause before they could read the contents of e-mail or other communications."

But in the best tradition of "bipartisanship," i.e., capitulation to the Security State, "after law enforcement groups including the National District Attorneys' Association and the National Sheriffs' Association organizations objected to the legislation," Leahy "pushed back the vote and reworked the bill as a package of amendments to be offered next Thursday."

The strongest objections to providing the public with privacy safeguards came, you guessed it, from officials within Obama's Department of Justice.

Earlier this year, CNET reported that the DOJ "offered what amounts to a frontal attack on proposals to amend federal law to better protect Americans' privacy."

"James Baker, the associate deputy attorney general, warned that rewriting a 1986 privacy law to grant cloud computing users more privacy protections and to require court approval before tracking Americans' cell phones would hinder police investigations."

During Senate testimony back in April, Baker claimed that requiring a search warrant "to obtain stored e-mail could have an 'adverse impact' on criminal investigations. And making location information only available with a search warrant, he said, would hinder 'the government's ability to obtain important information in investigations of serious crimes'."

In other words, even when there is no evidence a crime has been committed the Obama administration is asserting that constitutional safeguards on email stored in the cloud would get in the government's way and impose "an unnecessary burden" on state fishing expeditions by a multitude of law enforcement agencies.

Such fallacious claims come hot on the heels of administration efforts to convince Congress to rewrite wiretapping laws that would require internet firms such as Facebook, Google, Microsoft and Yahoo to build backdoors into their infrastructure for government surveillance.

Earlier this month, *Russia Today* disclosed that although the FBI "has been adamant about withholding information about their plans to ensure the government can access any

encrypted emails or messages sent over the Internet," a federal judge ordered the Bureau to "come clean."

"Washington," *RT* reported, "hopes to eventually roll out a program that will see that the FBI and other federal agencies are allowed backdoor access to any and all online communications."

The ruling by U.S. District Court Judge Richard Seeborg, in response to charges by the Electronic Frontier Foundation (EFF) that a government stonewall hindered their Freedom of Information Act lawsuit on the FBI's "Going Dark" program, ordered the Department of Justice to conduct "further review of the materials previously withheld."

Although the DOJ's Criminal Division had located 8,425 pages of "potentially responsive information," they only released "one page in full and 6 pages in part, and withheld 51 pages in full." How's *that* for "transparency"!

And with new Justice Department guidelines allowing "counterterrorism officials" to "lengthen the period of time they retain information about U.S. residents, even if they have no known connection to terrorism" as *The Washington Post* reported earlier this year, any and every scrap of electronic detritus generated by the billions of cell phone calls, text messages, emails and web searches made by Americans every day is considered fair game by government snoops.

The trend towards retaining more and more data by intelligence agencies and local police has accelerated with technological advances. As *The New York Times* reported in August, "not so long ago even the most aggressive government surveillance had to be selective: the cost of data storage was too high and the capacity too low to keep everything."

"Not anymore." According to to John Villasenor, a "senior fellow" at the elitist Brookings Institution, as data storage costs plummet "it will soon be technically feasible and affordable to record and store everything that can be recorded about what everyone in a country says or does."

The Brookings analyst averred that "estimates ... to store the audio from telephone calls made by an average person in the course of a year would require about 3.3 gigabytes and cost just 17 cents to store, a price that is expected to fall to 2 cents by 2015."

"Tracking a person's movements for a year, collected from their cellphone, would take so little space as to carry a trivial cost," the *Times* averred. "Storing video takes far more space, but the price is dropping so steadily that storing millions of hours of material will not be a problem soon."

But wouldn't securocrats drown in these vast oceans of electronic data? Not really. A "parallel revolution in search technology" will soon allow even the dimmest bulb at DHS or the FBI "to efficiently find anything of interest in the data."

This "parallel revolution" was hinted at by investigative journalist James Bamford. In his March piece in *Wired Magazine*, Bamford described efforts by the National Security Agency to build "super-fast computers to conduct brute-force attacks on encrypted messages."

In 2009, "they made a big breakthrough," a former "senior intelligence official" told *Wired*. "The NSA believes it's on the verge of breaking a key encryption algorithm–opening up

hoards of data."

"That," the former official noted, "is where the value of Bluffdale, and its mountains of long-stored data, will come in," Bamford wrote.

"What can't be broken today may be broken tomorrow. 'Then you can see what they were saying in the past,' he says. 'By extrapolating the way they did business, it gives us an indication of how they may do things now.' The danger, the former official says, is that it's not only foreign government information that is locked in weaker algorithms, it's also a great deal of personal domestic communications, such as Americans' email intercepted by the NSA in the past decade."

And if it can be intercepted, mined and stored, it can be searched, giving government snoops an unprecedented window into our lives.

More troubling still, with ECPA "reform" on the horizon, CNET disclosed that "Leahy's rewritten bill would allow more than 22 agencies–including the Securities and Exchange Commission and the Federal Communications Commission–to access Americans' e-mail, Google Docs files, Facebook wall posts, and Twitter direct messages without a search warrant."

In addition to the SEC, civil subpoena authority would be granted to diverse agencies such as the "Federal Reserve, the Federal Trade Commission, the Federal Maritime Commission, the Postal Regulatory Commission, the National Labor Relations Board, and the Mine Enforcement Safety and Health Review Commission," McCullough wrote.

It doesn't take a rocket scientist to infer that investigative digging by concerned citizens and journalists into the filthy shenanigans and "shitty deals" foisted on the public by banks, shady brokerage houses, mortgage lenders, defense corporations, petrochemical and mining interests, or unions out to "organize the unorganized," would be viewed as a dire threat to the current corporatist set-up.

According to draft proposals leaked to CNET we learn that if passed the new law "would give the FBI and Homeland Security more authority, in some circumstances, to gain full access to Internet accounts without notifying either the owner or a judge."

The Electronic Privacy Information Center (EPIC) reported last month, the organization "is seeking documents about DHS Internet monitoring that some Justice Department officials believe may 'run afoul of privacy laws forbidding government surveillance of private Internet traffic'."

"In February 2011," EPIC disclosed that "the Department of Homeland Security announced that the agency planned to implement a program that would monitor media content, including social media data."

The DHS initiative "would gather information from 'online forums, blogs, public websites, and messages boards' and disseminate information to 'federal, state, local, and foreign government and private sector partners'."

"The program would be executed, in part," EPIC also revealed, "by individuals who established fictitious usernames and passwords to create covert social media profiles to spy on other users. The agency stated it would store personal information for up to five years."

Ironically enough, in October the U.S. Senate Permanent Subcommittee on Investigations issued a report, Federal Support for and Involvement in State and Local Fusion Centers, which found "that DHS-assigned detailees to the fusion centers forwarded 'intelligence' of uneven quality–oftentimes shoddy, rarely timely, sometimes endangering citizens' civil liberties and Privacy Act protections, occasionally taken from already-published public sources, and more often than not unrelated to terrorism."

"Despite reviewing 13 months' worth of reporting originating from fusion centers from April 1, 2009 to April 30, 2010," Senate staff averred, "the Subcommittee investigation could identify no reporting which uncovered a terrorist threat, nor could it identify a contribution such fusion center reporting made to disrupt an active terrorist plot."

In their Freedom of Information Act lawsuit against DHS, the privacy watchdogs obtained nearly three hundreds pages of documents which revealed that the sprawling bureaucracy "is monitoring political dissent." According to EPIC, the documents described widespread surveillance by the agency and included "contracts and statements of work with General Dynamics for 24/7 media and social network monitoring and periodic reports to DHS. The documents reveal that the agency is tracking media stories that 'reflect adversely' on DHS or the U.S. government."

Meanwhile, Senate Subcommittee investigators also found that the agency's disbursement practices were so shoddy that "DHS revealed that it was unable to provide an accurate tally of how much it had granted to states and cities to support fusion centers efforts, instead producing broad estimates of the total amount of Federal dollars spent on fusion center activities from 2003 to 2011, estimates which ranged from $289 million to $1.4 billion."

But as I have pointed out many times, the machinery of state repression is lubricated with cold cash bestowed by taxpayers on privileged corporate insiders. Earlier this month, *Washington Technology* reported that "the top 20 contractors at the Homeland Security Department represent more than a third of all business done by contract at the department during fiscal 2011."

According to the report, "DHS spent $5.1 billion with the top 20 companies, and $14.2 billion on all contractors," with "IT and systems integration firms," integral to constructing and running the secret state's panopticon, topping the list.

• • •

Since the 9/11 provocation, intrusive surveillance of the American people by a host of shadowy government agencies and private corporations clearly demonstrates there is broad ruling class consensus for expanding authoritarian and dictatorial forms of rule under an unconstitutional "Unitary Executive."

Recent revelations by *The Washington Post* that the Obama regime "has been secretly developing a new blueprint for pursuing terrorists, a next-generation targeting list called the 'disposition matrix'," starkly reveals that when the president can spy on or kill whomever he pleases, on his own initiative and without the checks and balances enshrined in the U.S. Constitution, the Bill of Rights is effectively a dead letter.

While we do not know what form a "new and improved" ECPA will take when it emerges from the bipartisan congressional snake pit, the prospects for ever emerging from America's "friendly fascist" nightmare are growing dimmer.

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 independent research and media group of writers, scholars, journalists and activists based in Montreal, 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/