GlobalResearch
Center for Research on Globalization

Big Brother: Obama Demands Access to Internet Records, in Secret, and Without Court Review

By Tom Burghardt
Global Research, August 13, 2010
Antifascist Calling... 12 August 2010

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

The Obama administration is seeking authority from Congress that would compel internet service providers (ISPs) to turn over records of an individual's internet activity for use in secretive FBI probes.

In another instance where Americans are urged to trust their political minders, The Washington Post reported last month that "the administration wants to add just four words–'electronic communication transactional records'–to a list of items that the law says the FBI may demand without a judge's approval."

Under cover of coughing-up information deemed relevant to espionage or terrorism investigations, proposed changes to the Electronic Communications Privacy Act (ECPA) would greatly expand the volume of private records that can be seized through National Security Letters (NSLs).

Constitution-shredding lettres de cachet, NSLs are administrative subpoenas that can be executed by agencies such as the FBI, CIA or Defense Department, solely on the say so of supervisory agents.

The noxious warrants are not subject to court review, nor can a recipient even disclose they have received one. Because of their secretive nature, they are extremely difficult to challenge.

Issued by unaccountable Executive Branch agents hiding behind a façade of top secret classifications and much-ballyhooed "sources and methods," NSLs clearly violate our constitutional rights.

The fourth amendment unambiguously states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

However, in "new normal" America constitutional guarantees and civil rights are mere technicalities, cynical propaganda exercises jettisoned under the flimsiest of pretexts: the endless "War on Terror" where the corporate state's praetorian guards work the "dark side."

Once served, firms such as telecommunication providers, banks, credit card companies, airlines, health insurers, video rental services, even booksellers and libraries, are compelled to turn over what the secret state deem relevant records on targets of FBI fishing

expeditions.

If burdensome NSL restrictions are breeched for any reason, that person can be fined or even jailed if gag orders built into the draconian USA Patriot Act are violated.

However, even the Patriot Act's abysmally lowered threshold for seizing private records specify that NSLs cannot be issued "solely on the basis of activities protected by the first amendment of the Constitution of the United States."

Despite these loose standards, congressional investigators, journalists and civil liberties watchdogs found that the FBI violated the rules of the road, such as they are, thousands of times. Between 2003-2006, the Bureau issued 192,499 NSLs, according to current estimates, the FBI continues to hand out tens of thousands more each year.

According to a May 2009 Justice Department letter sent to the House and Senate Judiciary Committees, "in 2007, the FBI made 16,804 NSL requests" and followed-up the next year by issuing some "24,744 NSL requests … to 7,225 United States persons."

The Justice Department's Office of the Inspector General (OIG) issued a 2007 report which concluded that the Bureau had systematically abused the process and exceeded their authority. A follow-up report published by the OIG in January found that serious civil liberties breeches continue under President Obama.

This is hardly surprising given the track record of the Obama administration.

"Reform," Obama-Style

The latest White House proposal would hand the secret state unprecedented access to the personal communications of every American.

What Bushist war criminals did secretly, Obama intends to do openly and with the blessings of a supine Congress. As constitutional scholar Glenn Greenwald points out, "not only has Obama … blocked any reforms, he has taken multiple steps to further expand unaccountable and unchecked surveillance power."

Nowhere is this more apparent than by administration moves to "reform" ECPA.

While the Justice Department claims their newly sought authority does not include "'content' of email or other Internet communications," this is so much eyewash to deceive the public.

In fact, the addition of so-called transactional records to the volume of files that the state can arbitrarily seize, would hand the government access to a limitless cache of email addresses, dates and times they were sent and received, and a literal snap-shot on demand of what any user looks at or searches when they log onto the internet.

As I have pointed out before, most recently last month when Idescribed the National Security Agency's PERFECT CITIZEN program, the roll-out of privacy-killing deep-packet inspection software developed by NSA already has the ability to read and catalogue the content of email messages flowing across private telecommunications networks.

Former Bushist Homeland Security official, Stewart A. Baker, applauded the proposal and

told the Post, “it’ll be faster and easier to get the data.” Baker touts the rule change as a splendid way for ISPs to hand over “a lot more information to the FBI in response to an NSL.”

While the Post claims “many internet service providers” have “resisted the government’s demands to turn over electronic records,” this is a rank mendacity.

A “senior administration official,” speaking anonymously of course, told the Post that “most” ISPs already “turn over such data.” Of course they do, and at a premium price!

Internet security analyst Christopher Soghoian has documented that just one firm, Sprint Nextel, routinely turned over their customer’s geolocation data to law enforcement agencies and even built them a secure web portal to do so, eight million times in a single year!

Soghoian wrote last year that “government agents routinely obtain customer records from these firms, detailing the telephone numbers dialed, text messages, emails and instant messages sent, web pages browsed, the queries submitted to search engines, and of course, huge amounts of geolocation data, detailing exactly where an individual was located at a particular date and time.”

As a public service, the secrecy-shredding web site Cryptomehas published dozens of so-called compliance guides for law enforcement issued by a plethora of telecoms and ISPs. Readers are urged to peruse Yahoo’s manual for a taste of what these grifters hand over.

While the administration argues that “electronic communication transactional records” are the “same as” phone records that the Bureau can obtain with an NSL, seizing such records reveal far more about a person’s life, and political views, than a list of disaggregated phone numbers. This is precisely why the FBI wants unlimited access to this data. Along with racial and religious profiling, the Bureau would be handed the means to build a political profile on anyone they deem an “extremist.”

That “senior administration official” cited by the Post claims that access to a citizen’s web history “allows us to intercede in plots earlier than we would if our hands were tied and we were unable to get this data in a way that was quick and efficient.”

Perhaps our “change” administration has forgotten a simple historical fact: police states are efficient. The value of privacy in a republic, including whom one communicates with or where one’s interests lie, form the core values of a democratic order; principles sorely lacking in our “new normal” Orwellian order!

In a small but significant victory, the ACLU announced this week that “the FBI has partially lifted a gag it imposed on American Civil Liberties Union client Nicholas Merrill in 2004 that prevented him from disclosing to anyone that he received a national security letter (NSL) demanding private customer records.”

In a statement to reporters, Merrill said: “Internet users do not give up their privacy rights when they log on, and the FBI should not have the power to secretly demand that ISPs turn over constitutionally protected information about their users without a court order. I hope my successful challenge to the FBI’s NSL gag power will empower others who may have received NSLs to speak out.”

Despite this narrow ruling, the FBI intends to soldier on and the Obama administration is hell-bent on giving the Bureau even more power to operate in the dark.

Commenting on the Merrill case, The Washington Post reportedFBI spokesperson Mike Kortan claimed that NSL "secrecy is often essential to the successful conduct of counterterrorism and counterintelligence investigations" and that public disclosure "may pose serious risks to the investigation itself and to other national security interests."

Those "other" interests, apparently, do not extend to the right to express one's views freely, particularly when they collide with the criminal policies of the secret state.

READ TOM BURGHARDT'S CHAPTER IN NEW BOOK FROM GLOBAL RESEARCH
The Global Economic Crisis

Michel Chossudovsky
Andrew G. Marshall (editors)

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

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