GlobalResearch
Center for Research on Globalization

Institutionalized Spying on Americans: Big Brother is No Longer a Fiction

By Stephen Lendman
Global Research, May 01, 2013
Region: USA
Theme: Police State & Civil Rights

Big Brother no longer is fiction. It hasn't been for some time. It's official US policy. According to ACLU's Technology and Liberty Program director Barry Steinhardt:

> "Given the capabilities of today's technology, the only thing protecting us from a full-fledged surveillance society are the legal and political institutions we have inherited as Americans."
>
> "Unfortunately, the September 11 attacks have led some to embrace the fallacy that weakening the Constitution will strengthen America."

Manufactured national security threats matter more than fundamental freedoms. Domestic spying is institutionalized.

Anyone can be monitored for any reason or none at all. Privacy rights are lost. Patriot Act legislation authorized unchecked government surveillance powers.

Financial, medical and other personal information can be accessed freely. So-called "sneak and peak" searches may be conducted through "delayed notice" warrants, roving wiretaps, email tracking, and Internet and cell phone use.

The FBI, CIA, NSA, and Pentagon spy domestically. So do state and local agencies. Spies "R" us defines US policy. America is a total surveillance society. It's unsafe to live in. Everyone is suspect unless proved otherwise.

The 2012 FISA Amendments Reauthorization Act renewed warrantless spying. It passed with little debate. On Sunday, December 30, 2012 Obama signed it into law. Doing so largely went unnoticed.

These type disturbing measures usually slip below the radar. Weekends and holiday period enactments conceal blows to freedom. Warrantless spying became law for another five years.

Phone calls, emails, and other communications may be monitored secretly without court authorization. Probable cause isn't needed. So-called "foreign intelligence information" is sought. Virtually anything qualifies. Vague language is all-embracing.

Months after 9/11, Bush secretly authorized the NSA to eavesdrop on Americans lawlessly. Sweeping surveillance followed without court-approved warrants.

Doing so violates core constitutional protections. Major US telecommunications companies

are involved. They have been since 9/11. Things now are worse than then.

On April 29, Russia Today (RT) headlined "Spy, or pay up: FBI-backed bill would fine US firms for refusing wiretaps." A day earlier Washington Post article was cited.

It headlined "Panel seeks to fine tech companies for noncompliance with wiretap orders," saying:

> "A government task force is preparing legislation that would pressure companies such as Facebook and Google to enable law enforcement officials to intercept online communications as they occur, according to current and former US officials familiar with the effort."

At issue is alleged FBI concerns about "Internet communications of terrorists and other criminals."

FBI spying is longstanding. So are other lawless practices. Throughout its history, the agency operated within and outside the law.

J. Edgar Hoover ran it from 1924 – 1972. He waged war on communists, anti-war, human and civil rights activists, the American Indian Movement, Black Panther Party, and other groups challenging rogue state policies.

He ordered agents to infiltrate, disrupt, sabotage, and destroy them. Anyone advocating ethnic justice and racial emancipation, as well as economic, social, and political equality across gender and color lines became vulnerable.

Post-9/11, FBI abuses escalated. Intrusive surveillance tools now target ordinary Americans. Unchecked authority and other abusive practices are widespread. America's war on terror matters most.

Disturbing tactics include greater physical surveillance, commercial database data retrieval, paid informants infiltrating groups (or targeting individuals) on false pretenses, and letting covert unidentified agents conduct "pretext" interviews for information.

Muslims are America's target of choice. So are anti-war and social justice activists. A gloves off, no-holds barred approach is followed. Virtually anything is fair game. Innocent people are vulnerable.

The Patriot Act authorized so-called National Security Letters (NSLs). FBI agents take full advantage. They do so by demanding personal customer records from ISPs, financial institutions, credit companies, and other sources without prior court approval.

The FBI wants more. According to the Washington Post, it wants companies failing to heed wiretap orders penalized.

In February 2011, then FBI general counsel Valerie Caproni told House Crime, Terrorism and Homeland Security Subcommittee members about a "Going Dark" problem.

She explained the agency's inability to access comprehensive "communications and related data." She claimed a "public safety" threat when critical information is missed.

In March 2013, current FBI general counsel Andrew Weissmann addressed an American Bar Association discussion. He did so on legal challenges new technologies pose, saying:

“We don’t have the ability to go to court and say, ‘We need a court order to effectuate the intercept.’ Other countries have that. Most people assume that’s what you’re getting when you go to a court.”

Under current law, Internet communications companies can refuse to comply with court-ordered wiretaps. They can claim no practical way to do so.

Proposed legislation would change things. It would force companies to rebuild their capability to allow government monitoring.

Weissmann calls doing so a “top priority.” Proposed legislation is being drafted. It’s an extension of the 1994 Communications Assistance for Law Enforcement Act (CALEA).

It grants federal authorities sweeping surveillance powers. Doing so lets them spy on Americans more intrusively.

CALEA originally applied only to digital telephone networks. It forced telephone companies to redesign their network architectures to make wiretapping easier.

In 2005, online communications were added. Broadband providers had to rebuild their networks accordingly.

At issue was permitting access to Internet “phone calls” through VOIP applications, as well as online “conversations” by instant messaging programs.

Law enforcement wiretapping is longstanding. Existing laws permit tapping phone or online communications regardless of what programs or protocols are used.

Industry largely cooperates. Digital age surveillance is easier than authorities claim. They want greater ease than currently permitted. Expanding CALEA is overkill. Doing so enhances police state powers.

The FBI cites its “tappability principle.” It does so to justify its demands. It claims whatever is legally searchable sometimes should be physically searchable all times.

Applied to phone and Internet communications, it would require designing phones and computers with built-in bugs. Doing so would elevate surveillance powers. Everyone could be spied on at all times. Private communications no longer would exist.

Expanding CALEA is the tip of the iceberg. Perhaps software companies are next. Enhanced legislative authority may force them to create surveillance-ready programs. Doing so may compromise innovation.

Applying phone system rules to software development and online communications assures trouble. What’s longstanding policy for one compromises innovation for the others. It also more greatly undermines freedom.

Police state powers are enhanced. Companies are forced to comply. Under draft legislation, courts could levy fines. Judicial inquiries could impose additional ones. After 90 days, unpaid

amounts would double daily.

According to Center for Democracy and Technology senior counsel Greg Nojeim:

> "This proposal is a non-starter that would drive innovators overseas and cost American jobs. They might as well call it the Cyber Insecurity and Anti-Employment Act."

Former federal prosecutor Michael Sussman added:

> "Today, if you're a tech company that's created a new and popular way to communicate, it's only a matter of time before the FBI shows up with a court order to read or hear some conversation."
>
> "If the data can help solve crimes, the government will be interested."

In 2010, after its networks were hacked, Google began emails and text messages end-to-end encryption. Facebook followed suit.

Doing so compromises FBI monitoring. Agency officials want enhanced CALEA authorization permitting it.

They claim doing so only extends current law to new technologies. It requires phone and online companies to allow wiretapping.

It's much more than that. It elevates mass surveillance to a dangerously higher level. It's another step toward full-blown tyranny.

On April 29, the Center for Democracy & Technology (CDT) headlined "Feds Push for Backdoor Wiretap Capabilities."

According to CDT Senior Staff Technologist Joe Hall:

> "A wiretapping mandate is a vulnerability mandate. The unintended consequences of this proposal are profound."
>
> "At the very time when the nation is concerned about cybersecurity, the FBI proposal has the potential to make our communications less secure."
>
> "Once you build a wiretap capability into products and services, the bad guys will find a way to use it."

CDT President Leslie Harris added:

> "What the FBI is proposing sounds benign, but it comes with such onerous penalties that it would force developers to seek pre-approval from the FBI."
>
> "No one is going to want to face fines that double every day, so they will go to the FBI and work it out in advance, diverting resources, slowing innovation, and resulting in less secure products."
>
> "The sad irony," said Hall, "is that this is likely to be ineffective. Building a communications tool today is a homework project for undergraduates."

> "So much is based on open source and can be readily customized. Criminals and other bad actors will simply use homemade communication services based offshore, making them even harder to monitor."

Media scholar/critic/activist Robert McChesney told Progressive Radio News Hour listeners how Internet freedom has been compromised.

His important new book "Digital Disconnect: How Capitalism is Turning the Internet Against Democracy" explains what should concern everyone.

"The corporate media sector (did) everything in its immense power to limit (its) openness and egalitarianism…., he said."

> "….corporate and state surreptitious monitoring of Internet users" compromises fundamental freedoms.
>
> Doing so is "inimical to much of the democratic potential of digital communication."

Internet freedom depends on "arrest(ing) the forces that promote inequality, monopoly, hypercommercialism, corruption, depoliticization, and stagnation."

It requires ending mass surveillance powers. It's about restoring lost democratic principles. America's heading the wrong way. It's perilously close to ending freedom altogether.

Stephen Lendman lives in Chicago. He can be reached at lendmanstephen@sbcglobal.net.

His new book is titled "Banker Occupation: Waging Financial War on Humanity."

http://www.claritypress.com/LendmanII.html

Visit his blog site at sjlendman.blogspot.com.

Listen to cutting-edge discussions with distinguished guests on the Progressive Radio News Hour on the Progressive Radio Network.

It airs Fridays at 10AM US Central time and Saturdays and Sundays at noon. All programs are archived for easy listening.

http://www.progressiveradionetwork.com/the-progressive-news-hour

http://www.dailycensored.com/institutionalized-spying-on-americans/

Articles by: Stephen Lendman

About the author:

Stephen Lendman lives in Chicago. He can be reached at lendmanstephen@sbcglobal.net. His new book as editor and contributor is titled "Flashpoint in Ukraine: US Drive for Hegemony Risks WW III." http://www.claritypress.com/LendmanIII.html Visit his blog site at sjlendman.blogspot.com. Listen to cutting-edge discussions with distinguished guests on the Progressive Radio News Hour on the Progressive Radio Network. It airs three times weekly: live on Sundays at 1PM Central time plus two prerecorded archived programs.