GlobalResearch
Center for Research on Globalization

Internet Threatened by Censorship, Secret Surveillance, and Cybersecurity Laws

By Stephen Lendman
Global Research, May 22, 2009
22 May 2009

Region: USA
Theme: Media Disinformation, Police State & Civil Rights

At a time of corporate dominated media, a free and open Internet is democracy's last chance to preserve our First Amendment rights without which all others are threatened. Activists call it Net Neutrality. Media scholar Robert McChesney says without it "the Internet would start to look like cable TV (with a) handful of massive companies (controlling) content" enough to have veto power over what's allowed and what it costs. Progressive web sites and writers would be marginalized or suppressed, and content systematically filtered or banned.

Media reform activists have drawn a line in the sand. Net Neutrality must be defended at all costs. Preserving a viable, independent, free and open Internet (and the media overall) is essential to a functioning democracy, but the forces aligned against it are formidable, daunting, relentless, and reprehensible. Some past challenges suggest future ones ahead.

Censorship Attempts to Curtail Free Expression

The First Amendment states: "Congress shall make no law respecting an establishment of religion, or prohibiting the exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

Nonetheless, Congress and state legislatures have repeatedly tried to censor free speech, allegedly regarded as indecent, obscene, hateful, terrorist-related, or harmful to minors. However, the Supreme Court, in a number of decisions, ruled that the government may not regulate free expression, only its manner such as when it violates the right to privacy "in an essentially intolerable manner" – a huge hurtle to overcome, including online, because viewers are protected by simply "averting (one's) eyes (Cohen v. California – 1971)."

In 1998, the Child Online Protection Act (COPA) passed, but was blocked by federal courts as an infringement of free speech and therefore unconstitutional and unenforceable. In 1999, the law was struck down at the Appellate Court level, but it stayed on the books. In 2002, the Supreme Court reviewed the ruling and returned the case for reconsideration. It remained blocked. Then in March 2003, the Appellate Court again ruled it unconstitutional on the grounds that it would hinder protected adult speech that's likely what it was about in the first place.

Other litigation followed at the District and Appellate levels until on January 21, 2009, the Supreme Court killed COPA by refusing to hear appeals to affirm it. The Electronic Frontier Foundation put it this way: “After 10 Years, an Infamous Internet-Censorship Act is Finally Dead.” At least that’s the hope, but censorship attempts never die. They just reinvent themselves in new forms made all the easier when powerful corporate interests and their congressional allies support them.

In 2000, the Children’s Internet Protection Act (CIPA) became law, and the Supreme Court upheld it – to regulate online content deemed “indecent (or) harmful to minors.” The law requires schools, libraries and other public institutions to install blocking software to prevent minors from having access to it.

In 2006, the Deleting Online Predators Act (DOPA) passed the House but not the Senate. It also would have mandated schools, libraries and other public institutions to prevent minors from accessing “commercial social networking websites (and) chat rooms.”

Its language was broad enough to apply also to sites like Amazon, Yahoo, Wikipedia and others and would have made the FCC a gatekeeper/censor. As the Protecting Children in the 21st Century Act, the law was reintroduced in the Senate in January 2007 but never passed.

In February 1996, the Communications Decency Act (CDA) was passed – to regulate alleged indecent and obscene online content in violation of the First Amendment. Under the law, classic fiction would be banned as well as any material deemed offensive. In June, 1996, a three-judge federal panel partially struck it down for restricting adult free speech. In June 1997, the Supreme Court upheld the lower court ruling in Reno v. American Civil Liberties Union.

The Act was Title V of the 1996 Telecommunications Act titled Broadcast Obscenity and Violence that applied broadcast standards to the Internet. Under Section 230, Internet services operators aren’t considered publishers and thus have no liability for the words of third parties using their services.

In 2003, Congress amended CDA by removing struck down indecency provisions. In 2005, a three-judge Southern District of New York panel rejected Barbara Nitke’s obscenity provisions CDA challenge (in Nitke, et al v. Ashcroft). The Supreme Court upheld the decision.

In 2005, the Violence Against Women and Department of Justice Reauthorization Act (VAWDOJRA) became law – and another blow to online free speech by prohibiting “any device (like a modem) or software that can be used to originate….(anonymous or other) communications that are transmitted, in whole or in part, by the internet” for the alleged purpose of harassment, even if only vigorous constitutional debate was intended or ordinary free speech.

In October 2007, the House passed the Violent Radicalization and Homegrown Terrorism Act

called “the thought crime prevention bill.” It was introduced in the Senate, referred to the Homeland Security and Governmental Affairs Committee, but never voted on or passed.

If it ever becomes law in its present form, it will establish a commission and Center for Excellence to study and act against “thought criminals” (including online ones) for alleged acts of “violent radicalization (and) homegrown terrorism” defined as follows:

— “violent radicalization (to mean) adopting or promoting an extremist belief system (to facilitate) ideologically based violence to advance political, religious or social change;”

— “homegrown terrorism (to mean) the use, planned use, or threatened use, of force or violence by a group or individual born, raised, or based and operating primarily within the United States or any (US) possession to intimidate or coerce the (US) government, the civilian population….or any segment thereof (to further) political or social objectives.”

In other words, this law, if passed, will criminalize whatever the government wishes to include under the above two categories, including constitutionally protected speech online or elsewhere.

Another ongoing censorship issue involves craigslist – a worldwide online community network featuring classified ads for “jobs, housing, for sale, personals, services, local community, and events.”

On May 5, South Carolina Attorney (AG) General Henry McMaster notified its CEO, Jim Buckmaster, that unless an “erotic services” section is removed in 10 days, “craigslist management may be subject to criminal investigation and prosecution.” Other AGs in Rhode Island, Illinois, and Connecticut issued similar threats even though all of them are baseless.

Previous courts have held that Section 230 of the Communications Decency Act (CDA) protects “interactive computer service” providers like craigslist and lets them be self-regulating and free from liability. The law clearly states that they shouldn’t be responsible for third party content because they didn’t do enough to comply with individual State standards that may violate the First Amendment and federal law.

In craigslist’s case, it’s gone way beyond its legal obligations. In November 2008, it agreed to technical and policy changes to curb the use of its site for illegal purposes by third parties, including requiring telephone and credit card verification for “erotic services” ads to reject ones deemed illegal.

Earlier, craigslist screened out 90% of these ads. Nonetheless, it’s being unfairly targeted by AGs interpreting Section 230 and First Amendment rights as they please. Federal law, however, protects craigslist, but not against ambitious AGs harassment for their own political advantage and self-interest.

On May 20, craigslist announced that it filed suit against South Carolina Attorney General Henry McMaster seeking “declaratory relief and a restraining order with respect to criminal charges he has repeatedly threatened against craigslist and its executives.” Craigslist is on solid footing. It’s in full compliance with the law, but McMaster’s persistent threats forced it to sue in federal court.

These and numerous other congressional and other attempts aim to censor protected speech, including online. Expect more of this ahead, some legislation to be enacted, at times upheld by the courts, and, as a result, our liberties to be chipped away incrementally and lost – unless a line in the sand is drawn and defended by enough of the committed to do it.

On February 29, 2008, one skirmish turned out successfully when a federal judge let the anonymous whistle-blowing WikiLeaks resume operations after a week earlier ordering its US hosting company and domain registrar (Dynadot) to shut down and lock out its site. In his reconsidered ruling, District Judge Jeffrey White conceded he was having second thoughts regarding “serious questions of prior restraint (and) possible violations of the First Amendment.” He added that “the court does not want to be a part of any order that is not constitutional.” Even so, one triumph doesn’t mean victory. The struggle for unimpeded free speech continues.

Secret Unconstitutional Surveillance, Including Online Data Mining

The right to privacy is sacred even though no constitutional provision specifically mandates it. Nonetheless, the First Amendment guarantees free and open speech and beliefs. The Third Amendment the privacy of our homes against demands to be used to house soldiers. The Fourth Amendment against unreasonable searches and seizures. The Fifth Amendment against self-incrimination and privacy of our personal information.

Also, the Ninth Amendment states that the “enumeration of certain (of the Bill of) rights shall not be construed to deny or disparage other rights retained by the people.” In Griswold v. Connecticut (1965), the Supreme Court held that the Constitution protects privacy in a case affirming the right to use contraceptives and that banning them violated the “right to marital privacy.”

In Justice Arthur Goldberg’s concurring opinion, he cited the Ninth Amendment in defense of the ruling. Earlier High Courts also affirmed the constitutional right of privacy on matters of marriage, child rearing, procreation, education, termination of medical treatment, possessing and viewing pornography, abortion, and more as well as overall privacy protection.

The 14th Amendment’s “liberty” clause also relates to privacy by stating: “nor shall any State deprive any person of life, liberty, or property, without due process of law….” Courts have broadened the meaning of “liberty” to include personal, political and social rights and

privileges. Thus, invasion of private spaces is unconstitutional.

In Olmstead v. US (1928), Justice Louis Brandeis stated:

> "The makers of our Constitution understood the need to secure conditions favorable to the pursuit of happiness, and the protections guaranteed by this are much broader in scope, and include the right to life and an inviolate personality — the right to be left alone — the most comprehensive of rights and the right most valued by civilized men. The principle underlying the Fourth and Fifth Amendments is protection against invasions of the sanctities of a man's home and privacies of life. This is a recognition of the significance of man's spiritual nature, his feelings, and his intellect."

George Bush institutionalized lawless spying invasions of privacy on Americans and others. Barack Obama continues the practice under the same federal agencies, including the FBI, CIA, Pentagon and NSA. On April 15, The New York Times headlined: "Officials Say US Wiretaps Exceeded Law."

It cited the NSA's practice in recent months of intercepting private emails and phone calls of Americans "on a scale that went beyond the broad legal limits established by Congress last year…." Briefed intelligence officials and lawyers called it "significant and systematic….overcollection" in violation of the law.

The Justice Department acknowledged the problem but said it was resolved. For its part, the NSA said its "intelligence operations, including programs for collection and analysis, are in strict accordance with US laws and regulations." The Office of the Director of National Intelligence, in overall charge, downplayed the The Times story, referred to "inadvertent mistakes," and claimed efforts were immediately implemented to correct them.

Nonetheless, the issue remains unsettled, and new details reveal earlier domestic surveillance, including wiretapping a congressional member without court approval, and systematically doing it against many American citizens.

Tom Burghardt writes often on these issues for various publications, web sites, and his Antifascist Calling blog…."Exploring the shadowlands of the corporate police state." In calling "Spying on Americans: 'Business as Usual' under Obama," he reported that working cooperatively with private corporations, the NSA collects vast amounts of "transactional data such as credit card purchases, bank transactions and travel itineraries….sold to (the agency) by corporate freebooters." It's then data-mined for "suspicious patterns," a practice begun pre-9/11 but expanded greatly since then.

More than just financial transactions are monitored. According to investigative journalist Christopher Ketchum, "as many as '8 million Americans are now listed (as) secret enemies….who could face detention under martial law (and subjected) to everything from heightened surveillance and tracking to direct questioning" and possible internment.

Nothing under Obama has changed in spite of serious privacy, civil liberties, and other constitutional issues. Director Rod Beckstrom of DHS' Cyber Security Center resigned in March because of NSA's "greater role in guarding the government's computer systems" and its concentrated power without checks and balances.

According to Electronic Frontier Foundation's senior staff attorney Kevin Bankston: Obama's "Justice Department (is continuing) the Bush administration's cover-up of the National Security Agency's dragnet surveillance of millions of Americans, and insisting that the much-publicized warrantless wiretapping program is still a 'secret' that cannot be reviewed by the courts…." because doing so would harm national security.

Worse still is the DOJ's assertion that the US government is immune from illegal spying litigation even when in violation of federal privacy statutes, an unprecedented claim exceeding the Bush administration citing "sovereign immunity." Obama is going Bush one better by saying the Patriot Act immunizes the government from being sued under surveillance provisions of the Wiretap Act, Stored Communications Act, and Foreign Intelligence Surveillance Act's (FISA) enhanced warrantless wiretapping powers in cooperation with complicit telecom providers. In other words, Obama's DOJ absolves itself and its corporate allies of accountability under existing federal statutes that prohibit illegal spying on Americans.

On April 26, Burghhardt reported that "The Pentagon's Cyber Command Formidable Infrastructure arrayed against the American People" will be headed by the NSA's director, Lt. General Keith Alexander, to protect the military's networks from hacker attacks, especially from countries like China and Russia. How this will "affect civilian computer networks is unclear. However, situating" it alongside NSA at Fort Meade, MD "should set alarm bells ringing (because of NSA's) potential for (greater) abuse….given (its) role in illegal domestic surveillance….(and its) tremendous technical capabilities."

"As a Pentagon agency, NSA has positioned itself to seize near total control over the country's electronic infrastructure, thereby exerting an intolerable influence–and chilling effect– over the nation's political life." Recent history shows that "NSA and their partners at CIA, FBI, et. al. have targeted political dissidents," including anti-war protesters, environmentalists, and others for their activism and beliefs. Greater NSA powers will "transform 'cybersecurity' into a euphemism for keeping the rabble in line (and) achieving 'full spectrum dominance' via 'Cyberspace Offensive Counter-Operations.' "

Directed against ordinary Americans, democratic freedoms will be severely compromised. No matter as "the Obama administration (prepares) to hand control of the nation's electronic infrastructure over to a (rogue) agency" – with General Alexander telling the House Armed Services subcommittee that America needs a digital warfare force for defensive and offensive cyber operations. More resources are required to do it, not for public security, but for imperial conquest and containing dissent at home – in violation of constitutional freedoms and international law.

In a follow-up May 4 article, Burghardt explored the secret, unaccountable world of FBI data

mining through its Investigative Data Warehouse (IDW) containing over a billion documents, including many on US citizens. They come from our personal records and history, including what's obtainable online through illegal spying.

According to the Electronic Frontier Foundation's (EFF) Kurt Opsahl, "The IDW includes more than four times as many documents as the Library of Congress, and the FBI has asked for millions of dollars to data-mine this warehouse, using unproven science in an attempt to predict future crimes from past behavior." This illegal spying violates our constitutional right to privacy and endangers our freedom by generating unsubstantiated threats based on pure supposition.

Besides the FBI, it's virtually certain that other, perhaps all 16, government intelligence agencies conduct similar spying illegally, and as such, endanger everyone's freedom.

Earlier on July 14, 2008, an ACLU press release headlined: "Terrorist Watch List Hits One Million Names" based on government reported figures. They include: "Members of Congress, nuns, war heros and other 'suspicious characters' (like anti-war and environmental activists)….trapped in the Kafkaesque clutches of this list, with little hope of escape."

According to the ACLU's Technology and Liberty Program director, Barry Steinhardt, this data base represents "what's wrong with this administration's approach to security: it's unfair, out-of-control, a waste of resources, treats the rights of the innocent as an afterthought, and is a very real impediment in the lives of millions of (people) in this country. Putting a million names on a watch list is a guarantee (it) will do more harm than good" besides being ineffective to catch real criminals.

Given the current scope and intent of FBI data mining, with millions under surveillance, its potential for abuse far exceeds where it stood less than a year ago – because the Obama administration supports it. No longer is anything about us private, including:

— all our financial transactions and records;

— every check written;

— every credit card or other electronic purchase;

— our complete medical history;

— every plane, train, bus or ship itinerary;

— our phone records and conversations; and

— every computer key stroke.

Our entire private world is now public – if spy snoops decide to invade it.

Key Internet-based companies, like Google, do it routinely – the company UK-based Privacy International ranked worst in its September 2007 "Race to the Bottom" report. It stated:

"….throughout our research we have found numerous deficiencies and hostilities in Google's approach to privacy that go well beyond those of other organizations." It tops them all "as an endemic threat to privacy. This is in part due to the diversity and specificity of Google's product range and the ability of the company to share extracted data between these tools, and in part due to Google's market dominance and the sheer size of its user base."

It's also unmatched in "its aggressive use of invasive or potentially invasive technologies and techniques." It's able to "deep-drill into the minutiae of a user's life and lifestyle choices" irresponsibly. Its attitude toward privacy is blatantly hostile at worst and benignly ambivalent at best. Specifically:

— Google retains a large amount of user information with no limitation on its subsequent use or disclosure and with no chance for users to delete or withdraw it;

— it retains all "search strings and associated IP-addresses and time stamps for at least 18 to 24 months (retention) and does not provide users with an expungement option;"

— it has other personal information, including hobbies, employment, addresses, phone numbers, and more, and retains it even after users delete their profiles;

— it "collects all search results entered through Google Toolbar and identifies all Google Toolbar users with a unique cookie that allows Google to track the user's web movement;" it also retains information indefinitely with no expungement option;

— it doesn't follow OECD Privacy Guidelines and EU data protection law provisions;

— users have no option to edit or delete obtained records and information about them; and

— they can't access log information generated through various Google services, such as Google Maps, Video, Talk, Reader, or Blogger.

In 2004, Google also acquired the CIA-linked company Keyhole, Inc., that has a worldwide 3-D spy-in-the-sky images database. Its software provides a virtual fly-over and zoom-in capability to within a one-foot resolution. It's supported by In-Q-Tel, a venture capital CIA-funded firm that "identif(ies) and invest(s) in companies developing cutting-edge

information technologies that serve United States national security interests."

In 2003, its CEO, John Hanke, said: "Keyhole's strategic relationship with In-Q-Tel means that the Intelligence Community can now benefit from the massive scalability and high performance of the Keyhole enterprise solution."

In 2006, former CIA clandestine services case officer, Robert Steele, said:

"I am quite positive that Google is taking money and direction from my old colleague Dr. Rick Steinheiser in the Office of Research and Development at CIA, and that Google has done at least one major prototype effort focused on foreign terrorists which produced largely worthless data….I think (Google is) stupid to be playing with CIA, which cannot keep a secret and is more likely to waste time and money than actually produce anything useful."

On April 29, Willem Buiter's Maverecon site headlined "Gagging on Google" and said:

"Google is to privacy and respect for intellectual property rights what the Taliban are to women's rights and civil liberties: a daunting threat that must be fought relentlessly by all those who value privacy and the right to exercise, within the limits of the law, control over the uses made by others of their intellectual property."

This company should be rigorously regulated, "and if necessary, broken up or put out of business." With about half the global internet search market, it threatens enhanced "corporate or even official Big Brotherism."

For example, Google Street View, an addition to Google Maps, "provides panoram(ic) images visible from street level in cities around the world. The cameras record details of residents' lives" on all sorts of personal matters that no one should be able to snoop on, then save, without permission, for whatever purposes.

The company also invades our privacy through tracking cookies or "third-party persistent cookies" to assist interest-based advertising, a practice known as behavioral targeting. In the wrong hands, this information can be used "to put a commercial squeeze on people, but also to extort and blackmail them." And in government hands, it enhances "a pretty effective and very nasty police state."

Can Google be trusted to use this information responsibly? "Of course not." It's a business run by "amoral capitalists," out to make as much money as possible by any means necessary. Google and other Internet search engines "should not be trusted because they cannot be trusted." However, because of its size and dominance, Google is "the new evil empire of the internet," a "Leviathan" that must be tamed.

Cybersecurity Legislation

On April 1, two bills endangering a free and open Internet were introduced in the Senate:

— S. 773: Cybersecurity Act of 2009 "to ensure the continued free flow of commerce within the United States and with its global trading partners through secure cyber communications, to provide for the continued development and exploitation of the Internet and intranet communications for such purposes, to provide for the development of a cadre of information technology specialists to improve and maintain effective cybersecurity defenses against disruption, and for other purposes."

S. 773 was then referred to the Commerce, Science, and Transportation Committee and thus far not voted on.

— S. 778: A bill to establish, within the Executive Office of the President, the Office of National Cybersecurity Advisor (aka czar). The bill was referred to the Homeland Security and Governmental Affairs Committee and not yet voted on.

Accompanying information said Senators Jay Rockefeller and Olympia Snowe introduced the legislation to address:

> "our country's unacceptable vulnerability to massive cyber crime, global cyber espionage, and cyber attacks that could cripple our critical infrastructure."

We presently face cyber espionage threats, they said, as well as "another great vulnerability….to our private sector critical infrastructure – banking, utilities, air/rail/auto traffic control, telecommunications – from disruptive cyber attacks that could literally shut down our way of life."

"This proposed legislation will bring new high-level governmental attention to develop a fully integrated, thoroughly coordinated, public-private partnership to our cyber security efforts in the 21st century" through what's unstated – government affecting our private lives by threatening the viability of a free and open Internet.

During a March Senate Commerce, Science and Transportation Committee hearing, Senator Rockefeller said that we'd all be better off if the Internet was never invented. His precise words were: "Would it have been better if we'd never have invented the Internet and had to use paper and pencil or whatever!" Left unsaid was that without a free and open Internet, few alternatives for getting real news and information would exist, at least with the ease and free accessibility that computers can provide.

The Electronic Frontier Foundation's Jennifer Granick expressed alarm about the risk of "giving the federal government unprecedented power over the Internet without necessarily improving security in the ways that matter most. (These bills) should be opposed or radically amended."

Here's what they'll do:

— federalize critical infrastructure security, including banks, telecommunications and energy, shifting power away from providers and users to Washington;

— give "the president unfettered authority to shut down Internet traffic in (whatever he calls) an emergency and disconnect critical infrastructure systems on national security grounds….;"

— potentially "cripple privacy and security in one fell swoop" through one provision (alone) empowering the Commerce Secretary to "have access to all relevant data concerning (critical infrastructure) networks without regard to any provision of law, regulation, rule, or policy restricting such access…."

In other words, the Commerce Department will be empowered to access "all relevant data" – without privacy safeguards or judicial review. As a result, constitutionally protected private information statutory protections will be lost – guaranteed under the Electronic Communications Privacy Act, the Privacy Protection Act, and financial privacy regulations.

Another provision mandates a feasibility study for an identity management and authentication program that would sidestep "appropriate civil liberties and privacy protections."

At issue is what role should the federal government play in cybersecurity? How much power should it have? Can it dismiss constitutional protections, and what, in fact, can enhance cybersecurity without endangering our freedoms? S. 773 and 778, as now written, "make matters worse by weakening existing privacy safeguards (without) address(ing) the real problems of security."

In late February, Director of National Intelligence, Admiral Dennis Blair, told the House Intelligence Committee that the NSA, not DHS, should be in charge of cybersecurity even though it has a "trust handicap" to overcome because of its illegal spying:

"I think there is a great deal of distrust of the National Security Agency and the intelligence community in general playing a role outside of the very narrowly circumscribed role because of some of the history of the FISA issue in years past…." So Blair asked the committee's leadership to find a way to instill public confidence.

On February 9, Obama appointed Melissa Hathaway to be Acting Senior Director for Cyberspace for the National Security and Homeland Security Councils – in charge of a 60-day interagency cybersecurity review, now completed.

On April 21, NSA/Chief Central Security Service director, General Alexander, told RSA

Conference security participants that “The NSA does not want to run cybersecurity for the government. We need partnerships with others. The DHS has a big part, you do, and our partners in academia. It’s one network and we all have to work together….The NSA can offer technology assistance to team members. That’s our role.”

But someone has to be in charge. It may or may not be NSA, but no matter. At issue is our constitutional freedoms. Any infringement on them must be challenged and stopped.

Stephen Lendman is a Research Associate of the Centre for Research on Globalization. He lives in Chicago and can be reached at lendmanstephen@sbcglobal.net.

Also visit his blog site at www.sjlendman.blogspot.com and listen to The Global Research News Hour on RepublicBroadcasting.org Monday – Friday at 10AM US Central time for cutting-edge discussions with distinguished guests on world and national issues. All programs are archived for easy listening.

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

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.