GlobalResearch
Center for Research on Globalization

Privacy Protection and the Secret State's Surveillance Powers

By Tom Burghardt
Global Research, April 17, 2011
Antifascist Calling... 17 April 2011

Region: USA
Theme: Police State & Civil Rights

Call it another virtual "defense" of privacy rights by U.S. lawmakers.

In the week of April 11, senators John Kerry (D-MA) and John McCain (R-AZ) introduced legislation in the U.S. Senate, the "Commercial Privacy Bill of Rights Act of 2011," they claimed would "establish a framework to protect the personal information of all Americans."

During a D.C. press conference, McCain told reporters that the proposed law would protect a "fundamental right of American citizens, that is the right to privacy."

While Kerry and McCain correctly state that "The ease of gathering and compiling personal information on the Internet and off, both overtly and surreptitiously, is becoming increasingly efficient and effortless due to advances in technology which have provided information gatherers the ability to compile seamlessly highly detailed personal histories of individuals" (p. 4), there's *one* small catch.

CNET's Declan McCullagh reported that the bill "doesn't apply to data mining, surveillance, or any other forms of activities that governments use to collect and collate Americans' personal information."

While the measure would apply to "companies and some nonprofit groups," CNET disclosed that "federal, state, and local police agencies that have adopted high-tech surveillance technologies including cell phone tracking, GPS bugs, and requests to Internet companies for users' personal information–in many cases without obtaining a search warrant from a judge" would be exempt.

As we know, a gaggle of privacy-killing agencies inside the secret state, the National Security Agency, the Federal Bureau of Investigation, the U.S. Department of Homeland Security as well as offices and subunits sprinkled throughout the Pentagon's sprawling bureaucracy, including U.S. Cyber Command, all claim authority to extract personal information on individuals from still-secret Office of Legal Counsel memoranda and National Security Presidential Directives.

As the American Civil Liberties Union reported in March, what little has been extracted from the Executive Branch through Freedom of Information Act litigation is heavily-redacted, rendering such disclosures meaningless exercises.

For example, the bulk of the November 2, 2001 21-page Memorandum for the Attorney General, penned by former Deputy Assistant Attorney General John C. Yoo, which provided the Bush administration with a legal fig-leaf for their warrantless wiretapping programs, is

blank. That is, if one ignores exemptions to FOIA now claimed by the *Obama* administration. (B1, b3, b5, exemptions relate to "national security," "inter-departmental communications" and/or programs labelled "TS/SCI"–Top Secret/Sensitive Compartmented Information, the highest classification).

And, as of this writing, the American people still do not have have access to nor even knowledge of the snooping privileges granted securocrats by the Bush and Obama administrations under cover of the Comprehensive National Cybersecurity Initiative (CNCI).

As *Antifascist Calling* previously reported, CNCI derives authority from classified annexes of National Security Presidential Directive 54, Homeland Security Presidential Directive 23 (NSPD 54/HSPD 23) first issued by our former "decider."

Those 2008 presidential orders are so contentious that both the Bush and Obama administrations have even refused to release details to Congress, prompting a 2010 Freedom of Information Act lawsuit by the Electronic Privacy Information Center (EPIC) demanding that the full text, and underlying legal authority governing federal cybersecurity programs be made public.

McCullagh points out that the bill "also doesn't apply to government agencies including the Department of Health and Human Services, the Department of Veterans Affairs, the Social Security Administration, the Census Bureau, and the IRS, which collect vast amounts of data on American citizens."

Nor are there provisions in the bill that would force federal or state agencies to notify American citizens in the event of a data breach. No small matter considering the flawed data security practices within such agencies.

Just last week, *InformationWeek* revealed that the "Texas comptroller's office began notifying millions of people Monday that their personal data had been involved in a data breach. The private data was posted to a public server, where it was available–in some cases–for over a year."

"The posted records," we're told, "included people's names, mailing addresses, social security numbers, and in some cases also dates of birth and driver's license numbers."

None of the data was encrypted and was there for the taking by identity thieves or other shady actors. *InformationWeek* pointed out although "most organizations that experience a serious data breach" offer free credit monitoring services to victims, "to date, Texas has not said it will offer such services to people affected by the comptroller's breach."

CNET reminds us that the "Department of Veterans Affairs suffered a massive security breach in 2006 when an unencrypted laptop with data on millions of veterans was stolen."

McCullagh avers that "a government report last year listed IRS security and privacy vulnerabilities" and that "even the Census Bureau has, in the past, shared information with law enforcement from its supposedly confidential files."

The limited scope of the Kerry and McCain proposal is underscored by moves by the Obama Justice Department to actually *increase* the secret state's already formidable surveillance powers and short-circuit anemic privacy reforms that have been proposed.

In fact, as *Antifascist Calling* reported last week, during hearings before the Senate Judiciary Committee, Associate Attorney General James A. Baker warned the panel that granting "cloud computing users more privacy protections and to require court approval before tracking Americans' cell phones would hinder police investigations."

But even when it comes to reining-in out-of-control online tracking by internet advertising firms, the Kerry-McCain bill comes up short.

As the Electronic Frontier Foundation points out, the Kerry-McCain bill won't stop online tracking by advert pimps who hustle consumers' private details to the highest bidder.

The civil liberties' watchdogs aver, "the privacy risk is not in consumers seeing targeted advertisements, but in the unchecked accumulation and storage of data about consumers' online activities."

> "Collecting and retaining data on consumers can create a rich repository of information," EFF's legislative analyst Rainey Reitman writes, one that "leaves consumer data vulnerable to a data breach as well as creating an unnecessary enticement for government investigators, civil litigants and even malicious hackers."

Additionally, the proposal is silent on Do Not Track, "meaning there is no specific proposal for a meaningful, universal browser-based opt-out mechanism that could be respected by all large third-party tracking companies," and consumers "would still need to opt-out of each third party individually," a daunting process.

Worst of all, consumers "won't have a private right of action in the new Commercial Privacy Bill of Rights. That means consumers won't be granted the right to sue companies for damages if the provisions of the Commercial Privacy Bill of Rights are violated." In other words, even when advertising firms and ISPs violate their users' privacy rights, the bill would specifically prohibit individuals from seeking relief in the courts.

Moving in for the Cybersecurity Kill

While the Kerry-McCain bill would exempt government agencies from privacy protections, the Defense Department is aggressively seeking more power to monitor civilian computer networks.

NextGov reported that General Keith Alexander, the dual-hatted commander of U.S. Cyber Command and the National Security Agency said that his agency "cannot monitor civilian networks" and that congressional authorization will be required so that CYBERCOM can "look at what's going on in other government sectors" and other "critical infrastructures," i.e., civilian networks.

Mendacity aside, considering that NSA already vacuums-up terabytes of America's electronic communications data on a daily basis, reporter Aliya Sternstein notes that Alexander "offered hints about what the Pentagon might be pushing the Obama administration to consider."

"Civil liberties and privacy are not [upheld] at the expense of cybersecurity," he said. "They will benefit from cybersecurity," available only, or so we've been led to believe, from the

military, well-known for their commitment to civil liberties and the rule of law as the case of Pfc. Bradley Manning amply demonstrates.

Cyberspace, according to Alexander, is a domain that must be protected like the air, sea and land, "but it's also unique in that it's inside and outside military, civilian and government" domains.

Military forces "have to have the ability to move seamlessly when our nation is under attack to defend it … the mechanisms for doing that have to be laid out and agreed to. The laws don't exist in this area."

While Cyber Command currently shares network security duties with the U.S. Department of Homeland Security, as I reported last year, a Memorandum of Agreement between DHS and NSA, claims that increased "interdepartmental collaboration in strategic planning for the Nation's cybersecurity, mutual support for cybersecurity capabilities development, and synchronization of current operational cybersecurity mission activities," will be beneficial.

We were informed that the Agreement "will focus national cybersecurity efforts, increasing the overall capacity and capability of both DHS's homeland security and DoD's national security missions, while providing integral protection for privacy, civil rights, and civil liberties."

But as Rod Beckström, the former director of Homeland Security's National Cybersecurity Center (NCSC), pointed out in 2009 when he resigned his post, he viewed increased control by NSA over national cybersecurity programs a "power grab."

In a highly-critical letter to DHS Secretary Janet Napolitano, Beckström said that NSA "effectively controls DHS cyber efforts through detailees [and] technology insertions."

Citing the agency's role as the secret state's eyes and ears that peer into America's electronic and telecommunications' networks, Beckström warned that handing more power to NSA could significantly threaten "our democratic processes…if all top level government network security and monitoring are handled by any one organization."

Those warnings have gone unheeded.

National Defense Magazine reported that retired Marine Corps General Peter Pace, the former chairman of the Joint Chiefs of Staff, "would hand over the Department of Homeland Security's cybersecurity responsibilities to the head of the newly created U.S. Cyber Command."

Seconding Pace's call for cybersecurity consolidation, under Pentagon control, Roger Cressey, a senior vice president with the ultra-spooky Booz Allen Hamilton firm, a company that does billions of dollars of work for the Defense Department, "agreed that putting all the responsibility for the federal government's Internet security needs would help the talent shortage by consolidating the responsibilities under one roof."

"The real expertise in the government," Cressey told *National Defense*, "capable of protecting networks currently lies in the NSA."

Cressey's is hardly an objective opinion. The former member of the National Security Council and the elitist Council on Foreign Relations, joined Booz Allen after an extensive

career inside the secret state.

A military-industrial complex powerhouse, Booz Allen clocks-in at No. 9 on Washington Technology's list of 2010 Top 100 Contractors with some $3.3 billion in revenue.

As *Spies For Hire* author Tim Shorrock pointed out for CorpWatch, "Among the many services Booz Allen provides to intelligence agencies ... are data-mining and data analysis, signals intelligence systems engineering (an NSA specialty), intelligence analysis and operations support, the design and analysis of cryptographic or code-breaking systems (another NSA specialty), and 'outsourcing/privatization strategy and planning'."

With "data mining, surveillance, or any other forms of activities that governments use to collect and collate Americans' personal information" off the Kerry-McCain "privacy" bill table, as CNET reported, enterprising security firms are undoubtedly salivating over potential income–and lack of accountability–which a cybersecurity consolidation, Pentagon-style, would all but guarantee.

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, he is a Contributing Editor with Cyrano's Journal Today. His articles can be read on Dissident Voice, The Intelligence Daily, 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.*
