GlobalResearch
Center for Research on Globalization

Big Brother Obama: White House Plans Internet ID System

By Tom Burghardt
Global Research, January 18, 2011
Antifascist Calling... 18 January 2011

Region: USA
Theme: Police State & Civil Rights

by ***Antifascist Calling…***

Urged by one and all to "tone down" what media pundits and political elites describe as "strident," even "violent" rhetoric that has "poisoned" our "national conversation" and "sharply polarized" the population, the shooting rampage in Tucson which claimed six lives, including that of a nine-year-old girl is, in fact, emblematic of the moral bankruptcy and utter hypocrisy of those selfsame capitalist elites.

Faced with an unprecedented economic crisis that has destroyed the lives of tens of millions our fellow citizens, not to mention aggressive wars which have cratered entire societies and murdered hundreds of thousands of people who have done us no harm, when, pray tell, will the "conversation" turn to the unprecedented annihilation of democratic institutions and the rule of law which exonerates, even *celebrates*, those who murder, maim and torture on an industrial scale?

Just last week, the Obama administration announced plans to roll-out an "identity ecosystem" for the internet. Although passed over in silence by major media, at the risk of being accused of "incivility," particularly when it comes to the "hope" fraudster and war criminal in the Oval Office, Americans need to focus–sharply–on the militarists, political bag men and corporate gangsters working to bring George Orwell's dystopian world one step closer to reality.

Earlier this month, **CNET** disclosed that the administration "is planning to hand the U.S. Commerce Department authority over a forthcoming cybersecurity effort to create an Internet ID for Americans."

White House Cybersecurity Coordinator Howard Schmidt said that the secret state's latest move to lower the boom on privacy and free speech will embed the surveillance op at the Commerce Department. Schmidt, speaking at the Stanford Institute for Economic Policy Research said Commerce is "the absolute perfect spot in the U.S. government" to centralize these efforts.

According to CNET, the move "effectively pushes the department to the forefront of the issue, beating out other potential candidates, including the National Security Agency and the Department of Homeland Security."

Really? I don't think so.

NSA Clearly in the Frame

Last week, ***Government Computer News*** reported that the secretive Pentagon spy shop broke ground on a "massive new National Security Agency cyber intelligence center in Utah."

The multibillion dollar facility (cost overruns not included) "will have 100,000 square feet of raised-floor data center space and more than 900,000 square feet of technical support and administrative space" that "will support the Comprehensive National Cybersecurity Initiative."

In September, **NextGov** reported that then Deputy Director of National Intelligence for Collection, Glenn Gaffney, said the new data center "would support the intelligence community in providing foreign intelligence about cybersecurity threats and protect Defense Department networks."

Back in 2009, investigative journalist James Bamford wrote in ***The New York Review of Books*** that "the mammoth $2 billion structure will be one-third larger than the US Capitol and will use the same amount of energy as every house in Salt Lake City combined."

While corporate media tell us that the center will "enhance" the nation's capacity to thwart "cyber threats" the fact is, Bamford wrote, the complex will "house trillions of phone calls, e-mail messages, and data trails: Web searches, parking receipts, bookstore visits, and other digital 'pocket litter'." In other words, the vast data repository will serve as "spy central" for our digital minders.

"Just how much information will be stored in these windowless cybertemples?" Bamford wondered. According to a report prepared for the Pentagon by the ultra-spooky **MITRE Corporation**, "as the sensors associated with the various surveillance missions improve, the data volumes are increasing with a projection that sensor data volume could potentially increase to the level of Yottabytes (10 to the 24 Bytes) by 2015."

This is "roughly equal to about a septillion (1,000,000,000,000,000,000,000,000) pages of text, numbers beyond Yottabytes haven't yet been named," Bamford avers.

Leaving aside disinformational pyrotechnics by media cheerleaders that the NSA's data equivalent of a Wal-Mart supercenter will primarily exist for "cybersecurity," "foreign intelligence" and protecting "Defense Department networks," Bamford counters that "once vacuumed up and and stored in these near-infinite 'libraries,' the data are then analyzed by powerful infoweapons, supercomputers running complex algorithmic programs, to determine who among us may be–or may one day become–a terrorist."

"In the NSA's world of automated surveillance on steroids" Bamford avers, "every bit has a history and every keystroke tells a story."

Or as **Cryptohippie** puts it far less delicately, every keystroke or cellphone ping is "criminal evidence, ready for use in a trial."

Just what *are* they up to? Even Congress, always willing to give the Executive Branch a free pass when it comes to blanket surveillance, doesn't know. Last week the ***Associated Press*** reported that "the Pentagon failed to disclose clandestine cyber activities in a classified report on secret military actions that goes to Congress."

Citing “gaps” in reporting requirements on clandestine operations, “emerging high-tech operations are not specifically listed in the law,” AP averred. After all, “cyber oversight is still a murky work in progress for the Obama administration.”

Perhaps AP and other media outlets should look more closely at what’s hidden inside that “murky work” and where its authority comes from. “Oversight” is certainly *not* part of the equation.

Cybersecurity’s Brave New World

As ***Antifascist Calling*** previously reported, the operational nuts-and-bolts of the Comprehensive National Cybersecurity Initiative (**CNCI**) is a closely-held state secret that derives authority from classified annexes of the National Security Presidential Directive 54, Homeland Security Presidential Directive 23 (NSPD 54/HSPD 23) issued by our former “decider.”

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

Details on the “trusted identity” scheme are scarce, but back in July ***Antifascist Calling*** reported that the secret state had deployed *New York Times* reporter John Markoff as a conduit for administration **scaremongering**.

Schmidt told the “Gray Lady” that administration plans involved “a ‘voluntary trusted identity’ system that would be the high-tech equivalent of a physical key, a fingerprint and a photo ID card, all rolled into one.”

According to the *Times*, “the system might use a smart identity card, or a digital credential linked to a specific computer, and would authenticate users at a range of online services.”

U.S. Commerce Secretary Gary Locke was quick to downplay the more sinister implications of the hustle saying, “We are not talking about a national ID card.”

CNET reported Locke’s claim that “we are not talking about a government-controlled system. What we are talking about is enhancing online security and privacy, and reducing and perhaps even eliminating the need to memorize a dozen passwords, through creation and use of more trusted digital identities.”

Why bother with privacy when surrendering your rights is so convenient!

Touted as a warm and fuzzy “identity ecosystem,” ***Government Computer News*** reported that the National Institute of Standards and Technology (NIST) has even launched a dedicated website hawking the National Strategy for Trusted Identities in Cyberspace (**NSTIC**).

According to NIST, “NSTIC envisions a cyber world–the Identity Ecosystem–that improves upon the passwords currently used to login online.”

We’re informed that the “Identity Ecosystem will provide people with a variety of more secure and privacy-enhancing ways to access online services. The Identity Ecosystem

enables people to validate their identities securely when they're doing sensitive transactions (like banking) and lets them stay anonymous when they're not (like blogging). The Identity Ecosystem will enhance individuals' privacy by minimizing the information they must disclose to authenticate themselves."

Government Computer News tells us that the "identity ecosystem" isn't envisaged as a "national Internet ID to track online activities." The devil's in the details and what little we do know should set alarm bells ringing.

The program office will "support and coordinate interagency collaboration" and "promote pilot projects and other implementations." Which agencies are we talking about here? What pilot projects and "other implementations" are being alluding to? We don't know.

We *do* know however, that the National Security Agency and Department of Homeland Security have forged a **Memorandum of Agreement** which will increase Pentagon control over America's telecommunications and electronic infrastructure

In fact, as the Electronic Frontier Foundation **disclosed** in October, DHS has been tracking people online and that the agency even established a "Social Networking Monitoring Center" to explicitly do so.

Documents obtained by the civil liberties watchdog group revealed that the agency has been vacuuming-up "items of interest," systematically monitoring "citizenship petitioners" and analyzing "online public communication."

Wouldn't an "identity ecosystem" greatly facilitate online spying, despite administration claims to the contrary?

While the system is "voluntary" and individuals will not be compelled to sign up, the secret state is lusting after a sure fire means to identify the billions of computers, smart phones and other digital devices that plague us.

And even if you choose not to "opt in," well, plans are already afoot by advertising pimps and their partners in the national security state "to collect the digital equivalent of fingerprints from every computer, cellphone and TV set-top box in the world," ***The Wall Street Journal*** recently disclosed.

As with all other aspects of the "War on Terror" threatscape, the closer one looks at the Obama regime's "identity ecosystem" the less warm and fuzzy it becomes.

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****,, 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.*

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

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