GlobalResearch
Center for Research on Globalization

Are You a "Perfect Citizen"? Big Brother Deploys Snooping Sensors on Private Networks

By Tom Burghardt
Global Research, July 12, 2010
Antifascist Calling... 11 July 2010

Region: USA
Theme: Police State & Civil Rights

Rather than addressing an impending social catastrophe, Western governments, which serve the interests of the economic elites, have installed a "Big Brother" police state with a mandate to confront and repress all forms of opposition and social dissent. — Michel Chossudovsky and Andrew Gavin Marshall, Preface, The Global Economic Crisis: The Great Depression of the XXI Century, Montreal: Global Research, 2010, p. xx.

In a sign that illegal surveillance programs launched by the Bush administration are accelerating under President Obama, The Wall Street Journal revealed last week that a National Security Agency (NSA) program, PERFECT CITIZEN, is under development.

With a cover story that this is merely a "research" effort meant to "detect cyber assaults on private companies and government agencies running such critical infrastructure as the electricity grid and nuclear-power plants," it is also clear that the next phase in pervasive government spying is underway.

With "cybersecurity" morphing into a new "public-private" iteration of the "War On Terror," WSJ reporter Siobhan Gorman disclosed that giant defense contractor Raytheon "recently won a classified contract for the initial phase of the surveillance effort valued at up to $100 million."

This wouldn't be the first time that Raytheon had positioned itself, and profited from, a media-driven panic. As investigative journalist Tim Shorrock documented for CorpWatch, "as the primary spying unit of defense industry giant Raytheon," the firm's Intelligence and Information Services division (Raytheon IIS) is the premier provider of command and control systems "capable of transforming data into actionable intelligence."

According to Shorrock, the unit's "most important clients … are the NSA, NGA, and NRO, for which it provides signals and imaging processing, as well as information security software and tools;" in other words, agencies that are at the heart of America's electronic warfare complex.

The program, Gorman writes, "would rely on a set of sensors deployed in computer networks for critical infrastructure that would be triggered by unusual activity suggesting an impending cyber attack." While Journal sources claim the program "wouldn't persistently monitor the whole system," a leaked Raytheon email paints a different picture, in line with other NSA intrusions into domestic affairs.

"The overall purpose of the [program] is our Government…feel[s] that they need to insure the Public Sector is doing all they can to secure Infrastructure critical to our National

Security," the whistleblower writes. "Perfect Citizen is Big Brother."

These revelations have triggered concerns that projects like PERFECT CITIZEN, and others that remain classified, signal a new round of secret state surveillance and privacy-killing programs under the catch-all euphemism "cybersecurity."

The Journal reports that information captured by PERFECT CITIZEN "could also have applications beyond the critical infrastructure sector, officials said, serving as a data bank that would also help companies and agencies who call upon NSA for help with investigations of cyber attacks, as Google did when it sustained a major attack late last year."

In other words, the program will have major implications "beyond the critical infrastructure sector" and could adversely affect the privacy rights of all Americans. In fact, it wouldn't be much of a stretch to hypothesize that PERFECT CITIZEN may very well be related to other "intrusion detection programs" such as Einstein 3's deep-packet inspection capabilities that can read, and catalogue, the content of email messages flowing across private telecommunications networks.

One unnamed military source told the Journal, "you've got to instrument the network to know what's going on, so you have situational awareness to take action."

However, as the UK publication The Register noted, "many of the networks that the NSA would wish to place Perfect Citizen equipment on are privately owned, however, and some could also potentially carry information offering scope for 'mission creep' outside an infrastructure-security context."

The Register's Lewis Page, a former Royal Navy Commander and frequent critic of the surveillance state, writes that "full access to power company systems might allow the NSA to work out whether anyone was at home at a given address. Transport and telecoms information would also make for a potential bonanza for intrusive monitoring."

When queried whether the program would be yet another snooping tool deployed against the public, NSA spokesperson Judith Emmel told The Register Friday: "PERFECT CITIZEN is purely a vulnerabilities-assessment and capabilities-development contract."

According to NSA, "This is a research and engineering effort. There is no monitoring activity involved, and no sensors are employed in this endeavor. Specifically, it does not involve the monitoring of communications or the placement of sensors on utility company systems."

When specifically asked by Page if NSA is "seeking to spy on US citizens by means of examining their power or phone usage, tracking them through transport systems etc, the NSA would simply never think of such a thing."

"Any suggestions that there are illegal or invasive domestic activities associated with this contracted effort are simply not true. We strictly adhere to both the spirit and the letter of US laws and regulations," insisted Emmel.

Which raises an inevitable question: what would lead a Raytheon insider to compare the project to "Big Brother"? This is strong language from an employee of one of America's largest defense firms, a company in the No. 4 slot on Washington Technology's 2010 Top 100 list of prime federal contractors with some $6.7 billion in total revenue, 88% of which are derived from defense contracts.

At this point we don't know, and Siobhan Gorman hasn't told us since the Journal, as of this writing, hasn't seen fit to enlighten the public with the full text, if one exists, as to why someone obviously familiar with the program would put their job at risk if PERFECT CITIZEN were simply a "vulnerabilities-assessment and capabilities-development contract" and not something far more sinister.

The Pentagon Rules. Any Questions?

The Journal reported that the project began as "a small-scale effort" under the code name APRIL STRAWBERRY. Over time, the classified program was "expanded with funding from the multibillion-dollar Comprehensive National Cybersecurity Initiative, which started at the end of the Bush administration and has been continued by the Obama administration," Gorman wrote. Now, with billions of dollars available "the NSA is now seeking to map out intrusions into critical infrastructure across the country."

As Antifascist Calling reported earlier this year (see: "Obama's National Cybersecurity Initiative Puts NSA in the Driver's Seat"), although the administration has released portions of the Bush regime's National Security Presidential Directive 54 (NSPD-54) in a sanitized version called the Comprehensive National Cybersecurity Initiative (CNCI), the full scope of the program remains shrouded in secrecy.

Indeed, most of NSPD-54 and CNCI have never been released to the public. This led the Senate Armed Services Committee (SASC) to write in a 2008 report that "virtually everything about the initiative is classified, and most of the information that is not classified is categorized as 'For Official Use Only'."

Due to the opacity of the highly-secretive program and stonewalling by the administration, the SASC joined their colleagues on the Senate Select Committee on Intelligence and called for the initiative to be scaled-back "because policy and legal reviews are not complete, and because the technology is not mature."

Hardly beacons of transparency themselves when it comes to overseeing depredations wrought by the secret state, nevertheless SASC questioned the wisdom of a program that "preclude public education, awareness and debate about the policy and legal issues, real or imagined, that the initiative poses in the areas of privacy and civil liberties. … The Committee strongly urges the [Bush] Administration to reconsider the necessity and wisdom of the blanket, indiscriminate classification levels established for the initiative."

In fact, as the investigative journalism web site ProPublica reported last summer, the White House "has erased all mention of the Privacy and Civil Liberties Oversight Board from its Web site. The removal, which was done with no public notice, has underlined questions about the Obama administration's commitment to the board." As of this writing, it remains an empty shell.

Despite repeated efforts by civil liberties and privacy groups, the Obama administration has been no more forthcoming than the previous regime in answering these critical concerns, particularly when the "policy and legal issues" are cloaked in secrecy under a cover of "national security."

Instead, CNCI's "Initiative #12. Define the Federal role for extending cybersecurity into critical infrastructure domains," offer little more than linguistic sedatives meant to lull the

public as to how and through what means the administration plans to build "on the existing and ongoing partnership between the Federal Government and the public and private sector owners and operators of Critical Infrastructure and Key Resources (CIKR)."

While the administration claims that the "Department of Homeland Security and its private-sector partners have developed a plan of shared action with an aggressive series of milestones and activities," as we now know the civilian, though securocratic-minded Homeland Security bureaucracy is being supplanted by the Pentagon's National Security Agency and U.S. Cyber Command as the invisible hands guiding the nation's "cybersecurity" policies.

As I reported last month (see: "Through the Wormhole: The Secret State's Mad Scheme to Control the Internet"), corporate greed and venality aren't the only motives behind hyped-up "cyber threats." Armed with multibillion dollar budgets, most of which are concealed from public view under a black cone of top secret classifications, agencies such as NSA are positioning themselves as gatekeepers over America's electronic communications infrastructure.

The Media's Role

With corporate media serving as "message force multipliers" for the flood of alarmist reports emanating from industry-sponsored think tanks such as the Bipartisan Policy Center (BPC) and the Center for Strategic and International Studies (CSIS), or lobby shops like the Armed Forces Communications and Electronics Association (AFCEA) and the Intelligence and National Security Alliance (INSA), it is becoming clear that consensus has been reached amongst Washington power brokers, one that will have a deleterious effect on the free speech and privacy rights of all Americans.

Floated perhaps as a means to test the waters for restricting internet access, The New York Times reported July 4 that "the Internet affords anonymity to its users–a boon to privacy and freedom of speech. But that very anonymity is also behind the explosion of cybercrime that has swept across the Web."

Reporter John Markoff, a conduit for "cyberwar" scaremongering, informs us that "Howard Schmidt, the nation's cyberczar, offered the Obama administration's proposal to make the Web a safer place–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."

"The system" Markoff writes, "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."

Schmidt has described the Obama administration's approach (note the warm and fuzzy phrase hiding the steel fist) as a "voluntary ecosystem" in which "individuals and organizations can complete online transactions with confidence, trusting the identities of each other and the identities of the infrastructure that the transaction runs on."

Markoff's reporting would be humorous if we didn't already know that secret state agencies themselves have already compromised the Secure Socket Layer certification process (SSL, the tiny lock that appears during supposedly "secure" online transactions), as computer security and privacy researchers Christopher Soghoian and Sid Stamm revealed in their paper, Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL.

In March, Soghoian and Stamm introduced the public to "a new attack, the compelled certificate creation attack, in which government agencies compel a certificate authority to issue false SSL certificates that are then used by intelligence agencies to covertly intercept and hijack individuals' secure Web-based communications." They provided "alarming evidence" that suggests "that this attack is in active use," and that a niche security firm, Packet Forensics, is already marketing "extremely small, covert surveillance devices for networks" to government agencies.

Not everyone is thrilled by Schmidt's call to create this allegedly "voluntary" system. Lauren Weinstein, the editor of Privacy Journal, told the Times that "such a scheme is a pre-emptive push toward what would eventually be a mandated Internet 'driver's license' mentality."

The stampede for increased state controls are accelerating. Stewart Baker, the NSA's chief counsel under Bush, told the Times that the "privacy standards the administration wants to adopt will make the system both unwieldy and less effective and not good for security." Baker and his ilk argue that all internet users "should be forced to register and identify themselves, in the same way that drivers must be licensed to drive on public roads."

Considering that police have increasingly turned to license plate readers that are fast becoming "a fixture in local police arsenals," as the Center for Investigative Reporting revealed last month, and that such devices have been deployed for political surveillance here in the heimat and abroad, as both The Guardian and Seattle Weekly disclosed in reports documenting outrageous secret state spying, a licensing scheme for internet users is an ominous analogy indeed!

The Grim Road Ahead

A confidence game only works when "marks," in this case American citizens, allow themselves to be defrauded by a person or group who have gained their trust.

And when trust cannot be won through reason, fear tends to take over as a powerful motivator. This is amply on display when it comes to Washington's ginned-up "cybersecurity" panic.

According to this reading, fraudulent internet schemes, identity theft, even espionage by state- and non-state actors (say corporate spies who benefit from NSA's ECHELON program) have been transformed into a "war," one which Bush's former Director of National Intelligence, Mike McConnell, currently an executive vice president with the spooky Booz Allen Hamilton firm, claims the U.S. is "losing."

But as security technology expert Bruce Schneier wrote last week, "There's a power struggle going on in the U.S. government right now.

"It's about who is in charge of cyber security, and how much control the government will exert over civilian networks. And by beating the drums of war, the military is coming out on top."

Schneier avers that "the entire national debate on cyberwar is plagued with exaggerations and hyperbole." Googling "cyberwar," as well as "'cyber Pearl Harbor,' 'cyber Katrina,' and even 'cyber Armageddon'–gives some idea how pervasive these memes are. Prefix 'cyber' to something scary, and you end up with something really scary."

Hackers, criminals and sociopaths have been around since the birth of the “information superhighway.” Schneier writes, “we surely need to improve our cybersecurity. But words have meaning, and metaphors matter. There’s a power struggle going on for control of our nation’s cybersecurity strategy, and the NSA and DoD are winning. If we frame the debate in terms of war, if we accept the military’s expansive cyberspace definition of ‘war,’ we feed our fears.”

This is precisely the intent of our political masters. And if the purpose of “cyberwar” hype is to breed fear, mistrust and helplessness in the face of relentless attacks by shadowy actors only a mouse click away then, as Schneier sagely warns: “We reinforce the notion that we’re helpless–what person or organization can defend itself in a war?–and others need to protect us. We invite the military to take over security, and to ignore the limits on power that often get jettisoned during wartime.”

Destroy trust, increase fear: create the “Perfect Citizen.”

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