GlobalResearch
Center for Research on Globalization

The “Hi Tech” Corporate Police State: “Reengineering” the Internet … for Persistent Surveillance

Ghost in the Machine: Secret State Teams Up with Ad Pimps to Throttle Privacy

By Tom Burghardt
Global Research, December 02, 2010
Antifascist Calling... 2 December 2010

Theme: Intelligence, Police State & Civil Rights

The secret world of “cyber situational awareness” is a spymaster’s wet dream, made all the more alluring by the advent of ultra high speed computing and the near infinite storage capacity afforded by massive server farms and the ubiquitous “cloud.”

Within that dusky haze, obscured by claims of national security or proprietary business information, take your pick, would *you* bet your life that the wizards of misdirection and deception care a whit that you really *are* more than a disembodied data point?

Lost in the debate surrounding privacy invasion and data mining however, is the key role that internet service providers (ISPs) play as intermediaries and gatekeepers. From their perch, ISPs peer deeply into and collect and analyze the online communications of tens of millions of users simultaneously, in real-time.

Concerted efforts to eliminate online anonymity, in managed democracies and authoritarian regimes alike, are greatly enhanced by the deployment of deep packet inspection (DPI) sensors and software on virtually all networks.

As Canadian privacy watchdogs **DeepPacketInspection.ca** tell us, DPI offer ISPs “unparalleled levels of intelligence into subscribers’ online activities.”

“To unpack this a little” they aver, “all data traffic that courses across the ‘net is contained in individual packets that have header (i.e. addressing) information and payload (i.e. content) information. We can think of this as the address on a postcard and the written and visual content of a postcard.”

All of which is there for the taking, “criminal evidence, ready for use in a trial,” **Cryptohippie** chillingly informs.

Still the illusion persists that communication technologies are somehow “neutral.” Neither good nor bad but rather, much like a smart phone loaded with geolocation tracking chips or the surveillance-ready internet itself, simply *there* for all to use.

Reality as is its wont, bites with ever-sharper teeth.

As with other recent advances touted as breakthroughs–from the biomedical and

pharmaceutical research that spawned factory farming and genetically-modified crops to something as seemingly banal as the highway system that ushered in exurban sprawl–from the workplace to the car-pool lane to idle hours spent trolling the web, our techno-toys function rather handily as instruments of *social control*.

Simply put, DPI hand our minders an unprecedented means to examine and catalogue our online communications. From blog posts to web searches to the content of email and video files, we're delivered up every day, figuratively and literally, to advertising pimps or law enforcers, a faceless army of gatekeepers guarding an indefensible system in perpetual crisis.

Subtly guiding internet traffic into fast and slow lanes, based on the size and content of a particular file, or examining said file for malicious or illegal content, DPI has been deployed as a means of conserving bandwidth and as a defense against viral attacks.

Leaving aside the critical issue of net neutrality, linked to moves to further monetize the internet and hold communications hostage to the ability to pay for quicker network speeds, there is no question that ISPs and individual users should have a keen interest in defending themselves against the depredations of organized gangs of identity thieves and predators.

If DPI were solely a tool to weed out malicious hacks or channel traffic in more equitable ways, thereby ensuring the broadest possible access to all, it *could* provide concrete benefits to users and contribute to a safer and more secure communications' environment.

This hasn't happened. Instead, securocrats and corporatists alike are working feverishly to "reengineer the internet"–for the delivery of targeted ads and as a surveillance platform–and both view DPI's ability to read individual messages, the "deep packet" as it were, as a singular means to do just that.

Last year, ***Antifascist Calling*** reported on moves by surveillance mavens to deploy deep packet sniffing Einstein 3 software developed by the National Security Agency on the nation's telecommunications infrastructure.

As with the agency's pervasive driftnet spying on Americans, as AT&T whistleblower Mark Klein revealed in his release of internal company **documents**, DPI and the hardware that powers it is the "secret sauce" animating these illegal programs.

Earlier this year, Klein told ***Wired Magazine*** that the documents suggest that NSA's warrantless wiretapping "was just the tip of an eavesdropping iceberg," evidence of "an untargeted, massive vacuum cleaner sweeping up millions of peoples' communications every second automatically."

Ostensibly designed for detecting and thwarting malicious attacks aimed at government networks, ***The Wall Street Journal*** revealed that the packet sniffing Einstein 3 program, developed under the code name TUTELAGE, can screen computer traffic flowing into state portals from private sector networks, including those connecting people to the internet.

"Its filtering technology," journalist Siobhan Gorman wrote, "can read the content of email and other communications."

Einstein 3 is considered so toxic to privacy that AT&T sought "legal assurance that it will not be sued for participating in the pilot program," ***The Washington Post*** reported. Although

they were given assurances by Bush's former Attorney General, Michael B. Mukasey, that the firm "would bear no liability," AT&T deferred until the Obama administration granted the waiver in 2009. So far, the federal government has expended some $2 billion on the program.

Jacob Appelbaum, a security researcher with the **Tor Anonymity Project** told **CNET News** in March that expanding Einstein 3 to private networks "would amount to a partial outsourcing of security" to unaccountable corporations.

But it will do much, much more. Appelbaum averred that the project represents "a clear loss of control [for the public]. And anyone with access to that monitoring system, legitimate or otherwise, would be able to monitor amazing amounts of traffic."

A year later, a related program under development by NSA and defense giant Raytheon, "Perfect Citizen," relies on a suite of sensors deployed in computer networks that will persistently monitor whichever system they are plugged into. While little has been revealed about how Perfect Citizen will work, it was called by a corporate insider the cyber equivalent of "Big Brother," according to an email obtained by ***The Wall Street Journal***.

I have pointed out many times that under the rubric of cybersecurity (the latest profit-generating "War on Terror" front), the secret state, America's telecoms and internet service providers are conjoined at the hip in what are blandly called "public-private partnerships."

Indeed, the secrecy-shredding web site **Public Intelligence**, posted a confidential **document** that provided details on the inner workings of one such initiative, Project 12.

Ultimately, the goal of the secretive enterprise, **Public Intelligence** averred, "is not simply to increase the flow of 'threat information' from government agencies to private industry, but to facilitate greater 'information sharing' between those companies and the federal government."

This will be accomplished once "real-time cyber situational awareness" is achieved across all eighteen critical infrastructure and key resources (CIKR) sectors identified in the report.

Simply put, NSA's warrantless wiretapping program and a constellation of top secret cybersecurity projects will come to nought if filtering software that examines–and catalogues–the content, or deep packets, of those spied upon aren't deployed across all networks, public and private.

No surprise then, that the origins of the ghost in the internet surveillance machine lie in unscrupulous efforts by advert pimps to deliver us to market.

"Opting In" to the Corporate Police State

Readers are familiar with the practice of web sites that install tracking "cookies" and other nasty bits of code that follow our antics across the internet.

This information is sold to advertisers by firms such as Google and Yahoo who charge a premium price for the privilege of peering into browsing habits.

Last month ***The Wall Street Journal*** reported that a gaggle of niche firms "harvest online

conversations and collect personal details from social-networking sites, résumé sites and online forums where people might discuss their lives."

We're told that the dubious practice of "web scraping" provides the "raw material" in a rapidly expanding "data economy." *Journal* reporters found that marketers "spent $7.8 billion on online and offline data in 2009" and that "spending on data from online sources is set to more than double, to $840 million in 2012 from $410 million in 2009."

And with incentives such as these, and virtually nothing in the way of regulation, is it any wonder we find ourselves preyed upon.

While we might garner a measure of privacy from the prying eyes of ISPs, marketing vultures and our political minders through the use of strong encryption, as I **reported** last month, the Obama administration will soon seek congressional authorization which mandates that software designers and social networking sites build backdoors into their systems.

According to ***The New York Times***, the administration claims this is necessary so that law enforcement and intelligence snoops have a surefire means "to intercept and unscramble encrypted messages," because their "ability to wiretap criminal and terrorism suspects is 'going dark'."

Mendacious administration claims are more than matched by those in the online advertising industry.

Last week, ***The Wall Street Journal*** reported that deep packet inspection, "one of the most potentially intrusive technologies for profiling and targeting Internet users with ads is on the verge of a comeback, two years after an outcry by privacy advocates in the U.S. and Britain appeared to kill it."

Advertising grifters **Kindsight** and **Phorm** "are pitching deep packet inspection services as a way for Internet service providers to claim a share of the lucrative online ad market."

Right up front, Phorm declares that theirs' is a "global personalisation technology company" that "delivers a more interesting online experience," that is, if your interests lie in having a behavioral profile of yourself created, centered around intrusive web tracking and data mining technologies.

While both firms claim that user privacy is of "paramount" concern, the industry's track record suggests otherwise. In 2008 for example, internet marketing firm NebuAd planned to "use deep packet inspection to deliver targeted advertising to millions of broadband subscribers unless they explicitly opted out of the service."

An outcry ensued when the scheme became public knowledge. While NebuAd has gone out of business, "several U.S. ISPs who signed deals with NebuAd have been hit with class-action lawsuits accusing them of 'installing spyware devices; on their networks," the *Journal* averred.

According to **Ars Technica**, the **lawsuit** charged the firm and ISPs "Bresnan Communications, Cable One, CenturyTel, Embarq, Knology, and WOW! of all being involved in the interception, copying, transmission, collection, storage, usage, and altering of private data from users."

NebuAd was accused by plaintiffs of exploiting "normal browser platform security behaviors by forging IP packets, allowing their own JavaScript code to be written into source code trusted by the web browser," the complaint reads. "NebuAd and ISPs together cooperate in this attack against the intentions of the consumers, the designers of their software, and the owners of the servers they visit," attorneys charged.

"All of the involved parties," journalist Jacqui Cheng wrote, were "alleged to have violated the Electronic Communications Privacy Act of 1986, California's Computer Crime Law, the federal Computer Fraud and Abuse Act, and the California Invasion of Privacy Act."

In Britain, a similar controversy erupted when BT Group PLC were forced to disclose that they "had tested Phorm's technology on some subscribers without telling them. Last year, BT and two other British ISPs that explored deploying Phorm's service–Virgin Media Inc. and TalkTalk–abandoned it," the *Journal* reported.

At the time, the nose-tweaking tech web site ***The Register*** revealed that although Phorm refused to state how many BT customers had been profiled, "at the absolute least there are 38,000 BT Retail customers unaware their communications have been allegedly criminally intercepted in the last two years. The number could be as high as 108,000."

When grilled by *The Register* as to why Phorm doesn't believe "people have the right to know how likely it is they were part of a secret test," a Phorm spokesperson replied "'We're just not going to disclose that'." He claimed "'they were BT customers and you have to ask BT about that'."

BT also refused to respond to inquiries. How's that for transparency!

Why then, should users believe industry professions of faith that ISPs won't provide them with subscribers' real identities? After all, as one wag told the *Journal*, ISPs "feel like they have data and they ought to be able to use it" and "they really desperately want to."

Accordingly, the *Journal* reported that Kindsight, owned by telecommunications giant Alcatel-Lucent SA (talk about a seamless web!), "says six ISPs in the U.S., Canada and Europe have been testing its security service this year although it isn't yet delivering targeted ads. It declined to name the clients."

CEO Mike Gassewitz told *Journal* reporters that the company "has been placing ads on various websites to test the ad-placement technology and build up a base of advertisers, which now number about 100,000."

Phorm's history hardly inspires confidence. CEO Kent Ertugrul, "a Princeton-educated, former investment banker," we're informed by the *Journal*, honed his business skills in the early 1990s when he formed "a joint venture with the Russian Space Agency to offer joy rides to tourists in MiG-29 fighter jets."

Coming at the height of the Yeltsin kleptocracy that looted billions of dollars in assets from the sell-off of the prized possessions of the former Soviet Union, at the very least this should have raised an eyebrow or two.

Before changing its name to Phorm in 2007, Ertugrul ran an enterprise called 121Media. According to numerous published reports, the firm produced a spyware application called PeopleOnPage. "This application," **Wikipedia** averred, "acted as a browser hijacker and

passed details of the user's currently visited website to central ContextPlus servers, so that the user could be targeted with advertising" in the form of intrusive pop-ups.

The adware component, AproposMedia, was described by InternetSecurityZone.com as "...a malicious executable program that is usually installed without user consent or knowledge. AproposMedia may have the ability to secretly monitor, record, and transmit computer activity." Indeed, ***The Register*** reported that Ertugrul's PeopleOnPage ad network "was blacklisted as spyware by the likes of Symantec and F-Secure."

Former pop-up king Ertugrul has called online rights' campaigners "privacy pirates" who represent a "neo-Luddite retrenchment," and told ***The Daily Telegraph*** last year that Phorm's technology is a "game changer" in "protecting users' privacy."

But armed with a marketing scheme that promises "the potential for companies to collect substantially more revenue for literally any page on the internet," serious privacy concerns are a real issue when deep packet inspection technologies are touted as a splendid means to do so.

Web inventor Tim Berners-Lee told ***New Scientist*** in 2009 that the "ever-increasing power of computers that is helping the internet to grow is also threatening its future."

Berners-Lee "likened DPI to wiretapping, and pointed out that companies could use it to learn a huge amount about our 'lives, hates and fears'."

Information I might add, that is portable and readily exploitable by our political minders and the corporate grifters they so lovingly serve.

And with a national security state already monitoring huge volumes of data collected from the internet and other electronic communications' platforms, ***The Guardian*** warns that Britain and other managed Western democracies are "sleepwalking into a surveillance society."

Isn't it time we woke up?

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*.

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