GlobalResearch
Center for Research on Globalization

Underming the American People's Right to Privacy: The Secret State's Surveillance Machine

Following the Money Trail: Telecoms and ISPs

By Tom Burghardt
Global Research, December 11, 2009
Antifascist Calling... 10 December 2009
Region: USA
Theme: Intelligence, Police State & Civil Rights

"Follow the money."

And why not. As the interface between state and private criminality, following the money trail is oxygen and combustible fuel for rooting out corruption in high places: indelible signs left behind like toxic tracks by our sociopathic masters.

After all, there's nothing quite like exposing an exchange of cold, hard cash from one greedy fist to another to focus one's attention on the business at hand.

And when that dirty business is the subversion of the American people's right to privacy, there's also nothing quite like economic self-interest for ensuring that a cone of silence descends over matters best left to the experts; a veritable army of specialists squeezing singular advantage out of any circumstance, regardless of how dire the implications for our democracy.

In light of this recommendation researcher Christopher Soghoian, deploying the tools of statistical analysis and a keen sense of outrage, reaffirmed that "Internet service providers and telecommunications companies play a significant, yet little known role in law enforcement and intelligence gathering."

That the American people have been kept in the dark when it comes to this and other affairs of state, remain among the most closely-guarded open secrets of what has euphemistically been called the "NSA spying scandal."

And when the Electronic Frontier Foundation (EFF) posted thousands of pages of documents "detailing behind-the-scenes negotiations between government agencies and Congress about providing immunity for telecoms involved in illegal government surveillance" last month, they lifted the lid on what should be a major scandal, not that corporate media paid the least attention.

A lid that Obama's "change" regime hopes to slam back down as expeditiously as possible.

Hoping to forestall public suspicions of how things actually work in Washington, the administration has declared that "it will continue to block the release of additional documents, including communications within the Executive Branch and records reflecting the identities of telecoms involved in lobbying for immunity," according to EFF's Senior Staff Attorney Kurt Opsahl.

No small matter, considering that should a court ever find avaricious telecoms and ISPs liable for violating the rights of their customers, fines could mount into the billions. Even in today's climate of corporate bailouts and "too big to fail" cash gifts to executive suite fraudsters, damages, both in monetary terms and adverse publicity, would hardly be chump change.

Hence, last year's mad scramble for the retroactive immunity avidly sought by these grifters and granted by congressional con men on both sides of the aisle when they passed the despicable FISA Amendments Act, hastily signed into law by our former "war president."

Without belaboring the point that corporate media largely failed to expose the extent of the dirty deals struck amongst these scofflaws, Soghoian, a graduate student no less, stepped into the breech and filled some necessary gaps in the surveillance story.

Believing, naïvely perhaps, that numbers don't lie and that laying out the facts might just wake us from our deadly slumber, Soghoian writes: "If you were to believe the public surveillance statistics, you might come away with the idea that government surveillance is exceedingly rare in the United States."

Indeed, "the vast majority of … [court] intercept orders are for phone wiretaps. Thus, for example, of the 1891 intercept orders granted in 2008, all but 134 of them were issued for phone taps."

Which begs the question: "How often are Internet communications being monitored, and what kind of orders are required in order to do so."

Unsurprisingly, the threshold for obtaining personal records is exceedingly low and "very few of these methods require an intercept order."

All the government need do to obtain a pen register or trap and trace order, which examine to/from/subject lines of email messages, URLs of viewed web pages, search terms, telephone numbers dialed and the like, is to unilaterally declare that information obtained via this backdoor route is "relevant" to an ongoing criminal or counterterrorist investigation.

In other words, give us everything we want and move along!

The nation's telecoms and ISPs have been very accommodating in this regard. And, as with other recent historical examples that come to mind such as the rush by U.S. firms to "rebuild" Iraq, Afghanistan and other benighted nations "liberated" by that "shining city upon a hill" that bombs, maims and generally does what it pleases because it can, servicing the secret state's limitless appetite for "actionable intelligence" has proven to be a very lucrative cash cow indeed.

Open a Can of Worms and Blood-Sucking Night Crawlers Slither Out

Deciding to "follow the money," Soghoian hoped "to determine how often Internet firms were disclosing their customers' private information to the government." As often as possible as it turns out. Describing the nexus between Sprint Nextel and the secret state, Soghoian discloses:

> Sprint Nextel provided law enforcement agencies with its customers' (GPS) location information over 8 million times between September 2008 and

> October 2009. This massive disclosure of sensitive customer information was made possible due to the roll-out by Sprint of a new, special web portal for law enforcement officers.
>
> The evidence documenting this surveillance program comes in the form of an audio recording of Sprint's Manager of Electronic Surveillance, who described it during a panel discussion at a wiretapping and interception industry conference, held in Washington DC in October of 2009.
>
> It is unclear if Federal law enforcement agencies' extensive collection of geolocation data should have been disclosed to Congress pursuant to a 1999 law that requires the publication of certain surveillance statistics–since the Department of Justice simply ignores the law, and has not provided the legally mandated reports to Congress since 2004. (Christopher Soghoian, "8 Million Reasons for Real Surveillance Oversight," Slight Paranoia, December 1, 2009)

A web portal I might add, equipped with a built-in price list ready-made for charging securocrats who spy on our blog posts, emails, web searches, mobile phone pings; indeed, any data the government might deem worthy of an "investigation." Call it a PayPal for spooks; now how's that for convenience!

How did Soghoian dig up the facts on the firm's lucrative arrangement with the government? In October, he attended the ISS World 2009 conference, Intelligence Support Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering (ISS), described by Wired as "a surveillance industry gathering for law enforcement and intelligence agencies and the companies that provide them with the technologies and capabilities to conduct surveillance."

Closed to the media and the public, the enterprising researcher obtained entry as a graduate student and recorded several sessions, since taken down at the insistence of ISS's corporate master TeleStrategies, who hosted the conference.

Describing itself as "the leading producer of telecommunications conference events in the United States," the firm claimed that Soghoian's recordings "violated copyright law." But not having deep pockets to weather a Digital Millennium Copyright Act (DMCA) takedown fight, he removed the files from his blog.

Inquiring minds can't help but wonder what was so threatening to the corporatist apple cart that they threatened to bring their thumb down, on a student no less? Let's take a look!

Among the sponsors of this year's ISS confab, one finds the usual low-key suspects manning the exhibits, hawking their wares and delivering learned presentations to their "partners" in the intelligence and security "community."

Leading the pack is ETI Group, self-described as "a leading management consulting firm specializing in Process Management and Improvement." As a "leading provider" of so-called "lawful interception solutions" for security agencies, telecoms and ISPs, ETI Group provide "future proof and scalable platforms" for the acquisition of information from "multiple sources."

NICE Systems, another "leading provider" of what it calls "Insight from Interactions solutions" derived from the "the convergence of advanced analytics of unstructured

multimedia content and transactional data–from telephony, web, email, radio, video and other data sources." Partners in the "Security Sector" include, among others, Raytheon, Honeywell, Siemens, Lockheed Martin, HP, Tyco and Motorola, all of whom are heavy-hitters in the Military-Industrial-Intelligence Complex and niche players in the burgeoning electronic surveillance industry in their own right.

Next up is SAP, a firm whose Government Support & Services division provide "a comprehensive range" of "enterprise software applications" to "help the analysts of the Intelligence Community" obtain "timely, accurate, objective and relevant intelligence." One can only wonder whether Doug Feith's shop over at the Pentagon deployed SAP "solutions" to find Saddam's "weapons of mass destruction" during the run-up to the Iraq invasion!

Taking their turn on the dais is Spectronic Systems, a Danish firm that is "100% privately owned." Little however, could be gleaned from a perusal of their web site since the company kindly informs us that it "is strictly for the benefit of Government Agencies, Law Enforcement Agencies, Intelligence Agencies and Government Approved companies." However, ISS World was good enough to disclose that Spectronic activities include "the development and manufacturing of monitoring systems and monitoring centres" for telephone, internet, fax and modem traffic. Their systems are designed to "handle–i.e. retrieve, collect, decode, store and present–bulk data," that can double as "data retention systems" for "bulk monitoring of SMS, MMS, e-mails or other means of data communication." But how beneficial is it to the bottom line? Alas, a diligent search of the business press by this writer hit a veritable blank wall.

SS8 on the other hand is more forthcoming, claiming that their "products" allow intelligence agencies to "visualize and analyze a target's internet session" and to "recognize, monitor, investigate and prevent criminal activity." Proud that they have a "global reach," SS8 broadcasts that their "electronic surveillance solutions" are "deployed in over 25 countries" and that their data installations "can intercept more than 100 million subscribers." The firm's platform for internet, WiFi, broadband and satellite interception claims to be capable of ferreting out "hidden relationships" while identifying "trends" (code for data mining and social network analysis) that "meet the functional needs" of the secret state.

Telesoft Technologies, produce "monitoring probes" that "allow data extraction" from "cellular and fixed networks." This can be done for "fixed, 2/3G mobile and packet networks." According to the firm, their "universal passive probes extract call content, signalling [sic] and location information for use by monitoring applications," ensuring a seamless connection" of applications to "real world systems."

True Position; this firm's national security brief involves the identification and tracking of any mobile device in "real time" and offer "insightful intelligence" while "delivering powerful solutions" that "enable private enterprises and government agencies" the capability "to protect people, combat crime, and save lives like never before." According to the company's web site, the firm deploys data mining technologies that "monitor activity and behavior over time in order to build detailed profiles and identify others that they associate with."

Last, but certainly not least, is the ultra-spooky Israeli firm, Verint (formerly Comverse Infosys). Billing itself as the world leader in "actionable intelligence," readers are well-advised to peruse the documents on Verint products such as Reliant and Star Gate generously posted by our good friends over at the whistleblowing web site Quintessenz. And while your at it, why not check out AFC's piece, "Thick as Thieves: The Private (and very

profitable) World of Corporate Spying," where information on the shady activities of the firm's founder, Kobi Alexander, can be found. Currently holed-up in Windhoek, Namibia after becoming the recipient of a 2006 thirty-two count indictment by the Justice Department that charged the ex-Israeli intelligence officer and entrepreneur with backdating millions of stock options worth $138 million, Alexander is a sterling representative of an industry dedicated to "lawful interception" of our electronic communications to "prevent criminal activity."

Amongst the exhibitors at ISS World, one finds (yet another) spooky Israeli firm Narus, whose hardware was a permanent "guest" in ATT/NSA "secret rooms" scattered around the country for surveillance of the entire Internet. First disclosed by ATT whistleblower Mark Klein in his sworn affidavit on behalf of EFF's lawsuit, Hepting v. ATT, the firm's STA 6400 traffic analyzer can monitor traffic equal to 39,000 DSL lines at 10 Gbit/s, or in practical terms, a single Narus machine can surveil several million broadband users at any given time. In 2004, the former Deputy Director of NSA, William Crowell joined the firm's board of directors. As a result of FAA's retroactive immunity provision, *Hepting v. ATT* was dismissed in 2009.

Which brings us full-circle to Sprint Nextel's spiffy new web portal that enables the secret state to "ping" their customers' GPS locations eight million times in the space of a year.

Tip of the Proverbial Iceberg

Hoping to learn more, Soghoian filed multiple Freedom of Information Act (FOIA) requests with the Department of Justice, seeking relevant details on just how much these corporate grifters charge our silent guardians for their electronic spying.

It was at that point that Soghoian ran into a brick wall. When he uncovered evidence that the illicit surveillance compact amongst federal security agencies, telecoms and ISPs was a limitless gold mine enriching shareholders at the expense of our constitutional rights, the firms struck back.

"Verizon and Yahoo intervened and filed an objection on grounds that, among other things, they would be ridiculed and publicly shamed were their surveillance price sheets made public," Wired reported December 1.

What do these firms have to hide? Apparently, quite a lot.

Yahoo and Verizon weren't about to release the data and filed a 12-page objection letter with the Justice Department, claiming that if their pricing information were disclosed to Soghoian he would use it for nefarious ends "to 'shame' Yahoo and other companies–and to 'shock' their customers."

Cryptome Delivers the Goods, Again

Despite their whining, the indefatigable John Young, webmaster of the intelligence and security whistleblowing web site Cryptome, has published the Yahoo! Compliance Guide for Law Enforcement.

The 17-page handy guide for spooks and cops provides information on what the firm can and will provide the secret state (everything) and what it will cost.

Cryptome, never a site to run from a fight, has also posted the compliance guides of AT&T,

Verizon, Sprint, Voicestream, Cox, Cingular, SBC, and Pacific Telesis.

As Antifascist Calling has averred many times, since the business of America's security is, after all, business, let's just say the "service" Yahoo provides our nation's spooks doesn't come cheap.

For his sterling efforts to inform the public, Young has been threatened by Yahoo attorneys with the tony Washington law firm Steptoe & Johnson.

In a series of communications with Young, Yahoo's lawyers are threatening legal action in the form of a Digital Millennium Copyright Act (DMCA) takedown notice, claiming that "the unauthorized use and distribution of this document … infringes Yahoo's intellectual property rights and constitutes a violation of U.S. copyright law."

Attorney Michael T. Gershberg's tersely worded missive, alleges that the posted spy guide "also infringes Yahoo's trade secrets and constitutes business interference."

Young fired back December 2: "The Yahoo document hosted on Cryptome was found on the Internet at a publicly accessible site.

"There is no copyright notice on the document. Would you please provide substantiation that the document is copyrighted or otherwise protected by DMCA? Your letter does not provide more than assertion without evidence."

Gershberg countered: "On behalf of our client, Yahoo! Inc., attached please find a notice of copyright infringement pursuant to Section 512 of the Digital Millennium Copyright Act. Thank you for your cooperation in this matter."

Undeterred, Young shot back: "I cannot find at the Copyright Office a grant of copyright for the Yahoo spying document hosted on Cryptome. To assure readers Yahoo's copyright claim is valid and not another hoary bluff without substantiation so common under DMCA bombast please send a copy of the copyright grant for publication on Cryptome."

Continuing, Young wrote: "Until Yahoo provides proof of copyright, the document will remain available to the public for it provides information that is in the public interest about Yahoo's contradictory privacy policy and should remain a topic of public debate on ISP unacknowledged spying complicity with officials for lucrative fees."

According to Cryptome, "The information in the document which counters Yahoo's customer privacy policy suggests a clearing of the air is in order to assure customer reliance on Yahoo's published promises of trust. A rewrite of Yahoo's spying guide to replace the villainous one would be a positive step, advice of an unpaid, non-lawyerly independent panel could be sought to avoid the stigma associated with DMCA coercion.

"Note: Yahoo's exclamation point is surely trademarked so omitted here."

Commenting on the spy guide, Wired reported,

> The Compliance Guide reveals, for example, that Yahoo does not retain a copy of e-mails that an account holder sends unless that customer sets up the account to store those e-mails. Yahoo also cannot search for or produce deleted e-mails once they've been removed from a user's trash file.

> The guide also reveals that the company retains the IP addresses from which a user logs in for just one year. But the company's logs of IP addresses used to register new accounts for the first time go back to 1999. The contents of accounts on Flickr, which Yahoo also owns, are purged as soon as a user deactivates the account.
>
> Chats conducted through the company's Web Messenger service may be saved on Yahoo's server if one of the parties in the correspondence set up their account to archive chats. This pertains to the web-based version of the chat service, however. Yahoo does not have the content of chats for consumers who use the downloadable Web Messenger client on their computer.
>
> Instant message logs are retained 45 to 60 days and includes an account holder's friends list, and the date and times the user communicated with them. (Kim Zetter, "Yahoo Issues Takedown Notice for Spying Price List," Wired, December 4, 2009)

Well, just how much *does* Yahoo charge for their dubious shenanigans with the secret state? Wired reports: "According to this list, Yahoo charges the government about $30 to $40 for the contents, including e-mail, of a subscriber's account. It charges $40 to $80 for the contents of a Yahoo group."

Do the math for millions of customers whose rights have been abused and violated and pretty soon we're talking serious money!

Is this what Yahoo and Verizon mean when they claim that should their surveillance price lists be publicly disclosed to they would be used "to 'shame' Yahoo! and other companies–and to 'shock' their customers."

"Therefore," the company avers, "release of Yahoo's information is reasonably likely to lead to impairment of its reputation for protection of user privacy and security, which is a competitive disadvantage for technology companies."

Well guess what, guilty as charged! Now that the information has been widely posted and mirrored by the global whistleblowers Wikileaks and countless other web sites, we should consider the alarming implications of Christopher Soghoian's essential research to our privacy and democratic rights and act accordingly.

Barring a mechanism that guarantees public accountability from the secret state and their grifting corporate partners, we are left with no alternative but to name and shame. After all, democracy is *not* a spectator sport!

Articles by: **Tom Burghardt**

http://antifascist-calling.blogspot.com/