GlobalResearch
Center for Research on Globalization

# Multibillion "Homeland Security" Market: Telecoms Assist in NSA Spy Operations

By Tom Burghardt
Global Research, September 11, 2008
Antifascist Calling... 11 September 2008
Theme: Intelligence, Police State & Civil Rights

What do the NSA's warrantless wiretapping program and enterprising capitalist grifters have in common? Workarounds...and lots of them. The kind that aren't covered by *any* law.

Two highly-disturbing reports by **CNET** and the ***London Review of Books*** describe how government intelligence agencies and niche telecom providers have teamed-up to subvert our privacy rights–while providing security agencies with real-time cell phone tracking capabilities.

The stuff of paranoid delusions? Hardly.

According to *London Review of Books* editor Daniel Soar, to the Intelligence Support Systems Industry (ISS), "which sells analysis tools to government agencies, police forces and–increasingly–the phone companies themselves," the least interesting thing about your call may be what you say. Soar writes,

> At a very rough estimate half a trillion calls are made each day on the world's mobile networks: their origin and destination, their time and duration and all identifying codes are logged on telecom provider hard-drives and generally retained, under emerging legislation, for up to two years. It's impossible to exaggerate the value of these data. ... At the frequent ISS conferences–Dubai, Qatar, Washington, Prague–one of the key topics of discussion tends to be how to identify targets for LI (that's 'lawful intercept') in the first place: it's a cinch to bug someone, but how do you help a law enforcement agency decide who to bug? ("Daniel Soar Considers Mobile Surveillance," London Review of Books, 14 August 2008)

And with a swarming multitude of new companies crawling out of the woodwork to "service" the "homeland security" market, why its a snap. Firms such as **ThorpeGlen**, **VASTech**, **Kommlabs**, and **Aqsacom** all sell what CNET's Chris Soghoian describes as "off-the-shelf data-mining solutions to government spies interested in analyzing mobile-phone calling records and real-time location information."

Called "passive-probing" data mining, these companies are carving-out lucrative niche markets. Only there's nothing "passive" about these intrusive operations undertaken in concert with a veritable army of state and corporate spooks.

According to Soghoian, while firms such as AT&T, Verizon and Sprint directly collaborated with NSA on the agency's driftnet-style surveillance programs, legal experts are now suggesting that the public-private partnership in illegal spying may run far deeper into the

wireless phone industry than anyone suspects.

> With over 3,000 wireless companies operating in the United States, the majority of industry-aided snooping likely occurs under the radar, with the dirty-work being handled by companies that most consumers have never heard of. (Chris Soghoian, "Exclusive: Widespread Cell Phone Location Snooping by NSA?", CNET, September 8, 2008)

Indeed, a "**Webinar**" hosted by the UK's ThorpeGlen in May, demonstrated that company's tools by "mining a dataset of a single week's worth of call data from 50 million users in Indonesia, which it has crunched in order to try and discover small anti-social groups that only call each other," Soghoian reports.

In the case of the Indonesian analysis presented in ThorpeGlen's "Webinar," the *London Review of Books* reported that the VP of sales and marketing told prospective clients,

> Everyone on a network ... is part of a group; most groups talk to other groups, creating a spider's web of interactions. Of the 50 million subscribers ThorpeGlen processed, 48 million effectively belonged to 'one large group': they called one another, or their friends called friends of their friends; this set of people was dismissed. A further 400,000 subscriptions could be attributed to a few large 'nodes', with numbers belonging to call centres, shops and information services. The remaining groups ranged in size from two to 142 subscribers. Members of these groups only ever called each other–clear evidence of antisocial behaviour–and, in one extreme case, a group was identified in which all the subscribers only ever called a single number at the centre of the web. This section of the ThorpeGlen presentation ended with one word: 'WHY??' (LRB, op. cit.)

The question arises: Is the NSA deploying similar technologies in the United States to spy on citizens doing no more than exercising their constitutional rights to protest state policies? If the swift preemptive raids by St. Paul police and the FBI during last week's Republican National Convention are any indication, the answer inevitably is *yes*.

In other words, were the pin-point raids on homes shared by protest organizers and media workers such as **I-Witness Video** and the **Glass Bead Collective** simply the result of blind luck or human intelligence gathered by paid provocateurs? If report's emerging on real-time cell phone tracking are any indication of the state's desire to quash dissent–and those who document their repressive behavior, journalists–then the answer is a resounding *no*.

How then, would the NSA gather this information? Soghoian reports,

> The massive collection of customer data comes down to the interplay of two specific issues: First, thousands of companies play small, niche support roles in the wireless phone industry, and as such these firms learn quite a bit about the calling habits of millions of U.S. citizens. Second, the laws relating to information sharing and wiretapping **specifically regulate companies that provide services to the general public (such as AT&T and Verizon), but they do not cover the firms that provide services to the major carriers or connect communications companies to one other.** [emphasis added]

That's right. While it might be illegal for the NSA to obtain real-time customer location

information from any of the giant telecoms, Bushist spooks can simply go to the companies that *own and operate the wireless towers that the telecoms use for their networks* "and get accurate information on anyone using those towers–or go to other entities connecting the wireless network to the landline network. The wiretapping laws, at least in this situation, simply don't apply," Soghoian writes.

Since networks "are more and more disaggregated and outsourced," a single call is handled "by many more parties than the named provider today," according to Albert Gidari, a lawyer at Perkins Cole in Seattle "who frequently represents the wireless industry in issues related to location information and data privacy."

Such legal loopholes are in fact so massive that a fleet of tanker trucks could be driven right through them!

And since Sprint, AT&T or Verizon don't actually own their own cellular towers, TowerCo, the company that does, "learns some information on every mobile phone that communicates with one of its towers." But it gets worse, much worse. According to Soghoian, this is the tip of the proverbial iceberg.

> There are companies that provide "backhaul" connections between towers and the carriers, providers of sophisticated billing services, outsourced customer-service centers, as well as Interexchange Carriers, which help to route calls from one phone company to another. All of these companies play a role in the wireless industry, have access to significant amounts of sensitive customer information, which of course, can be obtained (politely, or with a court order) by the government.

As we know, perverse laws such as the USA Patriot Act and the FISA Amendments Act, not to mention FBI National Security Letters come with ready-made gag orders attached that forbid companies–or anyone else so served–from disclosing any information to the public or those whom the state is spying upon. Gidari told CNET,

"So any entity–from tower provider, to a third-party spam filter, to WAP gateway operator to billing to call center customer service–can get legal process and be compelled to assist in silence. They likely don't volunteer because of reputation and contractual obligations, but they won't resist either."

Short of a whistleblower like **Mark Klein** or **Babak Pasdar** spilling the beans, the existence of these programs will likely remain a closely-guarded state secret. Why? Paul Ohm, a cyberlaw professor at the University of Colorado Law School and former federal prosecutor told CNET,

> "Whether [a] vendor to a carrier to the public cooperates with agencies (either for a fee or by acquiescence in an order), is something you will not find out as FISA makes it so, regardless of whether the person is in the U.S. or communicating with a person abroad. Such means and methods largely are hidden."

And there you have it. Niche telecom providers are the latest players in the West's burgeoning "terrorism industry," one that "keeps us safe" by destroying our privacy and our rights with hefty profits all around. Call it another seamless victory for the market's

"invisible hand" that clenches as it morphs into the state's iron fist wrapped in American flags and blood-drenched corporate logos.

**Note**: Since *Antifascist Calling* **published** "New Spy Software Coming on-Line: 'Surveillance in a Box' Makes its Debut," last month, we've received an intriguing package from the good folks at **Quintessenz**, "IT and telco surveillance equipment–data sheets and presentations."

Described as, "A collection of network monitoring and datamining suites made by Nokia Siemens, Ericsson, Verint and others. All systems are compliant to ETSI and CALEA 'lawful interception' standards, the vendors themselves are involved in the standardization. While the official name of the game is still 'lawful interception' the newer suites also perform 'high speed government surveillance'. From Iran to China they are ab/used to track down the democratic opposition, dissidents, ethnic and religious minorities. The vendors are mostly European and US companies."

The power-point presentations and accompanying documentation are definitely worth a look and are highly recommended! **Check out**, "The making of the European Surveillance Union, 1993-2001," a real eye-opener!

*Tom Burghardt is a researcher and activist based in the San Francisco Bay Area. In addition to publishing in Covert Action Quarterly, Love & Rage and Antifa Forum, he is the editor of Police State America: U.S. Military "Civil Disturbance" Planning, distributed by* ***AK Press****.*



---



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