GlobalResearch
Center for Research on Globalization

The Development of "Privacy Killing Technologies": A Link to the Murdoch Scandal?

Black Ops for Major U.S. Banks and Corporations

By Tom Burghardt
Global Research, July 25, 2011
Antifascist Calling 25 July 2011

Region: USA
Theme: Intelligence, Police State & Civil Rights

Following revelations earlier this year by *The Tech Herald* that security firms with close ties to the Pentagon ran black ops for major U.S. banks and corporations, it became clear that proprietary software developed for the military and U.S. intelligence was being used to target Americans.

Those firms, including now-defunct HBGary Federal, parent company HBGary, Palantir (a start-up flush with cash from the CIA's venture capital arm In-Q-Tel) and Berico Technologies had partnered-up with the Bank of America's law firm Hunton & Williams and the U.S. Chamber of Commerce and devised a sub rosa plan of attack against WikiLeaks and Chamber critics.

And when the cyber-guerrilla collective Anonymous published some 70,000 emails and documents filched from HBGary servers, it was off to the races.

In the intervening months since that story first broke, journalists and researchers have turned their attention to a dark web of security firms developing surveillance software for law enforcement, the Pentagon, and repressive foreign governments.

Last week, *Wired* revealed that one such firm, TruePosition, "a holding of the Liberty Media giant that owns Sirius XM and the Atlanta Braves," is marketing "something it calls 'location intelligence,' or LOCINT, to intelligence and law enforcement agencies," investigative journalist Spencer Ackerman disclosed.

The Pennsylvania-based company has sold their location services system to NSA surveillance partner AT&T and T-Mobile, allowing those carriers to pinpoint "over 60 million 911 calls annually."

"For the better part of decade," Ackerman writes, "TruePosition has had contracts to provide E-911 services with AT&T (signed originally with Cingular in 2001, which AT&T acquired) and T-Mobile (2003)."

Known as "geofencing," the firm explains that location tech "collects, analyzes, stores and displays real-time and historical wireless events and locations of targeted mobile users."

Bloomberg BusinessWeek reported that amongst the services TruePosition offers clients are "products for safety and security applications, including family monitoring, personal medical alert, emergency number service, and criminal tracking."

Additionally, *BusinessWeek* reports, the company tailors its "enterprise applications" to corporations interested in "workforce management, asset tracking, and location-based advertising; consumer applications, including local search, traffic, and navigation."

But what should concern readers is the firm's "government applications" market which includes everything from "homeland security" and "military intelligence" to "force tracking."

According to a press release posted on the firm's web site, the "TruePosition Location Intelligence Management System (LIMS)" is a "a multi-dimensional database, which uses probes within mobile networks to capture and store all mobile phone network events–including the time and the location of events. Mobile phone events are items like calls made and received, text messages sent and received, a phone powered on and off, and other rich mobile phone intelligence."

Deploying technology dubbed Uplink Time Difference of Arrival (U-TDOA), the system, installed on cell phone towers, identifies a phone's approximate location–within 30 meters–even if the handset isn't equipped with GPS.

Undoubtedly the system *can* save lives. "In one case," Ackerman reports, "a corrections officer … was abducted by a recent parolee. But because her cellphone was turned on and her carrier used TruePosition's location tech, police were able to locate the phone along a Kentucky highway. They set up a roadblock, freed the officer and arrested her captor."

All well and good. However, in the hands of repressive governments or privacy-invading corporations, say Rupert Murdoch's media empire, there just might be far different outcomes.

A Link to the Murdoch Scandal?

The relevance of location intelligence in general and more pointedly, TruePosition's LIMS cellphone surveillance products which may, or may not, have been sold to London's Metropolitan Police and what role they may have played in the Murdoch *News of the World* (NoW) phone hacking scandal have not been explored by corporate media.

While the "who, what, where" aspects of the scandal are now coming sharply into focus, the "how," that is, the high-tech wizardry behind invasive privacy breaches, and which firms developed and profited from their sale, have been ignored.

Such questions, and related business entanglements, should be of interest to investigators on both sides of the Atlantic.

After all, TruePosition's parent company, the giant conglomerate Liberty Media currently holds an 18 percent stake in News Corporation.

With corporate tentacles stretching from investments in TimeWarner Cable to Expedia and from QVC to Starz and beyond, Liberty Media is a multi-billion dollar media behemoth with some $10.9 billion in revenue in 2010, according to an SEC filing by the firm.

With deep pockets and political clout in Washington the company is "juiced."

In 2011, Liberty's CEO, John C. Malone, surpassed Ted Turner as the largest private landowner in the United States, controlling some 2.1 million acres according to *The New*

York Times.

Dubbed "Darth Vader" by *The Independent*, Malone acquired a 20 percent stake in News Corp. back in 2000 and "was one of the main investors who rode to the rescue of Mr Murdoch in the early 1990s when News Corp was on its knees."

The New York Times reported back in 2005 that Malone's firm was "unlikely to unwind its investment in the News Corporation" because he considered "the stake in the News Corporation a long-term investment, meaning that the relationship between him and Rupert Murdoch, the chairman of the News Corporation, was not likely to be dissolved any time soon."

After acrimonious mid-decade negotiations that stretched out over two years, the media giants cobbled together a deal in 2006 resulting in a $11 billion asset swap, one that gave Liberty control of the DirectTV Group whilst helping Murdoch "tighten his grip" on News Corp., according to *The New York Times*.

Interestingly enough during those negotiations, investment banking firms Goldman Sachs and J.P. Morgan Chase along with the white shoe law firm Hogan & Hartson advised News Corp., while Liberty was represented by Bear Stearns and the Baker Botts law firm, long time Bush family consiglieres.

All this can be chalked-up to an interesting set of coincidences. However, the high stakes involved and the relationships and connections forged over decades, including those amongst players who figured prominently in capitalism's 2008 global economic crisis and Bush family corruption, cannot be ignored.

A Suspicious Death

Last week's suspicious death of former NoW whistleblower Sean Hoare should set alarm bells ringing.

When the scandal broke, it was Hoare who told *The New York Times* last year that senior editors at NoW and another Murdoch tabloid, *The Sun*, actively encouraged staff to spy on celebrities and others, including victims of the London terror attacks, British soldiers killed in Afghanistan and Iraq and the murdered teenager Milly Dowler; all in pursuit of "exclusives."

The Guardian reported that Hoare said that "reporters at the NoW were able to use police technology to locate people using their mobile phone signals, in exchange for payments to police officers."

"He said journalists were able to use 'pinging', which measured the distance between a mobile handset and a number of phone masts to pinpoint its location," *The Guardian* revealed.

Hoare described "how reporters would ask a news desk executive to obtain the location of a target: "Within 15 to 30 minutes someone on the news desk would come back and say 'Right, that's where they are.'"

Quite naturally, this raises the question which "police technology" was used to massage NoW exclusives and which firms made a pretty penny selling their wares to police, allegedly

for purposes of “fighting crime” and “counterterrorism”?

It was Hoare after all who told *The New York Times* just days before his death that when he worked for NoW “pinging cost the paper nearly $500 on each occasion.”

According to the *Times*, Hoare found out how the practice worked “when he was scrambling to find someone and was told that one of the news desk editors, Greg Miskiw, could help.”

The *Times* reports that Miskiw “asked for the person’s cellphone number, and returned later with information showing the person’s precise location in Scotland.”

An unnamed “former Scotland Yard officer” interviewed by the *Times* said “the individual” who provided confidential information to NoW and other Murdoch holdings “could have been one of a small group entitled to authorize pinging requests,” that is a senior counterterrorism officer charged with keeping the British public “safe.”

Hoare told the *Times* “the fact that it was a police officer was clear from his exchange with Mr. Miskiw.”

“‘I thought it was remarkable and asked him how he did it, and he said, ‘It’s the Old Bill, isn’t it?'”

“At that point, you don’t ask questions,” Hoare said.

Yet despite the relevance of the reporter’s death to the scandal, police claimed Hoare’s sudden demise was “unexplained but not thought to be suspicious.” Really?

As the *World Socialist Web Site* points out: “The statement is at the very least extraordinary, and at worst sinister in its implications.”

Left-wing journalist Chris Marsden wrote that “Hoare is the man who broke silence on the corrupt practices at the *News of the World* and, most specifically, alleged that former editor Andy Coulson, who later became Prime Minister David Cameron’s director of communications, was fully aware of phone hacking that took place on an ‘industrial scale’.”

Aside from the secret state, what other entities are capable of intercepting phone and other electronic communications on “an industrial scale”? Given Rupert Murdoch’s close ties to the political establishment on both sides of the Atlantic, is it a stretch to speculate that a “sympathetic” intelligence service wouldn’t do all they could to help a “friend,” particularly if cash payments were involved?

How could Hoare’s death *not* be viewed suspiciously?

Indeed, “the morning after Hoare’s body was found,” Mardsen writes, “former Metropolitan Police Commissioner Sir Paul Stephenson and his former deputy, John Yates, were to give evidence before a home affairs select committee. Stephenson had tendered his resignation Sunday and Yates Monday.”

Conveniently, for those with much to hide, including police, “the death of Hoare means that his testimony will never be heard by any such inquiry or, more importantly, by any criminal investigation that may arise.”

Yet, despite a pending coroner's inquest into the exact cause of the reporter's death, corporate media have rushed to judgement, labeling anyone who raise suspicions as being, what else, "conspiracy theorists."

This despite the fact, as the *World Socialist Web Site* reported Saturday that information has surfaced "regarding the extent of News International links to known criminals."

Indeed, on July 6 left-wing journalist Robert Stevens reported that "Labour MP Tom Watson told Parliament that News International chief executive and former *News of the World* editor Rebekah Brooks 'was present at a meeting with Scotland Yard when police officers pursuing a murder investigation provided her with evidence that her newspaper was interfering with the pursuit of justice'."

"'She was told of actions by people she paid to expose and discredit David Cook [a Detective Superintendent] and his wife Jackie Haines so that Mr. Cook would be prevented from completing an investigation into a murder'.

"Watson added," Stevens writes, that "'News International was paying people to interfere with police officers and were doing so on behalf of known criminals. We know now that News International had entered the criminal underworld'."

Although Hoare had suffered from years of alcohol and cocaine abuse, he was in rehab and by all accounts on the road to recovery. Hoare *could* have died from natural causes but this has not yet been established.

Pending histology and toxicology tests which will take weeks, and a coroner's inquest was adjourned July 21 until said test results were in, short of a definitive finding, nothing can nor should be ruled out, including murder, by a party or parties unknown.

While it would be a fatal exercise in rank stupidity for News Corp. to rub out Sean Hoare, would others, including police or organized crime figures caught up in the scandal and known to have been paid by News Corp. "people to interfere with police officers" and to have done so "on behalf of known criminals," have such qualms?

An Open Question

We do not know if TruePosition sold LIMS to London's Metropolitan Police, key players in the Murdoch hacking scandal, and the firm won't say who they sell to.

However, whether they did or did not is a relevant question. That security firms develop and sell privacy-killing products and then wash their hands of responsibility *how* and by *whom* their products are used–for good or ill–is hardly irrelevant to victims of police repression or private corruption by entities such as News Corp.

The issue here are the actions taken by our corporate and political minders who believe that everything in terms of smashing down walls between public and private life is up for grabs, a commodity auctioned off to the highest bidder.

While we are told by high-tech firms out to feather their nests and politicians that "law enforcement" require we turn over all our data to police to "keep us safe," the Murdoch scandal reveals *precisely* that it was police agencies corrupted by giant corporations which had allowed such criminal behavior to go unchecked for years.

And with Congress and Obama Justice Department officials pursuing legislation that will require mobile carriers to store and disclose cell-tower data to police and secret state agencies–all without benefit of a warrant, mind you–as well as encryption back doors built into the internet, we are reaching a point where a perfect storm threatens privacy well into the future, if not *permanently*.

A Looming Threat

Since LIMS 2008 introduction some 75,000 mobile towers in the U.S. have been equipped with the system, *FoxNews*, ironically enough, reported two years ago.

That same report informed us that "LOCINT continues to operate in Middle Eastern and Asia-Pacific nations where no legal restrictions exist for tracking cell phone signals."

TruePosition's marketing vice president Dominic Li told *Fox* "when you establish a geofence, anytime a mobile device enters the territory, our system will be alerted and provide a message to the customer."

Li went on to say, "we realize that this has a lot of value to law enforcement agencies outside of search and rescue missions. It gives rise to a whole host of new solutions for national security."

In keeping with the firm's penchant for secrecy, risk averse when it comes to negative publicity over the civil liberties' implications of their products, "citing security concerns," *Fox* reported that "company officials declined to specify which countries currently use the technology."

TruePosition claims that while wireless technology "has revolutionized communication" it has a "dark side" as "terrorists and criminals" exploit vulnerabilities to create "serious new threats to the security of nations worldwide."

Touting their ability to combine "location determination and network data mining technologies," TruePosition "offers government agencies, security experts and law enforcement officials powerful, carrier-grade security solutions with the power to defend against criminal and terrorist activity."

Never mind that most of the "serious new threats" to global citizens' rights come from unaccountable state security agencies and international financial cartels responsible for the greatest theft of resources in human history.

For interested parties such as TruePosition, "actionable intelligence" in the form of "data mining to monitor activity and behavior over time in order to build detailed profiles and identify others that they associate with," will somehow, magically one might say, lead to the apprehension of "those who threaten the safety of citizens."

Unasked is the question: who will protect *us* from those who develop and sell such privacy killing technologies?

Certainly not Congress which has introduced legislation "that would force Internet companies to log data about their customers," *CNET News* reported earlier this month.

"As a homeland security tool," *Wired* reported, LIMS is "enticing." Brian Varano,

TruePosition's marketing director told Spencer Ackerman to "imagine an 'invisible barrier around sensitive sites like critical infrastructure,' such as oil refineries or power plants."

"The barrier contains a list of known phones belonging to people who work there, allowing them to pass freely through the covered radius. 'If any phone enters that is not on the authorized list, [authorities] are immediately notified,'" Varano told *Wired*.

While TruePosition's technology may be useful when it comes to protecting nuclear installations and other critical infrastructure from unauthorized breaches and may be an important tool for investigators tracking down drug gangs, human traffickers, kidnappers and stalkers, as we have learned from the Murdoch scandal and the illegal driftnet surveillance of Americans, the potential that governments and private entities will abuse such powerful tools is also likely.

According to *Wired* while "TruePosition sells to mobile carriers," the company is "cagey about whether the U.S. government uses its products." Abroad however, Ackerman writes, "it sells to governments, which it won't name. Ever since it came out with LOCINT in 2008," Varano said that "'Ministries of Defense and Interior from around the world began beating down our door'."

That technological "quick fixes" such as LOCINT can augment the power of secret state agencies to "easily identify and monitor networks of dissidents," doesn't seem to trouble the firm in the least.

In fact, such concerns don't even enter the equation. As *Wired* reported, the company "saw a growth market in a field" where such products would have extreme relevance: "the expanding, globalized field of homeland security."

"It really was recession-proof," Varano explained to Ackerman, "because in many parts of the world, the defense and security budgets have either maintained where they were or increased by a large percentage."

Small comfort to victims of globalized surveillance and repression that in many places, including so-called "Western democracies," are already an ubiquitous part of the political landscape.

Consider the ease with which police can deploy LIMS for monitoring dissidents, say anticapitalist activists, union leaders or citizen organizers fighting against the wholesale theft of publicly-owned infrastructure to well-connected corporations (Greece, Ireland or Spain for example) by governments knuckling-under to IMF/ECB demands for so-called "deficit reduction" schemes.

As Stephen Graham points out in his seminal book *Cities Under Siege*, "as the everyday spaces and systems of urban everyday life are colonized by militarized control technologies" and "notions of policing and war, domestic and foreign, peace and war become less distinct, there emerges a massive boom in a convergent industrial complex encompassing security, surveillance, military technology, prisons, corrections, and electronic entertainment."

> "It is no accident," Graham writes, "that security-industrial complexes blossom in parallel with the diffusion of market fundamentalist notions for organizing social, economic and political life."

Creating a climate of fear is key to those who seek to manage daily life. Thus the various media-driven panics surrounding nebulous, open-ended "wars" on "deficits," "drugs," "terror" and now "cyber-crime."

That firms such as TruePosition and hundreds of others who step in to capitalize on the highly-profitable "homeland security" market, hope to continue flying under the radar, we would do well to recall U.S. Supreme Court Justice Louis Brandeis who strongly admonished us that "sunlight is the best disinfectant."

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, he is a Contributing Editor with Cyrano's Journal Today. 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/