GlobalResearch
Center for Research on Globalization

The Orwellian Internet Surveillance Noose: No Privacy, No Place to Hide…

New Smartphone Spy Scandal Unwinds

By Tom Burghardt
Global Research, April 24, 2011
Antifascist Calling... 24 April 2011

Region: USA
Theme: Police State & Civil Rights

As the United States morphs into a failed state, one unwilling and soon perhaps, unable, to provide for the common good even as it hands over trillions of dollars to a gang of financial brigands engorged like parasitic ticks on the wealth of others, keeping the lid on is more than just an imperial obsession: it's big business.

Earlier this month, ***New Scientist*** reported that "a new way of working out where you are by looking at your internet connection could pin down your current location to within a few hundred metres."

Although similar techniques are already in use, they are not very accurate in terms of closing the surveillance trap. "Every computer connected to the web has an internet protocol (IP) address, but there is no simple way to map this to a physical location," reporter Jacob Aron informs us. "The current best system can be out by as much as 35 kilometres."

However, Yong Wang, "a computer scientist at the University of Electronic Science and Technology of China in Chengdu, and colleagues at Northwestern University in Evanston, Illinois, have used businesses and universities as landmarks to achieve much higher accuracy."

According to *New Scientist*, "Wang's team used Google Maps to find both the web and physical addresses of such organisations, providing them with around 76,000 landmarks. By comparison, most other geolocation methods only use a few hundred landmarks specifically set up for the purpose."

With geolocation tracking devices embedded in smartphones (and, as we'll see below, this data is stored without their users' consent), all of which is happily turned over to authorities by telecoms (for the right price, of course!), as privacy researcher Christopher Soghoian **revealed** in 2009, it becomes abundantly clear that sooner than most people think they'll be no escaping Big Brother's electronic dragnet.

"The new method," Aron writes, "zooms in through three stages to locate a target computer." First, the team of public-private financed research snoops measured "the time it takes to send a data packet to the target and converts it into a distance–a common geolocation technique that narrows the target's possible location to a radius of around 200 kilometres."

Wang and his cohorts then "send data packets to the known Google Maps landmark servers

in this large area to find which routers they pass through." *New Scientist* reports that when "a landmark machine and the target computer have shared a router, the researchers can compare how long a packet takes to reach each machine from the router; converted into an estimate of distance, this time difference narrows the search down further."

"We shrink the size of the area where the target potentially is," Wang cheerfully explained.

"Finally," Aron writes, "they repeat the landmark search at this more fine-grained level: comparing delay times once more, they establish which landmark server is closest to the target."

"On average," we're told, "their method gets to within 690 metres of the target and can be as close as 100 metres–good enough to identify the target computer's location to within a few streets."

While *New Scientist* focused their attention on how an IP address tracking tool might be a boon to advert pimps, who *else* might find the method "useful in certain situations"?

Tightening the Surveillance Noose

Back in December, ***The Wall Street Journal*** reported that "few devices know more personal details about people than the smartphones in their pockets: phone numbers, current location, often the owner's real name–even a unique ID number that can never be changed or turned off."

As part of the *Journal's* excellent **"What They Know"** series, reporters Scott Thurm and Yukari Iwatani Kane revealed that an examination of more than 100 smartphone apps for Apple's iPhone and Google's Android platforms "showed that 56 transmitted the phone's unique device ID to other companies without users' awareness or consent," 47 apps "transmitted the phone's location in some way," and "five sent age, gender and other personal details to outsiders."

Like the *New Scientist* report above, the *Journal* focused their investigative lens on "intrusive effort[s] by online-tracking companies to gather personal data about people in order to flesh out detailed dossiers on them."

Without a doubt, such data is already being collected by various police intelligence agencies at the local, state and federal levels.

In all likelihood, smartphone geolocation data has now been added to the dossier creation mix, another component of the secret state's massive national security index called "Main Core" by investigative journalists **Christopher Ketchum** and **Tim Shorrock**.

As Ketchum reported in his 2008 piece, three unnamed former intelligence officials told him that "8 million Americans are now listed in Main Core as potentially suspect" and, in the event of a national emergency, "could be subject to everything from heightened surveillance and tracking to direct questioning and even detention."

We've now learned that Apple's iPhone and iPad and Google's Android smartphone platforms "constantly track users' physical location and store the data in unencrypted files that can be read by anyone with physical access to the device," ***The Register*** disclosed.

And with technological advances far-outstripping legal remedies to protect Americans' privacy as Soghoian **wrote** last week, and with Congress and the Obama administration further lowering the boom, the notion that our personal communications are off-limits to advertisers and government officials is as quaint as the concept that financial institutions should be transparent when it comes to investing our hard-earned dollars.

According to researchers Pete Warden and Alasdair Allen, who first reported their findings on the **iPhone Tracker** blog, the geolocation file is stored on both the iOS device and "any computers that store backups of its data," and "can be used to reconstruct a detailed snapshot of the user's comings and goings, down to the second."

The researchers aver that despite Apple's refusal to even acknowledged the existence of these files, or frankly what the firm does with the data once its been downloaded to their servers, users of iPhones and iPads are put at risk that their movements are available to any and all comers with the requisite skills to access their information.

"The most immediate problem is that this data is stored in an easily-readable form on your machine," Warden and Allen wrote.

"Any other program you run or user with access to your machine can look through it. By passively logging your location without your permission, Apple have made it possible for anyone from a jealous spouse to a private investigator to get a detailed picture of your movements."

Needless to say, such information would be a boon to police agencies seeking to "terminate with extreme prejudice" the ability of protest organizers to communicate with demonstrators, as happened during the G20 protests in Pittsburgh, as ***Antifascist Calling*** reported in 2009.

Elliot Madison was arrested after he relayed a police order to disperse message via Twitter to demonstrators during the protests. A week later, his New York City home was raided by the FBI's Joint Terrorism Task Force (!) which carted off his computers and cell phone as "evidence." Madison and co-defendant Michael Wallschlaeger were criminally charged with using computers, cell phones and a police scanner to track the movements of "Pittsburgh's finest." Federal prosecutors charged the activists with "hindering apprehension or prosecution, criminal use of a communication facility, and possession of instruments of crime."

While such repressive acts may have raised eyebrows two years ago, they have now become part of the seamless panopticon spreading across the "shining city on a hill" like an invisible swarm of privacy-killing locusts.

Last week, in the wake of the smartphone tracking scandal, **CNET News** reported that "law enforcement agencies have known since at least last year that an iPhone or iPad surreptitiously records its owner's approximate location, and have used that geolocation data to aid criminal investigations."

Security journalist Declan McCullagh revealed that although "Apple has never publicized the undocumented feature buried deep within the software that operates iPhones and iPads," the secretive Mountain View firm acknowledged to Congress last year that "cell tower and Wi-Fi access point information" is "intermittently" collected and "transmitted to Apple"

every 12 hours.

CNET reported that “phones running Google’s Android OS also store location information,” according to Swedish programer Magnus Eriksson. Another researcher told McCullagh that “‘virtually all Android devices’ send some of those coordinates back to Google.”

“Among computer forensics specialists,” CNET avers, “those location logs–which record nearby cell tower coordinates and time stamps and cannot easily be disabled by someone who wants to use location services–are not merely an open secret. They’ve become a valuable sales pitch when targeting customers in police, military, and intelligence agencies.”

In other words, enterprising grifters from niche security firms servicing the secret state–or anyone willing to pay for their unique services, say a dodgy employer, a jealous spouse or a sociopathic freak for that matter–can take advantage of a smartphone’s embedded location files.

CNET reported that the “U.K-based company Forensic Telecommunications Services advertises its iXAM product as able to ‘extract GPS location fixes’ from an iPhone 3GS including ‘latitude, longitude, altitude and time’.”

“Its literature boasts,” McCullagh writes, that “‘these are confirmed fixes–they prove that the device was definitely in that location at that time’.”

“Another mobile forensics company, Cellebrite,” CNET avers, even “brags that its products can pluck out geographical locations derived from both ‘Wi-Fi and cell tower’ signals, and a third lists Android devices as able to yield ‘historical location data’ too.”

Just last week, ***The Tech Herald*** disclosed that the Michigan State Police have been using a handheld device and “secretly extracting information from cell phones during traffic stops,” and have refused to release information on this program to the ACLU.

The Tech Herald reports that for “nearly three years, the ACLU has attempted to get the Michigan State Police (MSP) to answer questions over their use of Cellebrite’s UFED Physical Pro scanner.”

“The handheld device allows police to extract data from phones and SIM memory,” journalist Steve Ragan writes, and that “in addition to the normal information, such as contact lists, email, and text messages, the UFED is also able to recover hidden and deleted data.”

Manufactured by security outfit **Cellebrite**, the company boasts that their “mobile forensics products enable extraction and analysis of invaluable evidentiary data including deleted and hidden data for military, law enforcement, governments, and intelligence agencies across the world,” according to a blurb on their web site.

The ACLU **charges** that the device is routinely used during traffic stops and that state troopers were able to access the mobile devices without their users being aware their data was being grabbed.

In their letter to the MSP, the ACLU cautioned that “The Fourth Amendment protects citizens from unreasonable searches. With certain exceptions that do not apply here,” the civil liberties watchdogs averred, “a search cannot occur without a warrant in which a judicial

officer determines that there is probable cause to believe that the search will yield evidence of criminal activity."

"A device that allows immediate, surreptitious intrusion into private data creates enormous risks that troopers will ignore these requirements to the detriment of the constitutional rights of persons whose cell phones are searched."

Sounds reasonable, right? The MSP responded by demanding the ACLU fork over $544,680 before they'd even consider releasing these *public* documents!

But as Cryptohippie reported in their excellent study, ***The Electronic Police State***, "two crucial facts about the information gathered under an electronic police state are these: 1. It is criminal evidence, ready for use in a trial. 2. It is gathered universally ('preventively') and only later organized for use in prosecutions."

"In an Electronic Police State," researchers averred, "every surveillance camera recording, every email sent, every Internet site surfed, every post made, every check written, every credit card swipe, every cell phone ping… are all *criminal evidence*, and all are held in searchable databases. The individual can be prosecuted whenever the government wishes."

Called a "Universal Forensic Extraction Device," Cellebrite claims their "UFED family of products is able to extract and analyze data from more than 3000 phones, including smartphones and GPS devices."

According to the firm, such tools will prove invaluable to secret state snoops. "Diving deeper into a mobile phone's memory than ever before provides them with the ability to gather data and establish connections between networks and people that is quicker and easier to arrive at."

The secret-spilling web site **Cryptome** has generously provided us with with Cellebrite's **Smartphone PDA Spy Guide**. Amongst other things, we're told that the firm's "UFED Forensics system empowers law enforcement, anti-terror and security organizations to capture critical forensic evidence from mobile phones, Smartphones and PDAs."

"UFED," we're informed, "extracts vital data such as phonebook, camera pictures, videos, audio, text messages (SMS), call logs, ESN IMEI, ICCID and IMSI information from over 1,600 handset models, including Symbian, Microsoft Mobile, Blackberry and Palm OS devices."

Think you've erased those messy call logs or text messages to your girl- or boyfriend? Better think again! With Cellebrite on the job, "the UFED can extract data from a phone, or directly from the SIM card. When extracting from phone, the UFED connects to the phone via cable, Bluetooth or infrared, and the data is read logically from the phone. It also performs a physical extraction from SIM cards, allowing extraction of additional data such as deleted SMS, ICCID, IMSI, location information and more."

We're told that the company's UFED "helps intelligence agencies widen their view and form a complete picture with access to content that can be repurposed, analyzed, and linked to information existing in databases," Main Core, or a similar national security index, perhaps?

"For us, people look like little particles…"

While digital technologies advance by leaps and bounds, the Empire's political-economic

requirements are determining how new devices will be used, who has access to the data points and, once our personal details are extracted–by corporations or shadowy intel outfits (public and private) who do their bidding–what happens to it once it's been stored in giant data farms.

The Wall Street Journal reported that Massachusetts Institute of Technology researchers are conducting a study that "has tracked 60 families living in campus quarters via sensors and software on their smartphones–recording their movements, relationships, moods, health, calling habits and spending."

"In this wealth of intimate detail," reporter Robert Lee Hotz writes, MIT researcher Alex Pentland "is finding patterns of human behavior that could reveal how millions of people interact at home, work and play."

According to preliminary findings, "the data can predict with uncanny accuracy where people are likely to be at any given time in the future," and the data "can reveal subtle symptoms of mental illness, foretell movements in the Dow Jones Industrial Average, and chart the spread of political ideas as they move through a community much like a contagious virus, research shows."

"Advances in statistics, psychology and the science of social networks are giving researchers the tools to find patterns of human dynamics too subtle to detect by other means," the *Journal* reports.

At Northeastern University in Boston for example, "network physicists discovered just how predictable people could be by studying the travel routines of 100,000 European mobile-phone users."

"After analyzing more than 16 million records of call date, time and position," Hotz reports, "the researchers determined that, taken together, people's movements appeared to follow a mathematical pattern," and that given enough information about past movements, scientists averred "they could forecast someone's future whereabouts with 93.6% accuracy."

Chillingly, Northeastern physicist Albert-Laszlo Barabasi, who conducted the study, told the *Journal*: "For us, people look like little particles that move in space and that occasionally communicate with each other. We have turned society into a laboratory where behavior can be objectively followed."

Ruthless "objectivity" such as this have real world consequences, not that it matters to those whose butter their bread by bludgeoning our privacy and cratering our political rights.

"As a reward when the [MIT] experiment was done," the *Journal* laconically observed, "the students were allowed to keep the smartphones used to monitor them."

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/