GlobalResearch
Center for Research on Globalization

Smartphones: The Tracking and Surveillance of Millions of Americans

By Tom Burghardt
Global Research, May 02, 2011
Antifascist Calling... 2 May 2011

Region: USA
Theme: Police State & Civil Rights

As Smartphone Scandal Grows, Tech Firms Run for Cover, Reap Windfall Profits

Recent revelations that Apple's iPhone and iPad, Google's Android and Microsoft's Windows Phone 7 operating systems collect, store and transmit records of users' physical locations to central databases–secretly, and without consent–have ignited a firestorm over Americans' privacy rights in an age of hypersurveillance.

And with a lawsuit filed last week in U.S. District Court in Florida by two iPhone users, ***The Register*** reports, Apple guru Steve Jobs was forced to respond to complaints after the firm's usual tactic–deafening silence–failed to assuage customer's anxieties.

The lawsuit alleges that "irreparable injury has resulted and continues to result from Apple's unauthorized tracking of millions of Americans," plaintiffs Vikram Ajjampur and William Devito averred. They are requesting their case be granted class-action status, a move likely to send shudders along the silicon spine of the secretive Cupertino high-tech powerhouse.

In response to the outcry, ***The Wall Street Journal*** reported that Apple "is scaling back how much information its iPhones store about where they have been and said it will stop collecting such data when consumers request it, as the company tries to quell concerns it was tracking iPhone owners."

But as journalists Yukari Iwatani Kane and Jennifer Valentino-Devries point out, "a week of silence on the growing controversy, raised new questions and criticism about its data-handling practices."

The ecumenical nature of the smartphone spying scandal tapped another firm, beloved by Wall Street grifters and national security mavens alike, on the shoulders last week.

The Detroit News reported that two "Oakland County women have filed a $50 million class-action lawsuit against Google Inc. to stop the company from selling phones with Android software that can track a user's location."

Like Apple, Google claims that tracking software is meant "to provide a better mobile experience on Android devices," and stressed that "any location sharing is done with the user's permission."

That's rather rich coming from a firm whose former CEO, Eric Schmidt, told **CNBC** in 2009, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place," a telling statement all the more pertinent here when secret state

snoops demand access to your search history, conveniently "retained" for the asking by the search and advertising giant.

> "If Android location services are turned on," independent security researcher Samy Kamkar told **The Register**, "the OS sends Google a MAC addresses, network signal strength, and GPS coordinates for each Wi-Fi network, as well as a unique identifier for the phone that grabs the information and the time of day." (emphasis added)

"By combining the identifier with the location data," Kamkar told the nose-tweaking UK publication, "Google could easily determine where you work and where you live. If this location information and unique IDs remain on Google's servers, it could potentially be extracted via subpoena or national security letter."

As privacy and security researcher Christopher Soghoian **revealed** in 2009, "Sprint Nextel" and other telecom giants "provided law enforcement agencies with its customers' (GPS) location information over 8 million times between September 2008 and October 2009."

Soghoian wrote that 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," a service eagerly provided our political minders by the telecoms as the secrecy-shredding web site **Cryptome** revealed with their publication of *dozens* of **Online Spying Guides**.

As we now know, secret state agencies such as NSA and the FBI routinely grab customer records from the telecoms to obtain dialed telephone numbers, text messages, emails and instant messages, as well as web pages browsed and search engine queries in addition to a staggering mountain of geolocational data, oftentimes with a simple, warrantless request.

The NSA's so-called "President's Surveillance Program" for example, vacuums-up huge volumes of "transactional" records gleaned from domestic emails and internet searches as well as bank transfers, credit card transactions, travel itineraries and phone records from other secret state satrapies as well as banks, credit reporting agencies and data-mining firms.

As ***The Wall Street Journal*** reported more than three years ago, "the NSA's enterprise" is linked to "a cluster of powerful intelligence-gathering programs, all of which sparked civil-liberties complaints when they came to light."

Investigative journalist Siobhan Gorman revealed that "the effort also ties into data from an ad-hoc collection of so-called 'black programs' whose existence is undisclosed," the tip of a vast surveillance iceberg.

But such programs could not function without the close, one might argue incestuous, collaboration between the secret state and their corporate partners as *The Washington Post* disclosed last year in their **"Top Secret America"** investigation.

In fact, as Soghoian and other researchers have learned, internet service providers and the telecoms "all have special departments, many open 24 hours per day, whose staff do nothing but respond to legal requests. Their entire purpose is to facilitate the disclosure of their customers' records to law enforcement and intelligence agencies–all following the

letter of the law, of course."

Plaintiffs Julie Brown and Kayla Molaski said they neither "opted-in" to Google's surveillance features nor approved of being tracked, by their phones no less, asserting that Android's tracking capability puts "users at serous risk of privacy invasions, including stalking," according to their complaint.

And with congressional grifters on both sides of the aisle poised to hold hearings this month about the controversy, it appears that smartphone manufacturers will have some 'splainin' to do. Right-wing congressman Joe Barton (R-TX) told the *Journal* that Apple "apparently 'lied' to him and another lawmaker last year when it said its phones don't collect and transmit location-based data when location services such as mapping are turned off."

Damage Control

Seeking to tamp down criticism, Apple claimed it was all a mistake, the result of "software bugs" which they are now striving mightily to "fix."

Strange then, or perhaps not, given the company's notorious penchant for secrecy, that nary a hint of a problem passed their granola-flecked lips prior to revelations which researchers Pete Warden and Alasdair Allen posted on their **iPhone Tracker** blog.

To wit, the researchers discovered that 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."

A particularly convenient "feature" when the feds, local cops, your boss or a seedy private snoop comes a calling.

According to iPhone Tracker's FAQ: "If you run it on an OS X machine that you've been syncing with an iPhone or an iPad with cellular plan, it will scan through the backup files that are automatically made, looking for the hidden file containing your location. If it finds this file, it will then display the location history on the map."

In response to the question: "Why is Apple collecting this information?" the researchers answer "it's unclear." However, "one guess might be that they have new features in mind that require a history of your location, but that's pure speculation. The fact that it's transferred across devices when you restore or migrate is evidence the data-gathering isn't accidental."

"The more fundamental problem," Warden and Allen write "is that Apple are collecting this information at all."

An April 27 damage control **statement** from the firm claims that "Apple is not tracking the location of your iPhone. Apple has never done so and has no plans to ever do so."

They assert that "iPhone is not logging your location," but rather, is "maintaining a database of Wi-Fi hotspots and cell towers around your current location." You see it's all an innocent misunderstanding, nothing more than a convenient means for users to "quickly find GPS satellites."

While the “entire crowd-sourced database is too big to store on an iPhone,” we’re told that they “download an appropriate subset (cache) onto each iPhone.”

Further claiming that “this cache is protected but not encrypted,” it’s “backed up in iTunes whenever you back up your iPhone. The backup is encrypted or not, depending on the user settings in iTunes.”

In other words, we won’t tell you we’re downloading an unencrypted locational cache onto your iTunes library where it can be read by anyone with access to your laptop or home computer, so any trouble that might attend an unauthorized peek at your data is *your* problem.

But because “we care,” and not because of the adverse publicity generated by the firm treating their customers “like little particles that move in space … that occasionally communicate with each other,” as physicist Albert-Laszlo Barabasi told ***The Wall Street Journal***, Apple plans “to cease backing up this cache in a software update coming soon.”

However, **CNET News** reported last week that Rep. Jay Inslee (D-WA), “isn’t satisfied with Apple’s explanation of why iPhones keep track of their users’ locations and wants a federal probe into the Cupertino software marker’s privacy practices.”

For their part Microsoft, journalist Declan McCullagh writes, “says it does not save location histories directly on Windows Mobile 7 devices,” but acknowledge that “in some circumstances” the firm “collects information including a unique device ID, details about nearby Wi-Fi networks, and the phone’s GPS-derived exact latitude and longitude.”

Like Apple and Microsoft, CNET reports that “Android devices store a limited amount of location information but transmit to Google current and recent GPS coordinates, nearby Wi-Fi network addresses, and two 16-letter strings apparently representing a device ID that’s unique to each phone,” a point emphasized by the women suing Google over the firm’s privacy breach.

Paranoia or Well-Founded Suspicions? You Make the Call!

Surveillance concerns are inevitable, especially when advert pimps seek to market useless junk to consumers or unaccountable secret state agencies monitor political dissidents at home and abroad, by peeping at locational data when the “unique device ID is transmitted, which allows a company to track a customer’s whereabouts over an extended period of time,” as CNET cautions.

Similar privacy and surveillance issues also surround unencrypted connections to the internet with the largely opaque practice of deep-packet inspection (DPI), a favorite tool beloved by marketeers and government spies alike, as ***Antifascist Calling*** reported back in December.

It now appears that smartphone manufacturers have joined their telecom partners in the spy game, a scandal that first broke the surface when whistleblower Mark Klein **spilled the beans** about AT&T’s close collaboration in NSA’s warrantless wiretapping program, a constitution-shredding operation that continues apace under the “change” regime of “transparency president,” Barack Obama.

Concerns over the uses of geolocational databases are not **fodder**, as some would have it,

for “privacy conspiracy theorists screaming back to their panic rooms,” but rather is an inevitable outgrowth of a culture of secrecy and deceit that permeates the opaque universe shared by corporations and governments.

As Declan McCullagh and other journalists have pointed out, “location databases can be a gold mine for police or civil litigants: requesting cell phone location information from wireless carriers has already become a staple of criminal investigations, often without search warrants being sought.”

Increasingly, niche security outfits such as the **Israeli-owned** firm **Cellbrite**, whose top executives possess high-level security résumés, along with probable connections to Israel’s NSA equivalent, Unit 8200, tout their ability to customers in global police, military and intelligence agencies to extract location histories from smartphones in under two minutes as ***The Tech Herald*** reported.

Such marketing ploys however, are fully in tune with today’s “cybersecurity” paradigm, the latest front (and profit center) in America’s endless “War On Terror.”

As George Mason University researchers Jerry Brito and Tate Watkins reported in an essential new study, ***Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy***, “the rhetoric of ‘cyber doom'” that calls forth new control measures, “lacks clear evidence of a serious threat that can be verified by the public. As a result, the United States may be witnessing a bout of threat inflation similar to that seen in the run-up to the Iraq War.”

“Additionally,” Brito and Watkins write, “a cyber-industrial complex is emerging, much like the military-industrial complex of the Cold War. This complex may serve to not only supply cybersecurity solutions to the federal government, but to drum up demand for them as well,” a point that *Antifascist Calling* has reported many times.

While criminals, stalkers, identity thieves and other miscreants exploit systemic vulnerabilities for their own sociopathic ends, much the same can be said of private security firms such as HBGary, Palantir and *hundreds of others* servicing the secret state, all capitalizing on “zero day vulnerabilities” in software and operating systems while designing stealthy, undetectable **“root kits”** for their government partners.

One can imagine that similar “black programs” exist for exploiting smartphone vulnerabilities, a likely prospect made all the easier when they are built-in features of the operating systems.

High-Tech Misery Fuels Windfall Profits

Spying isn’t the only issue battering tech giant Apple’s squeaky-clean image.

As workers around the world celebrate May Day, ***The Observer*** revealed that some 500,000 workers at the Shenzhen and Chengdu factories owned by Foxconn, Apple’s primary contractor, which produces millions of iPhones and iPads yearly for the global market are treated “inhumanely, like machines.”

Growth by the firm is predicated on driving production and labor costs down, a strategy that helped rocket Apple past software giant Microsoft as ***Bloomberg News*** reported last week.

Microsoft's share price "declined as much as 74 cents to $25.97 in extended trading," and "shares dropped 9 percent last quarter, while the Standard and Poor's 500 Index rose 5.4 percent."

"The results," *Bloomberg* reports, "underscore the ascendance of Apple, which surpassed Microsoft as the world's most valuable technology company in May. Apple's profit in the period that ended in March almost doubled to $5.99 billion, compared with $5.23 billion for Microsoft in the same period. That was the first time Apple's profit topped Microsoft's in two decades."

These results tend to emphasize the predatory nature of the *entire* high-tech sector, fueled both by consumer demand for new products and the windfall profits generated by production in low-wage, highly-repressive states such as China.

Several studies of Apple's production practices undertaken by the Netherlands-based Centre for Research on Multinational Corporations (**SOMO**) revealed "disturbing allegations of excessive working hours and draconian workplace rules at two major plants in southern China. It has also uncovered an 'anti-suicide' pledge that workers at the two plants have been urged to sign, after a series of employee deaths last year," *The Observer* reports.

While the Taiwanese-owned firm denies wrongdoing, researchers disclosed that "in some factories badly performing workers are required to be publicly humiliated in front of colleagues."

A second report released by the Hong Kong-based labor rights group Students & Scholars Against Corporate Misbehavior (**SACOM**) "describes how a culture of absolute obedience is imposed on workers from the first day of their recruitment. Workers are punished for all kinds of 'misconduct,' including not meeting their daily production quota, making mistakes or taking too much time for a bathroom visit."

"Disciplinary actions," the group reports, "include taking away bonus points, making workers publicly confess their mistakes and scolding and humiliating them in front of gathered colleague workers, making workers copy quotations of CEO Terry Gou, etc."

"Security guards," according to testimony by Foxconn employees, "were found to regularly assault workers verbally and physically."

With a basic 48-hour work week, Chinese workers are forced to work up to 98 hours of overtime a month to meet demands by Western consumers for Apple products. Foxconn manager Louis Woo however, told *The Observer* that "all the extra hours were voluntary."

Last month, **SACOM** reported that a second, grifting capitalist outfit, Wintek, had routinely poisoned workers by substituting the toxic chemical "n-hexane in violation of local codes and without proper safety equipment."

Used in the production of touch screens for Apple, SACOM revealed that "medical maladies … began when their employer, a factory owned by Taiwan's Wintek, swapped basic rubbing alcohol with the more dangerous toxin n-hexane in the final cleaning process of touch screens to shave off a few seconds off production time. N-hexane is a known toxin and prolonged, high-level exposure can caused nerve damage and a long list of medical problems."

In response to the charges, Apple said they are "committed to ensuring the highest standards of social responsibility throughout our supply base. Apple requires suppliers to commit to our comprehensive supplier code of conduct as a condition of their contracts with us. We drive compliance with the code through a rigorous monitoring programme, including factory audits, corrective action plans and verification measures."

But as with *all* aspects of the globalized capitalist economy, profits by Western firms like Apple and other high-tech parasites take precedence over the labor and social rights of workers. Chantal Peyer, a researcher with the Swiss group Bread for All said that "A brand like Apple has a very high profit margin on hardware: more than 40%. But it asks suppliers, which have a much lower profit margin of about 4%, to lower production costs. As a result, labour costs are squeezed and workers never get living wages."

Such outrages however, are not the result of a few "bad apples, but rather, lie at the heart of a heartless system that profits off the misery of the vast majority of the world's population, including here in the United States.

As researcher and economist Michel Chossudovsky points out in ***The Global Economic Crisis: The Great Depression of the XXI Century***: "The development of world capitalism is predicated on a profit-driven global cheap labor economy. One of the main features of this system has been the development (over the last thirty to forty years) of industrial colonies in low-wage countries. The relocation of industry to these countries has led to corporate downsizing and layoffs, as well as the outright closing down of a wide range of productive activities in the developed countries."

"Mass poverty and a worldwide decline in living standards," Chossudovsky writes, "are largely the result of this global cheap labor economy." This trend has accelerated since the 2008-2009 global economic meltdown. "In developing countries, including China," Chossudovsky avers, which is America's largest industrial colony, the levels of employment are in a freefall. The pre-existing structures of Third World poverty are replaced by social destitution and, in many regions of the developing world, by outright starvation."

As workers globally, and the United States is no exception to the rule imposed by the ruthless, continue to be squeezed as living standards and social benefits decline, revolt becomes inevitable. In this context, the burgeoning police state that functions as a well-armed pit bull for financial swindlers and capitalist oligarchs alike, are being marshaled to surveil and when necessary, repress, those challenging the prevailing "free market" paradigm.

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****, an independent research and media group of writers, scholars, journalists and activists based in Montreal, 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.*

Read about Osama Bin Laden in Michel Chossudovsky's international best-seller

America's "War on Terrorism"

by Michel Chossudovsky
also available in pdf format

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

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