

Companies sell mobile phone spying tools to governments worldwide

Thomas Gaist
26 August 2014

Cell phone location tracking technologies long used by the US National Security Agency and British GCHQ are increasingly available for purchase by other governments throughout the world, the *Washington Post* reported Monday.

Cell phone location data tracking systems, which include a range of associated intelligence gathering capabilities, are constantly being developed and marketed by private security contractors. The technology enables governments and private entities to track the movements of cell phone users across national boundaries, in many cases pinpointing users' precise locations within a few meters.

One surveillance firm, called Defentek, boasts on its web page that its Infiltrator Global Real-Time Tracking System can "locate and track any phone number in the world." The Infiltrator System is "a strategic solution that infiltrates and is undetected and unknown by the network, carrier, or the target," the site says.

Analysis of cell phone location tracking software by the watchdog group Privacy International highlighted the role of Verint, a sophisticated Israeli-American private security and intelligence contractor that employs former government agents, including special forces soldiers.

Verint reports on its web page that the company's systems are used by "more than 10,000 organizations in over 180 countries," the *Washington Post* reported.

The spread of such cutting-edge surveillance systems by private security and intelligence firms is taking place with the help of the major telecommunications corporations. Verint states that it has installed location data capture software on cellular networks in numerous countries with the knowledge and cooperation of major telecommunications providers.

A confidential Verint advertising brochure posted

online by Privacy International detailed the wide array of surveillance capabilities offered by Verint to clients. According to its advertising material, Verint's "Solution's Portfolio" includes "Cellular Interception and Control, Mobile Satellite Interception, Global Cellular Location, and IP Interception and Tampering." The brochure notes that the company sells "Monitoring Centres that can operate at nationwide levels and has been known to have had installations in Slovakia, Ivory Coast, India and Vietnam."

For the right price, Verint will also carry out and/or facilitate a number of other intelligence-related operations on behalf of its clients, including:

- * Identifying potential targets and building an intelligence picture over cellular networks
- * Passively and covertly collecting cellular traffic in an area and analyzing it in real time to identify potential targets
- * Identifying suspicious communication patterns using a range of analysis tools, including Location, Speech Recognition, Link Analysis, Text Matching
- * Intercepting voice calls and text messages of potential targets
- * Identifying, intercepting, decoding, manipulating and analyzing WiFi-enabled devices such as tablets, smartphones, and laptops

Verint also claims that it can break into encrypted communications and remotely activate microphones on cell phones, and the company offers training sessions simulating a range of tactical scenarios with its in-house veteran military and intelligence personnel.

Reports from the summer of 2013 showed that Verint provided systems used by the Mexican government during the administration of President Felipe Calderon to capture and analyze all types of communications in that country beginning in 2007, as part of operations

initiated in coordination with the US State Department.

In its report, the *Washington Post* noted that surveillance agencies and private companies are increasingly deploying “IMSI catchers,” also referred to as StingRays, which enable users to send fake text messages, inject malware into targeted phones, and intercept the content of various forms of cellphone-based communications.

In addition to using StingRays, surveillance agencies can tap directly into cell phone towers to identify movement patterns of nearby telephone users. Location data from cell phone towers, moreover, is regularly transferred in bulk to federal, state, and local security agencies across the US through a procedure known as “tower dumps.”

Revelations from December of 2013 have already shown that the NSA’s CO-TRAVELLER program gathers around 5 billion pieces of cell phone location data worldwide on a daily basis, and has been capable of tracking the location of cellphones, even when switched off, since 2004. Location data gathered by the NSA allows the agency to map the overall movement pattern of targeted individuals, their daily routes and habitual meeting places.

The US uses related technology to orchestrate its drone wars in Afghanistan, Pakistan, Yemen and elsewhere. As part of a program codenamed GILGAMESH, the NSA’s “Geo Cell” program, which sports the motto “We Track ‘Em, You Whack ‘Em,” guides drone strikes against alleged terrorists by tracking the location of SIM cards inside their cellphones.

All of these surveillance and tracking programs are part of the efforts of the US and other imperialist states to compile comprehensive databases on their respective populations in response to growing popular opposition to the growth of social inequality and attacks on democratic rights.



To contact the WSWs and the
Socialist Equality Party visit:

wsws.org/contact