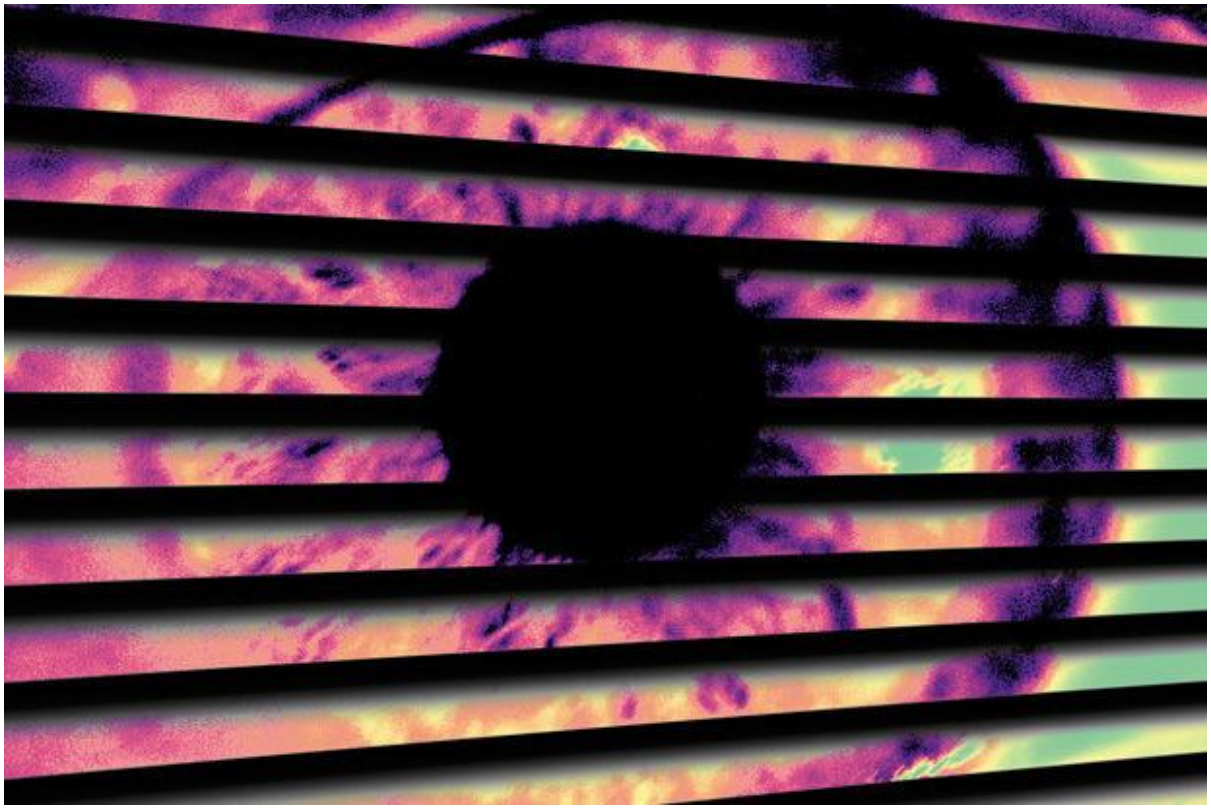
Spy equipment suppliers: Report exposes who sells surveillance tech to Colombia

A baby's car seat complete with audio and video recorder for covert surveillance…Privacy International's investigative report reveals the companies selling surveillance tech to Colombia, despite that it may be used for unlawful spying.

Computerworld | Sep 2, 2015 11:31 AM PT



"We always assume we are being watched. It is part of our understanding. We think it's a tactic to wear us down. We get tipped off by people in the state. They tell us 'people are listening to you.'…" Would you be surprised to learn that a priest said that? Father Alberto is just one person living under surveillance in Colombia; he was interviewed by Privacy International as it investigated the shadow surveillance state in Colombia. The second investigative report looked into more than a dozen international companies selling surveillance equipment to Colombian government agencies and police.

In the past, "intercepted communications were vital to covert Colombian and CIA operations against the FARC." The DEA "heavily" supports Esperanza, Colombia's most visible communications interception system that "can obtain mobile and fixed-line call data." But it is far from the only surveillance system in the country, surveillance equipment

that has been used for unlawful surveillance after being sold and supported by international companies.

Although some Colombian companies "integrate their own tactical interception systems," such as Emerging Technologies Corporation, which is developing" drone plug n' play technology with California-based DreamHammer, other equipment is purchased outright at surveillance and security tech trade shows like the "Wiretappers' Ball" by ISS World. Here are some of the international companies mentioned in Privacy International's investigative report "Demand/Supply: Exposing the Surveillance Industry in Colombia" (pdf).

"The types of surveillance products purchased by Colombian agencies from the private sector generally fall into two categories – those required for network surveillance and those that facilitate tactical surveillance."

While you might have heard of some surveillance products, you might not know about some of the smaller tactical products "on sale" in Colombia. For example, have you heard of a child's car seat being equipped with video and audio recording devices so it can be used for covert surveillance?

Bloomberg Business noted that "LMW Electronics Limited designs, manufactures, and services video and audio transmission systems and rugged covert cameras for directed and intrusive surveillance." While the LMW surveillance link redirects to this site which offers very little insight, Privacy International's report included a flyer for the "LMW babyseat" sold by UK Company LMW Electronics.

The creepy covert surveillance car seat is powered by an internal battery to remotely control the "vertically mounted pan, tilt and zoom camera" with "front and rear viewing" and optical and digital zoom options. Recordings include a "burnt in" timestamp and can be retrieved from a USB drive hidden in the baby seat.

The report also shows a flyer for a credit card recording device by the Swiss company Nagra and a device dubbed a "'Pointer." The latter, as seen on the right side in the image above, is "a hand-held device that can be used to determine the direction in which a person using a communications device is travelling."

Network surveillance

Privacy International's report includes detailed descriptions of network surveillance and the companies who sold it to the Colombian police. It also talks about home-grown firms that worked with international surveillance sellers, but here are some of the international firms which made sure Colombia had invasive network surveillance.

US tech firm Pen-Link provided Colombian agents with the Esperanza interface used "to manage and analyze intercepted phone data and content." Pen-Link also sells the Lincoln server platform that hosts intercepted data. "Lincoln can 'receive real-time intercept information delivered by the carriers, for any of the agency's legally authorized intercepts'." Pen-Link 8 client software controls the collection process. Pen-Link, Privacy International wrote, "is a preferred supplier" of the DEA.

The report mentions Komcept Solutions' mobile audio recording device that resembles a briefcase. A quick search found the DM-144 which has 144 miniature microphones (pdf) that can be hidden in a laptop bag and left unattended while it records from over 50 meters away. The person doing the spying can sit elsewhere to control the device, listening live, while appearing to be listening to music via headphones.

Verint Systems Ltd, an Israeli sister company to the US Verint Systems Inc, sold mass surveillance tech to Colombian cops. Verint Systems, back in the 2000s, was involved in supplying the wiretapping equipment to Verizon during the NSA warrantless wiretapping scandal. Although the report remarks upon Verint System's SkyLock system which can "track the location of a mobile phone anywhere in the world," it primarily talks about Verint's PUMA.

The PUMA interception system is a "powerful and invasive" technology "designed to collect all data that passes through the cables for subsequent analysis." PUMA is "linked directly to the service providers' network infrastructure, usually at the mobile switching center, by a probe that routes all data directly to the law enforcement monitoring facility without interfering with the transmission of the data between the send and recipient."

PUMA launched in 2007, but while it was being built the police created the Integrated Recording System (IRS) platform. IRS could monitor "massive communications traffic; it "was not limited to targeted surveillance" as it could generate new targets. In 2013, Colombian police contracted Israeli tech company NICE Systems to expand PUMA's interception capacity; the cops were then able to intercept and collect 100 million cell calls and 20 million text messages per day without service providers' knowledge.

Super-PUMA could also monitor ISP traffic and up to 700 workstations; data was "intercepted by eight 'NiceTrack IP' probes that 'filter and extract huge quantities of data delivered simultaneously over highly loaded IP links'." For the first time, 4G data could also be intercepted.

Another company, UK-headquartered Network Critical, provided "fiber optic passive traffic access points;" it's used as a network sniffer.

Tactical surveillance

IMSI catchers, aka stingrays, trick mobile devices into connecting to their strong wireless signals. The devices can target a specific person's phone, or grab everyone's data that connects to the fake cellphone tower. Some include location monitoring solutions that "determine the location of a target to within one meter."

Regarding IMSI catchers sold to and used for interception in Colombia, the Laguna system was supplied by the Spectra Group and the Canadian telecommunications company Exfo exported NetHawK F10 IMSI catcher. However Privacy International called the Bulldog and Nesie systems "popular items."

Bulldog acts like a fake cell tower so phones will connect to it; when used with direction finding equipment, Bulldog can "locate target devices and their users from among a pool of

devices in a given area." Nesie can do the same, but can also "deny access of specific phones to the real network, forcing those phones to connect with the Nesie device and communicate real-time unencrypted call content to Nesie operators." Both are sold by UK surveillance company Smith Myers Communications.

A person's communications can also physically be obtained from their device when it is seized covertly or when a person is arrested. Colombia used the Forensic Toolkit (FTK) made by US-based AccessData. The 3.0 FTK allowed an "analyst to not only 'preview a target's machine from across the network to determine relevancy prior to acquisition, but … also acquire and fully analyze the data on the system, including the system's RAM.' A remote drive feature enables analysts to forensically analyze live data – such as system memory, logical volumes, physical devices – on a remote device from the analyst's system. The software could also be used to decrypt PGP-encrypted disks."

Last but not least is the Hacking Team, which sold its Remote Control System toolkit to the Colombian police. "RCS can be used to hijack computer and mobile devices while remaining undetectable to users as it is designed to bypass common antivirus programs and encryption," the report stated. It can not only capture data and passwords, but also remotely access webcams and microphones. After the Hacking Team was hacked, Rook Security provided a free Milano tool to find out if your PC is infected with Hacking Team malware.

Does it matter to these suppliers that the Colombian government has used the equipment for unlawful spying? Do the companies disregard interception scandals in their quest to rake in millions of dollars? An "estimated 600 public figures including parliamentarians, journalists, human rights activists, lawyers, and judges," and others have been spied upon. Privacy International added, "Targets have been spied upon and harassed in horrifying ways, and it continues to this day."

Privacy International wrote, "The illegal interception of communications and the abuses of privacy rights will continue so long as the technologies that the surveillance industry sells and the ways in which they are used stay in the shadows."