The Espionage Economy

U.S. firms are making billions selling spyware to dictators.

Ricardo Martinelli resides in a condo at the Atlantis, a luxury high-rise on Florida's Biscayne Bay made famous by the TV series *Miami Vice*. A hefty, white-haired billionaire, Martinelli, 63, was viewed just a few years ago as one of Latin America's most popular leaders: From 2009 until 2014, he was president of Panama. But now, though he's living in high style, Martinelli is a fugitive from justice.

He fled his country on Jan. 28, 2015, hours before Panama's Supreme Court announced a corruption investigation into his administration. Among the charges Martinelli faces is political espionage, with a possible prison sentence of 21 years, for illegally eavesdropping on the phones and emails of more than 150 people: Panamanian opposition leaders, journalists, judges, business rivals, cabinet members, U.S. Embassy officials, a Roman Catholic archbishop, and even a woman identified as Martinelli's mistress.

Much of this alleged activity was made possible by the burgeoning business of private companies selling military-grade spyware. In 2011, the *Wall Street Journal* reported that the retail market for surveillance tools had increased in value from virtually nothing 10 years prior to around $5 billion annually. Yet the market functions largely unencumbered, and even since the National Security Agency eavesdropping scandal broke in 2013, U.S. policymakers have paid little attention to firms that sell surveillance equipment to foreign governments.

The scandal in Panama offers a unique window into how dangerous the espionage export business has become. Without restrictive controls, the risks the industry poses will only grow: More and more countries will acquire the tools to perpetrate corruption and abuse human rights.

* * *

Panamanian prosecutors are building a case against Martinelli that his lawyer, Rogelio Cruz, calls "Kafkaesque." His client, who is seeking asylum in the United States, is innocent of all charges, Cruz claims. However, according to a 2009 diplomatic cable released by WikiLeaks, Martinelli demanded bugging equipment from the U.S. Drug Enforcement Administration soon after taking office; he intended to use it against security threats. The cable, prepared by Barbara Stephenson, then the U.S. ambassador to Panama, noted "Martinelli's near-obsession with wiretaps." The request was rejected, Stephenson wrote, because Martinelli "made no distinction between legitimate security targets and political enemies." The cable concluded, "We believe that he has tasked several subordinates to obtain wiretap capacity by reaching out to other governments and the private sector."

This information, it seems, was correct.

According to regional media, Martinelli paid at least $13.4 million for devices to monitor phones and tap into email and contact lists. (The *PanAm Post* has alleged that he dipped into a food program for the poor to cover the cost.)

According to regional media, Martinelli paid at least $13.4 million for devices to monitor phones and tap into email and contact lists. (The *PanAm Post* has alleged that he dipped into a food program for the poor to cover the cost.) One of the companies Martinelli used was NSO Group Technologies, an Israeli intelligence firm owned by a U.S. outfit, Francisco Partners. According to NSO's promotional material, its system "introduces a powerful and unique monitoring tool, called Pegasus, which allows remote and stealth monitoring and full data extraction from remote target[ed] devices via untraceable commands." An internal memo from Italian malware vendor Hacking Team, made public last summer by WikiLeaks, notes that the tool sends a targeted phone "a silent sms [message] which exploits the device." For an attack to work, the message merely needs to be read.

Panama's government isn't the only one using spyware purchased on the private market. According to a 2015 report by the U.K.-based watchdog group Privacy International, another U.S.-Israeli firm, Verint, has supplied Colombia's security apparatus with sophisticated surveillance systems. "Since 2005, the company has been central to the development of mass interception capabilities in Colombia," the report states. (In February 2015, a former Colombian security chief was convicted for her role in illegal wiretapping during the 2002-2010 tenure of President Álvaro Uribe.)

Verint and an Israeli tech company called Nice Systems, according to another Privacy International report, have also sold hardware and software to Kazakhstan and Uzbekistan, enabling the countries' repressive governments to spy on landlines, mobile phones, and Internet networks. This has helped officials institute near-airtight clampdowns on political dissent. As the report's co-author, Edin Omanovic, told *Vice* in 2014, "The brutal secret police of authoritarian states have been empowered with sweeping surveillance capabilities aimed at putting the private lives of every individual within their reach. This is exactly the kind of nightmare scenario that becomes inevitable when you have an unaccountable industry operating under the radar."

Privacy International found that, at one point, Verint reached out to a California-based firm, Netronome, for technology that would help Uzbek officials break encryption systems used

by Facebook, Gmail, and other sites. (Whether the program succeeded is unclear.) Following the report's release, Netronome said in a statement that it "does not condone any violation of human rights or personal privacy" and that it complies with the laws of the countries in which it operates.

* * *

Therein lies the rub, however: The privatization of mass surveillance is the result of weak export controls and voluntary international agreements regarding invasive spyware. The only mechanism for regulating spying systems is the Wassenaar Arrangement, which allows for countries to regularly exchange information on transfers of conventional weapons and dual-use goods and technologies. But it is nonbinding on its 41 signatories, including the United States, and Israel has never formally agreed to its terms.

In Washington, Rep. Chris Smith (R-N.J.) introduced a bill in 2013 designed to "prevent United States businesses from cooperating with repressive governments in transforming the Internet into a tool of censorship and surveillance." The legislation never even made it out of a subcommittee. Today, unsurprisingly, the matter remains very low on Republicans' priority scale.

Citizens used to have technology on their side. In the age of analog communications, mass surveillance was labor-intensive; there were too many people, too many wires, and too few listeners. Today, however, advanced digital technology is on the side of the oppressor. It is impossible to turn back the clock, but it is not too late to enact strict regulations on spyware. And there are at least two precedents: In 2012, both the United States and the European Union imposed bans on the sale, supply, transfer, and export of espionage technology to Syria and Iran.

Unless more countries agree to treat systems of mass surveillance as they do weapons of mass destruction, the words of George Orwell's *1984* could become a constant reality: "You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized."

Illustration by Matthew Hollister