Trade in surveillance technology raises worries

Sari Horwitz, Shyamantha Asokan, Julie Tate ⋮ 14-17 minutes ⋮ 12/1/2011

Northern Virginia technology entrepreneur Jerry Lucas hosted his first trade show for makers of surveillance gear at the McLean Hilton in May 2002. Thirty-five people attended.

Nine years later, Lucas holds five events annually around the world, drawing hundreds of vendors and thousands of potential buyers for an industry that he estimates sells $5 billion of the latest tracking, monitoring and eavesdropping technology each year. Along the way, these events have earned an evocative nickname: the Wiretappers' Ball.

The products of what Lucas calls the "lawful intercept" industry are developed mainly in Western nations such as the United States but are sold all over the world with few restrictions. This burgeoning trade has alarmed human rights activists and privacy advocates, who call for greater regulation because the technology has ended up in the hands of repressive governments such as those of Syria, Iran and China.

"You need two things for a dictatorship to survive: propaganda and secret police," said Rep. Christopher H. Smith (R-N.J.), who has proposed bills to restrict the sale of surveillance technology overseas. "Both of those are enabled in a huge way by the high-tech companies involved."

But the overwhelming U.S. government response has been to engage in the event not as a potential regulator but as a customer.

The list of attendees for this year's local Wiretappers' Ball, held in October at the North Bethesda Marriott Hotel and Conference Center, included more than 35 federal agencies, Lucas said. The list, he added, included the FBI, the Secret Service and every branch of the military, along with the IRS, the Agriculture Department and the Interior Department's Fish and Wildlife Service. None would comment on their participation in the event.

Representatives of 43 countries also were there, Lucas said, as were many people from state and local law enforcement agencies. Journalists and members of the public were excluded.

On offer were products that allow users to track hundreds of cellphones at once, read e-mails by the tens of thousands, even get a computer to snap a picture of its owner and send the image to police — or anyone else who buys the software. One product uses phony updates for iTunes and other popular programs to infiltrate personal computers.

Many monitoring systems work by cloning e-mails or making records of Web traffic, allowing police or other users to track the use of key words. Others use stand-alone hardware to eavesdrop on nearby cellphone or WiFi signals.

The Commerce Department regulates exports of surveillance technology, but its ability to restrict the trade is limited. Intermediaries sometimes redirect sales to foreign governments, even those that are subject to economic sanctions, once products leave the United States. The State Department, which has spent $70 million in recent years to promote Internet freedom abroad, has expressed rising alarm over such transactions but has no enforcement authority.

U.S. law generally requires law enforcement agencies to obtain court orders when intercepting domestic Internet or phone communications. But such restrictions do not follow products when they are sold overseas.

Industry officials say their products are designed for legitimate purposes, such as tracking terrorists, investigating crimes and allowing employers to block pornographic and other restricted Web sites at their offices.

"This technology is absolutely vital for civilization," said Lucas, president of TeleStrategies, which hosts the events, officially called Intelligent Support Systems World Conferences. "You can't have a situation where bad guys can communicate and you bar interception."

But the surveillance products themselves make no distinction between bad guys and good guys, only users and targets. Several years of industry sales brochures provided to The Washington Post by the anti-secrecy group WikiLeaks, and released publicly Thursday, reveal that many companies are selling sophisticated tools capable of going far beyond conventional investigative techniques.

“People are morally outraged by the traditional arms trade, but they don’t realize that the sale of software and equipment that allows oppressive regimes to monitor the movements, communications and Internet activity of entire populations is just as dangerous,” said Eric King of Privacy International, a London-based group that seeks to limit government surveillance. Sophisticated technology “is facilitating detention, torture and execution,” he said, “and potentially smothering the flames of another Arab Spring.”

Surging demand worldwide

Demand for surveillance tools surged after the Sept. 11, 2001, attacks as rising security concerns coincided with the spread of cellphones, Skype, social media and other technologies that made it easier for people to communicate — and easier for governments and companies to eavesdrop on a mass scale.

The surveillance industry conferences are in Prague, Dubai, Brasilia, the Washington area and Kuala Lumpur, whose event starts Tuesday. They are invitation-only affairs, and Lucas said he bars Syria, Iran and North Korea, which are under sanctions, from participating.

The most popular conference, with about 1,300 attendees, was in Dubai this year. Middle Eastern governments, for whom the Arab Spring was “a wake-up call,” are the most avid buyers of surveillance software and equipment, Lucas said. Any customers who come to the event are free to buy the products there.

“When you’re selling to a government, you lose control of what the government is going to do with it,” Lucas said. “It’s like selling guns to people. Some are going to defend themselves. Some are going to commit crimes.”

The suppliers are global as well. About 15 of the vendors for the conference in Bethesda were based in the United States, Lucas said. Others were from Germany, Italy, Israel, South Africa and Britain; many of these also have U.S. offices targeting the market for law enforcement agencies and other government buyers.

Of the 51 companies whose sales brochures and other materials were obtained and released by WikiLeaks, 17 have secured U.S. government contracts in the past five years for agencies such as the FBI, the State Department and the National Security Agency, according to a Washington Post analysis of federal procurement documents.

Federal agencies declined to comment on the use of surveillance technology. But Lucas said the Fish and Wildlife Service uses monitoring gear to catch poachers, the Agriculture Department to investigate abuse of grants and the IRS to search for evidence that tax filers have understated their income.

“The IRS loves to find people filing zero income on their tax returns with photos of Ferraris on their Facebook pages,” Lucas said.

An IRS spokesman declined to comment.

Privacy experts say that the legal framework governing the industry has not kept up with its growth and that products sold for legitimate purposes, such as blocking access to certain Web sites or investigating sexual predators, can easily be adapted for broader surveillance.

Far-reaching tools

The brochures collected by WikiLeaks make clear that few forms of electronic communication are beyond the reach of available surveillance tools. Although some simple products cost just a few hundred dollars and can be bought on eBay, the technology sold at the trade shows often costs hundreds of thousands or millions of dollars. Customization and on-site training can provide years of revenue for companies.

One German company, DigiTask, offers a suitcase-size device capable of monitoring Web use on public WiFi networks, such as those at cafes, airports and hotels. A lawyer representing the company, Winfried Seibert, declined to elaborate on its products. "They won't answer questions about what is offered," he said. "That's a secret. That's a secret between the company and the customer."

Another German firm, Elaman, touts in its government security brochure the capacity to “identify an individual’s location, their associates and members of a group, such as political opponents.”

A British company, Cobham, creates bogus cellphone towers that let users track phones up to three miles away and listen to some calls, according to its brochure. A spokesman confirmed it provides cellular tracking devices for “bona fide law enforcement agencies worldwide.”

The FinFisher program, which creates fake updates for iTunes, Adobe Acrobat and other programs, was produced by a British company, Gamma International. The Wall Street Journal reported on this product, and several other surveillance tools described in sales brochures, in an article last month. Apple said that on Nov. 14 it altered iTunes to block FinFisher intrusions.

A lawyer who represents Gamma, Peter Lloyd, said that FinFisher is a vital investigative tool for law enforcement agencies and that the company complies with British law. “Gamma does not approve or encourage any misuse of its products and is not aware of any such misuse,” he said.

The WikiLeaks documents, which the group also provided to several European news organizations and one in India, do not reveal the names of buyers. But when Arab Spring revolutionaries took control of state security agencies in Tunisia, Egypt and Libya, they found that Western surveillance technology had been used to monitor political activists.

"We are seeing a growing number of repressive regimes get hold of the latest, greatest Western technologies and use them to spy on their own citizens for the purpose of quashing peaceful political dissent or even information that would allow citizens to know what is happening in their communities," Michael Posner,

assistant secretary of state for human rights, said in a speech last month in California. "We are monitoring this issue very closely."

In Syria, where President Bashar al-Assad's efforts to crush an uprising have left 3,500 people dead, by U.N. calculations, police have reportedly been using surveillance technology to eavesdrop on electronic communications and block access to Web sites.

Syrian activist Rami Nakhle said that after he set up an online newspaper and started blogging about human rights, Syria's secret police last year began summoning him for regular interrogations that involved threats of torture and a day in solitary confinement. Officers made it clear that they had watched him online despite his efforts to conceal his identity.

Police also hacked into fellow activists' Facebook accounts, said Nakhle, 29. "Before, they were not very good at this, but now they are getting more advanced," he said.

Nakhle fled to Lebanon in January and now lives in suburban Washington as a political exile. Many of his friends are still in Syrian prisons. "I am not that idealistic. I know that companies need money, but this is about people's lives," he said.

A Syrian Embassy spokesman did not respond to messages seeking comment on the government's use of surveillance technology.

Getting past sanctions

The Commerce Department is investigating how monitoring devices made by Blue Coat Systems, based in Sunnyvale, Calif., reached Syria despite sanctions, according to several U.S. officials who spoke on the condition of anonymity to discuss an ongoing investigation. Blue Coat Systems has said it didn't know its products were being used by Syria and that the devices in question were intended for the Iraqi communications ministry. A distributor, the company said, shipped the products to a reseller in Dubai late last year.

In a statement last month, Blue Coat said it was cooperating with government agencies probing "this unlawful diversion" and conducting its own internal review. A spokesman for the company declined to comment further.

NetApp, also of Sunnyvale, produced hardware and software that the Syrian government was using to build a system to intercept and catalogue vast amounts of e-mail, according to Bloomberg News. NetApp has denied selling equipment to Syria. The project, which was never finished, also included computer equipment from another California company and two European businesses.

The technology's spread is not limited to the Middle East. A federal lawsuit filed in May accuses Cisco Systems of helping China monitor the Falun Gong group.

The lawsuit, filed by the U.S.-based Human Rights Law Foundation, alleges that Cisco helped design and provide equipment for China's "Golden Shield," a firewall that censors the Internet and tracks government opponents. Cisco has acknowledged that it sells routers, which are standard building blocks for any Internet connection, to China. But it denies the allegations in the suit, saying that it has not customized any items for use in censorship.

A spokesman for the Chinese Embassy did not respond to messages seeking comment. U.S. companies that want to export devices "primarily useful for the surreptitious interception of wire, oral or electronic communications" must apply to the Commerce Department for a license to sell to overseas buyers under the department's Export Administration Regulations.

But it can be hard to prove that an export is "primarily useful" for surveillance. Some products need to be used in combination with other equipment in order to eavesdrop. Even standard anti-virus software can be retooled to read e-mails and attachments.

Daniel Minutillo, a Silicon Valley-based lawyer who advises technology companies, said that in most cases his clients can show that their products have multiple uses, making them exempt from export licensing rules.

Human rights groups want this exemption ended. "As long as the market is increasing and there is a lack of regulation, it's a perfect mix," said Arvind Ganesan, who studies online surveillance for Human Rights Watch. "The Obama administration has not led in this regard, and there are only a few voices in Congress talking about this. It's a massive oversight."

Smith's bill, which has stalled in committee several times in recent years, would prevent sales to countries, such as China and Syria, that restrict Internet freedom. Yet more aggressive U.S. laws might push the industry overseas if other nations don't impose similar restrictions. Indian and Chinese vendors have attended Wiretappers' Balls in recent years.

A State Department official who attended the event in October was pessimistic that government regulation could curb a fast-changing technology sector. "We've lost," said the official, who spoke on the condition of anonymity. "If the technology people are selling at these conferences gets into the hands of bad people, all we can do is raise the costs. We can't completely protect activists or anyone from this."