Written by **Joe Wolverton, II, J.D.** on July 14, 2015

Leaked E-mails Expose Efforts to Secretly Expand Surveillance State

What do an Italian software company and an Orlando law enforcement agency have in common? Growing the surveillance state. On July 11, the *Orlando Sentinel* reported:

> An Italian company that sells surveillance software to governments and law enforcement agencies worldwide was negotiating to provide an Orlando police agency with spyware technology that infiltrates phones and computers, according to emails just released.

The *Sentinel* noted that "the emails and files, which have since been catalogued by WikiLeaks, show that Hacking Team was selling its products to nations with records of human rights abuses, including Ethiopia, Bahrain, Egypt, Kazakhstan, Russia, Saudi Arabia, Sudan and Azeraijan. The paper continued,

> The technology, developed by Hacking Team, can monitor conversations and emails, and even turn phones and laptops into surveillance devices by remotely activating cameras and microphones.

And:

> On April 22, Agent Randall Pennington of the Metropolitan Bureau of Investigation — a major-crimes task force that covers Orange and Osceola counties — emailed Hacking Team: "We are a law enforcement task force located in Orlando, Florida. I would like to speak with someone regarding your products."
>
> Within a month, a Hacking Team employee, Daniele Milan, flew from Italy to Orlando to meet with four MBI agents, including the director, Larry Zweig. According to an email Milan sent his co-workers, MBI wanted to increase its surveillance capability. Budget wasn't a concern, the MBI officials said, even though a leaked company invoice shows Hacking Team services can cost more than $400,000.

Of course, budgets are becoming less and less of a concern for local law enforcement as the federal government doles out billions of dollars in grant money.

According to a statement made by Zweig, the MBI didn't end up buying the Hacking Team's product, the *Sentinel* reports.

Hacking Team's internal database of potential customers ranked MBI highly, even reportedly adding a "smiley face" emoticon to the spreadsheet next to the entry for the Florida law enforcement agency.

While the deal between MBI and Hacking Team may not have gone down as easily as both sides would have liked, Hacking Team knows to keep fishing in Florida's big pond of police departments.

Particularly as police in Florida (in)famously have been busy buying the tools of the surveillance state for years.

Last year, for example, federal law enforcement officers seized the records of a police force's use of a controversial surveillance system known as "Stingray" just before the information was scheduled to be released to the public.

The U.S. Marshals Service "stunned" the American Civil Liberties Union (ACLU), which was waiting on the imminent release of the documents pursuant to a public records request the group filed in 2014 with the Sarasota, Florida, police department. The petition sought to shed light on the scope of the department's use of the Stingray device.

According to the ACLU, its representatives were scheduled to be given access to the documents just days before federal marshals showed up and took possession of the entire cache, claiming they were the property of the U.S. Marshals Service. The feds forbade the local police from releasing the documents as planned.

Wired reports that Wessler said this behavior "is consistent with what we've seen around the country with federal agencies trying to meddle with public requests for stingray information." The blog also notes that the Department of Homeland Security has gone to similar lengths to prevent Stingray surveillance details from becoming public. "The feds are working very hard to block any release of this information to the public."

Police in Tallahassee have deployed the devices as well — an act which invoked an ACLU motion with a local court, requesting information about use of the Stingray. Later, a judge in Tallahassee ordered the information released.

According to the group's blog, the behavior that prompted their petition was its discovery that

> police used a stingray to track a phone to a suspect's apartment without getting a warrant. Although the detective responsible for the tracking testified in court about using a stingray, in deference to the government's demand for secrecy the court closed the hearing to the public and sealed the transcript.

Trying desperately to keep the records sealed, the government argued that revealing the information would violate various federal statutes, including the Homeland Security Act.

The court was not persuaded and ordered the release of the entire transcript of the hearing on the use of the Stingray.

The transcript reveals, according to the ACLU, six violations of the Fourth Amendment and other constitutional guarantees of civil liberty:

> Stingrays "emulate a cellphone tower" and "force" cell phones to register their location and identifying information with the stingray instead of with real cell towers in the area.
>
> Stingrays can track cell phones whenever the phones are turned on, not just when they are making or receiving calls.
>
> Stingrays force cell phones in range to transmit information back "at full signal, consuming battery faster." Is your phone losing battery power particularly quickly today?
>
> Maybe the cops are using a stingray nearby.
>
> When in use, stingrays are "evaluating all the [cell phone] handsets in the area" in order to search for the suspect's phone. That means that large numbers of innocent bystanders' location and phone information is captured.

> In this case, police used two versions of the stingray — one mounted on a police vehicle, and the other carried by hand. Police drove through the area using the vehicle-based device until they found the apartment complex in which the target phone was located, and then they walked around with the handheld device and stood "at every door and every window in that complex" until they figured out which apartment the phone was located in. In other words, police were lurking outside people's windows and sending powerful electronic signals into their private homes in order to collect information from within.
>
> The Tallahassee detective testifying in the hearing estimated that, between spring of 2007 and August of 2010, the Tallahassee Police had used stingrays approximately "200 or more times."

The suitcase-sized Stingray masquerades as a cell tower to trick cellphones into connecting to it. It can give police tracking identifiers for phones within a mile or more, depending on terrain. Given the mobility of the device, police who use it can triangulate a target's location with better accuracy than if they relied on data transferred by traditional cell towers.

The Guardian reported on the desperate attempts by the feds to keep secret this sector of the surveillance state:

> The FBI is taking extraordinary and potentially unconstitutional measures to keep local and state police forces from exposing the use of so-called "Stingray" surveillance technology across the United States, according to documents obtained separately by the *Guardian* and the American Civil Liberties Union.
>
> Multiple non-disclosure agreements (NDAs) revealed in Florida, New York and Maryland this week show federal authorities effectively binding local law enforcement from disclosing any information — even to judges — about the cellphone dragnet technology, its collection capabilities or its existence.
>
> In an arrangement that shocked privacy advocates and local defense attorneys, the secret pact also mandates that police notify the FBI to push for the dismissal of cases if technical specifications of the devices are in danger of being revealed in court.
>
> The agreement also contains a clause forcing law enforcement to notify the FBI if freedom of information requests are filed by members of the public or the media for such information, "in order to allow sufficient time for the FBI to seek to prevent disclosure through appropriate channels."

This equipment isn't cheap. According to published reports, each Stingray device costs about $150,000. However, *USA Today* recently reported that, despite the cost, at least 25 police departments admit to owning a Stingray, with 30 other cities refusing to disclose whether or not they own one of these expensive surveillance devices.

Back in Orange County, the jurisdiction of the MBI, the *Sentinel* story reports that the sheriff's office "conducted 558 investigations from 2008 – 2014," all of which may have been carried out with the help of the Stingray.

To be fair, Florida isn't the exclusive venue of violations of the Fourth Amendment. This is a national constitutional crisis. There is so much compelling evidence that Americans are witnessing the accelerated establishment of a nationalized police force built upon the foundation of formerly free local law enforcement and equipped with technology, tactics, and weapons of immense power.