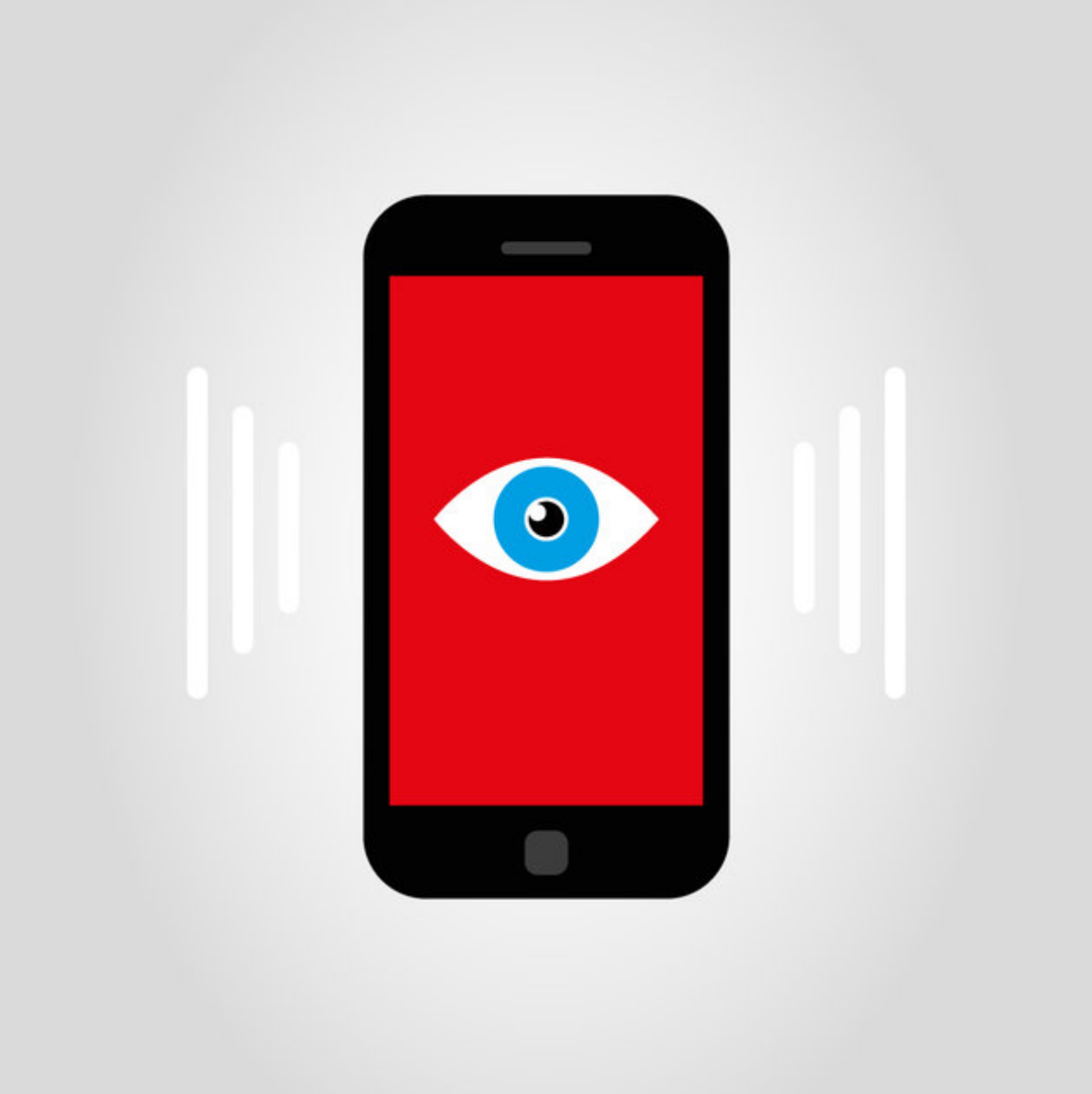
Miami, Along with Many Other Cities, Is Turning to 'Spyware' to Copy Cellphone Info

February 12, 2018



(TNS) — Criminals, like the rest of us, conduct a lot of business on cellphones — personal hand-held devices that have fast become primary targets for law enforcement. But accessing the information in them isn't as easy as a detective asking Siri to spill what's inside.

There are technical barriers as well as complicated and unresolved legal questions and civil rights concerns before police can begin digging through a suspect's cellphone data.

In the face of those challenges, police departments around the country have increasingly turned to what some critics have dubbed cellphone spyware. It's a device with software that when attached to a cellphone can extract and store contacts, pictures, GPS locations and frequented social media sites — information that can potentially help make criminal cases.

Miami's police force, which purchased the software a little over a year ago, is the latest South Florida police department to join the growing wave of cellphone spyware users. Miami-Dade, the largest police department in the southeast U.S., has had such devices for more than a decade, but has purchased several newer versions, the latest last August.

Law enforcement agencies stress that there are strict laws that limit how they can employ cellphone spyware. They can't just suck out the data from a suspect via Bluetooth or Wi-Fi, for instance. They've got to seize it first. And police insist they don't use the system without the consent of an owner or without a search warrant.

Once a phone is confiscated, it is stored in a place that blocks incoming data so that the information can't be updated, altered or erased, which could contaminate the phone data as evidence.

There are also technical roadblocks. Not all cellphones can be entered without a password, and technological advances in phone security systems are constantly making it more difficult. The newer versions of the iPhone, for example, are out of reach for law enforcement without a password.

"They're constantly updating (the technology) to try and get around passwords," said Eldys Diaz, the executive officer to the chief of police in Miami. "In some cases you can't get a complete forensic dump without someone providing that info."

Defense attorneys and civil rights groups also are fighting the spyware, arguing the systems amount to a broad invasion of privacy often built on the narrow confines of a search warrant. For instance, if police are looking for evidence of one crime and find material to support another charge, should they be allowed to use it?

A Miami-Dade court case last summer shows some of the obstacles law enforcement often face in trying to obtain stored cellphone information.

In a case that was closely watched by the legal community, a Miami-Dade judge decided not to hold reality TV star Hencha Voigt in contempt of court for failing to give up the password to her iPhone. Voigt, a self-described " fitness model," and a man named Wesley Victor were accused of shaking down a social media celebrity for $18,000 in exchange for the duo not releasing stolen sex videos of socialite YesJulz.

Voigt's phone was confiscated a year earlier when she was arrested. Two times before the judge issued his decision, Voigt said she couldn't remember her cellphone password. Civil rights advocates sided with the judge, arguing giving up the password would have violated Voigt's Fifth Amendment right not to incriminate herself.

"If it's the type of phone you don't have a password for, you're out of luck," Diaz said.

A month after the judge's ruling, the FBI somehow managed to hack into Voigt's phone. Texts between the fitness model and Victor in which the sex tapes were discussed seemed to bolster the state's case.

Miami-Dade Police Lt. Juan Villalba Jr., whose agency has had equipment supplied by the digital intelligence company Cellebrite for more than a decade, said using the spyware is no different than an IRS agent showing up at a business with a warrant demanding financial information.

"We're going to leverage emerging technologies in combating crime," said the lieutenant. "Everybody these days is walking around with a smartphone in their pocket."

Still, civil rights groups such as the American Civil Liberties Union are concerned that investigators who fail to narrow searches on personal devices could extract personal information that has little or nothing to do with a specific case.

"It's important that a warrant describes what particular thing police are looking for," said ACLU staff attorney Nate Wessler, who is currently arguing a cellphone case before the U.S. Supreme Court. "Most of the time, personal photos aren't relevant."

Wessler said there are a handful of judges around the country who have started writing limitations into search warrants. A good practice, he said, is to have someone other than the actual investigator search through and extract the specific information listed in the warrant from cellphones.

Diaz, Miami's executive officer to the chief, said obtaining a search warrant for a cellphone is similar to getting one for a home — police must show that the phone was either part of the crime or that there is likely evidence in it pertaining to a crime.

"It would depend on the facts of the case and the connection to a crime," he said. Diaz said all of Miami's search warrants are reviewed by the Miami-Dade State Attorney's Office before being presented to a judge.

The extraction devices have become so popular that an investigation last year by CityLab, an online arm of The Atlantic magazine, found that the vast majority of the largest 50 police departments in the U.S. use cellphone extraction devices. CityLab began its investigation after The Intercept released a catalog of military tools used by domestic law enforcement that was leaked to it by an intelligence community source concerned about the militarization of domestic law enforcement.

Cellphones have forced law enforcement and the courts to constantly change tactics to keep up with modern-day criminals and still-evolving surveillance laws. There are no longer many land lines that, with court approval, can be tapped. Burner cells, basically throwaway phones, are common. In the past, police have been reprimanded in the courts for the use of a tracking device called a Stingray — a cell site simulator that mimics towers and sends out signals to trick cellphones in the area into transmitting locations — without warrants.

Last September, an appeals court in Washington ruled that search warrants are needed for police to use the Stingray. It was the fourth similar ruling by a state appeals or federal district court on the controversial technology.

Wessler, the ACLU attorney, argued a case before the U.S. Supreme Court in November that raises the question as to whether the 4th Amendment — which covers unreasonable search and seizure — is violated when law enforcement accesses cellphone location records without a warrant.

The case involves four men who used weapons to rip off Radio Shack and T-Mobile stores in Detroit between 2010 and 2011. The suspects were arrested and one of the men turned over his cellphone to police. Information from the phone was used to determine that Timothy Carpenter — who was not one of the original men arrested — took part in the crime. He was later arrested.

Carpenter filed a lawsuit claiming a search warrant was needed for law enforcement to obtain the records from a cellphone store that led to his arrest. When a lower court judge determined the FBI did not need a search warrant to learn where the suspects' phones were used and at what times, the case moved on to the U.S. Supreme Court. A final decision is expected by the summer.

Since 9/11, local police agencies have seen an influx of federal dollars that have been used to bolster local crime-fighting and terrorism. Most of them are far larger and more intimidating than the small devices that extract cellphone information.

It's no longer unusual to see what used to be strictly military vehicles like a Bearcat — an eight-ton tank-like vehicle with turrets for sharpshooters — during standoffs or when police are issuing arrest warrants. Giant, bus-like mobile command centers installed with closed-circuit cameras commonly pop up during active crime scenes. Police are often outfitted with gas detectors and thermal and night vision devices.

Backed by a federal grant of almost $5 million this year, Miami police are making a series of purchases that include four giant cameras on trailers that are capable of turning 360 degrees and relaying pictures in high definition. The city deployed similar cameras during Art Basel in December and says they will be used for large events like the Coconut Grove Arts Festival.

"They're a vital part of our operations," said Diaz. "Some of those things are expensive and we would have a hard time budgeting for them."

As for the less intimidating policing tools, like the cellphone extraction system, Diaz is careful to say Miami police take almost every possible precaution to make sure laws are followed and privacy isn't invaded.

"We must follow legal procedures," he said. "We have to obtain an actual warrant for it. Those are devices that store very private information."

http://www.govtech.com/public-safety/Miami-Along-with-Many-Other-Cities-is-Turning-to-Spyware-to-Copy-Cell-Phone-Info.html