POPULAR MECHANICS

The High-Tech Way the Feds Found Ghislaine Maxwell

Courtney Linder

January 5, 2021

On July 2, 2020, the U.S. Federal Bureau of Investigation (FBI) tracked down Ghislaine Maxwell, a longtime alleged associate of convicted sex offender Jeffrey Epstein, at a secluded mountain hideaway in Bradford, New Hampshire. Maxwell was charged with enticement of minors, sex trafficking, and perjury.

To find Maxwell, the FBI used smartphone data to pinpoint her exact location, according to a newly unsealed affidavit supporting a search warrant application. An FBI agent filed that affidavit on July 1, 2020, just one day before Maxwell's arrest, the *Daily Beast* first reported on Monday.

Prior to arresting Maxwell, the FBI had general information about her hideout thanks to a search warrant obtained in New York that allowed authorities to receive GPS and historical cell site data from her smartphone. Maxwell had opened a new cell phone account under the moniker "G Max," which featured a Northeastern Massachusetts area code.

With that information in hand, the authorities were able to track Maxwell's location within a radius of approximately one square miles. But that wasn't specific enough, according to the affidavit, because the FBI didn't know which building Maxwell was living in at the time.

"The FBI does not know Maxwell’s current location and accordingly requires the information sought in this application in order to locate and arrest Maxwell," the document reads.

Ultimately, when authorities approved the New Hampshire search warrant, FBI agents were permitted to use an "investigative device or devices capable of broadcasting signals that will be received by" Maxwell's smartphone, "or receiving signals from nearby cellular devices," according to the affidavit. That didn't include phone calls, texts, or other kinds of data.

That means the feds likely used a stingray device, also known as a "cell site simulator" or "IMSI catcher," to get Maxwell's phone to fork over its precise GPS location. Stingrays are a type of invasive cell phone surveillance equipment that "mimic cell phone towers and send out signals

to trick cell phones in the area into transmitting their locations and identifying information," according to the American Civil Liberties Union (ACLU), a nonprofit devoted to preserving individual rights and freedoms in the U.S.

Specifically, stingrays take advantage of cell phones' ability to automatically connect to the cell tower with the strongest signal. Stingray devices produce a beefed-up signal that "muscles out the signals from legitimate cell towers and becomes the preferred signal source for the cell phone," according to a policy analysis from the Cato Institute, a libertarian think tank.

The devices conduct a general search of all cell phones within the stingray's radius, and can log International Mobile Subscriber Identity (IMSI) numbers that serve as unique identifiers for each individual smartphone, according to the Electronic Frontier Foundation (EFF), a nonprofit focused on digital rights.

But here's the problem: When authorities use a stingray to capture a suspect's location through their device's GPS data, the gadget also collects information from the phones of innocent passersby.

The ACLU says 75 agencies in 27 states and the District of Columbia own stingrays, according to November 2018 data. But lots of other departments could be using the technology, since "many agencies continue to shroud their purchase and use of stingrays in secrecy." That includes U.S. Immigration and Customs Enforcement (ICE), the U.S. Army, the Internal Revenue Service (IRS), and the National Security Agency (NSA), among others.

Realistically, the only way to keep your devices safe from this sort of attack is through a Faraday cage, or a device that blocks all electromagnetic communications. It's an enclosure that distributes an electrical charge or radiation all around the exterior of the cage, protecting anything inside. A Faraday cage is a hollow conductor, and the charge is on the outside surface of the container.

Because stingrays are notoriously "easy to acquire or build, with homemade devices costing less than $1,000 in parts," according to the EFF, it couldn't hurt to slip your smartphone or laptop into a Faraday sleeve if you're going to leave your device in the car for some reason and wish to avoid any possible detection.

Still, no need to be paranoid—unless, you know, you're on the run.