

US police phone-tracking accords often kept secret (Update)

March 21 2014, by Jack Gillum



This Oct. 24, 2013 file photo shows a youth checking his smartphone in Glenview, Ill. Local police may be tracking your cell phone. But they're regularly censoring information about how the technology's used or how much it costs taxpayers. Police departments nationwide have released incomplete details about a phone-surveillance tool known as a Stingray, and have blacked out or denied contracts with the device's maker. Even in states with strong freedom-of-information laws like Florida and Arizona, police say law-enforcement sensitivities and non-disclosure agreements have forced them to stay mum following public inquiries. (AP Photo/Nam Y. Huh, File)

Police across the U.S. may be intercepting phone calls or text messages to find suspects using a technology tool known as Stingray. But they are refusing to turn over details about its use or heavily censoring files when they do.

Police say Stingray, a suitcase-sized device that pretends it is a cell tower, is useful for catching criminals, but that is about all they will say.

For example, they will not disclose details about contracts with the device's manufacturer, Harris Corp., insisting they are protecting both police tactics and commercial secrets. The secrecy—at times imposed by non-disclosure agreements signed by police—is pitting obligations under private contracts against government transparency laws.

Even in states with strong open records laws, including Florida and Arizona, little is known about police use of Stingray and any rules governing it.

A Stingray device tricks all cellphones in an area into electronically identifying themselves and transmitting data to police rather than the nearest phone company's tower. Because documents about Stingrays are regularly censored, it's not immediately clear what information the devices could capture, such as the contents of phone conversations and text messages, what they routinely do capture based on how they're configured or how often they might be used.

In one of the rare court cases involving the device, the FBI acknowledged in 2011 that so-called cell site simulator technology affects innocent users in the area where it's operated, not just a suspect police are seeking.

Earlier this month, journalist Beau Hodai and the American Civil Liberties Union of Arizona sued the Tucson Police Department, alleging

in court documents that police did not comply with the state's public-records law because they did not fully disclose Stingray-related records and allowed Harris Corp. to dictate what information could be made public.

Disclosures about surveillance programs run by the federal National Security Agency have driven a sustained debate since last summer on the balance between privacy and government intrusion. Classified NSA documents, leaked to news organizations, showed the NSA was collecting telephone records, emails and video chats of millions of Americans who were not suspected of crimes.

That debate has extended to state and local governments. News organizations in Palm Springs, California; Tallahassee, Florida; Sacramento, California, and Pittsburgh are among those that have been denied records about Stingrays or Stingray-like devices, including details of contracts that Harris has with government agencies.

In a response to a records request from the Tallahassee Democrat newspaper about Florida's use of cell-tracking technology, the state's top police agency provided a four-page, heavily censored document signed by a police investigator. The newspaper reported that the document referred to guidelines concerning the purchase of items and sought the department's agreement to the "provisions/content of the Non-Disclosure Agreement."

The Desert Sun of Palm Springs made a similar request to the San Bernardino County Sheriff's Department, which said it had to maintain secrecy even though the newspaper found information online about cell site simulators.

And in Sacramento, the local sheriff's office told a TV station it would "be inappropriate for us to comment about any agency that may be using

the technology" in light of a Harris non-disclosure agreement.

Many of the requests were part of an effort to investigate the devices by Gannett Co. Inc., which publishes USA Today and owns other newspapers and television stations around the country.

"I don't see how public agencies can make up an agreement with a private company that breaks state law," said David Cuillier, the director of the University of Arizona's journalism school and a national expert on public-records laws. "We can't have the commercial sector running our governments for us. These public agencies need to be forthright and transparent."

A representative for Harris Corp. declined to comment or elaborate on how the company's agreements comport with open records laws. Court documents in Hodai's case show Harris' agreement required the Tucson city government not to "discuss, publish, release or disclose any information" about its products without the company's written consent.

© 2014 The Associated Press. All rights reserved.

Citation: US police phone-tracking accords often kept secret (Update) (2014, March 21)
retrieved 25 April 2024 from <https://phys.org/news/2014-03-police-phone-tracking-secret.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.