

[Blogs](#)

March 13, 2023

Northern District of Illinois Clarifies Standards for Tower Dumps



The U.S. District Court for the Northern District of Illinois recently found that in order for cell tower warrants to be supported by probable cause and satisfy Fourth Amendment concerns, they must include protocols limiting the government's collection of information from individuals not involved in the underlying criminal activity.

In *In re Application for Tower Dump Data for a Sex Trafficking Investigation*, No. 23 M 87, 2023 WL 1779775 (N.D. Ill. Feb. 6, 2023), the court only approved a "tower dump" warrant, commonly named as such for its tendency to sweep broadly and collect innocent third parties' information, after the government provided restrictions on its search.

The *Tower Dump* Decision

The federal government sought a tower dump warrant to locate multiple suspects in five armed attacks on six victims related to sex trafficking.^[1] The warrant sought records for all cell phones that pinged cell towers in the five different locations of the attacks. This had the potential to lead the government to identify the perpetrators of the crimes but also risked the government identifying individuals that were not involved in the crimes in any way, a total the court said that could be "in the hundreds, thousands, or hundreds of thousands."^[2] As the U.S. Supreme Court highlighted, without any constraints on the government, "'with just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense.'"^[3]

Because the warrant originally lacked any protocols to address the lack of particularity and overbreadth associated with tower dump warrants, the court required the government to amend the warrant application to curb the amount of cell-site data of uninvolved third parties the tower dump search would uncover, which included:

- Seizure of data *only* if the phone number hits two or more towers within a specific time range of 30 minutes to one hour, depending on the particular location;
- No further law enforcement efforts taken regarding identifiers that did not hit two or more towers within the time range; and
- Produced data that does not meet the first requirement to be segregated and maintained by someone not involved in the investigation.

With these protocols, the court recognized that cell phone identifiers of innocent third parties would likely still be produced to the government, but that these restrictions ensured that the government would not determine the specific identities of just anyone swept up in the government's search. Moreover, the court concluded that these restrictions on the government's conduct ensure there is a "fair probability" that the information produced would be that of a suspect, and that the Fourth Amendment does not require "certainty" for evidence to be seized.^[1]

Takeaways

This decision follows the increasing number of cases addressing geofence and reverse search history warrants, both of which—like tower dump warrants—sweep broadly and undoubtedly result in the collection of uninvolved individuals' information. Importantly, by seeking a warrant in this matter, the government conceded "that there is a reasonable expectation of privacy in one's location data in connection with a tower dump warrant."^[2] This is a break from the government's historical practice of obtaining tower dumps with a court order under the lower standard of relevance and materiality under 18 U.S.C. § 2703(d). Companies that receive these types of warrants should carefully review them for particularity and breadth in accordance with the Fourth Amendment. The Illinois court acknowledged that cell tower dump data may have "lesser privacy interests" than GPS data,^[3] but tower dump warrants must still be reasonably specific and satisfy Fourth Amendment principles of probable cause.

^[1] *Id.* at *1.

^[2] *Id.* at *2.

^[3] *See id.* (citing *Carpenter v. United States*, 138 S. Ct. 2206, 2217–18 (2018) (acknowledging that cell-site records provide "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations'")).

^[1] 2023 WL 1779775, at *4–5.

^[2] *Id.* at *2 n.3.

^[3] *Id.* at *4.

Explore more in

[Privacy & Security](#) [Perkins on Privacy](#)