

# Newsweek

## ICE just launched a \$2.4M contract with a secretive data surveillance company that tracks you in real time

Chantal Da Silva

June 7, 2018

The U.S. Immigration and Customs Enforcement (ICE) agency has signed a \$2.4 million contract with a little-known surveillance company that mines communications data and provides "real-time" tracking.

Data published on the [U.S. government's spending website](#) shows the Department of Homeland Security contracted Pen-Link Ltd. (PenLink), a software company that develops communications surveillance collection systems, on June 4 with ICE listed as the contracting subagency.

PenLink provides software that allows enforcement bodies to collect and analyze "massive amounts of social media and internet communications data," as well as collect wiretap intercepts "in real-time" for "tracking" and "live monitoring," [according to its website](#).

Julian Sanchez, a privacy and surveillance expert with the Cato Institute, said the company appears to specialize in telephone data analysis and geolocation data mining and tracking that could potentially determine where people are "within a block" of a cell tower.

"It used to be that cell towers weren't very precise as location finders because you could be anywhere near that tower, but especially in urban areas now that there are so many cell towers to handle the density of data being transferred, location information could be found within a block," Sanchez told *Newsweek*.

"One obvious use that an immigration agency might want to do with that information is when you have a fugitive or some specific person you want to track, you can track and arrest them," Sanchez said.

While information on PenLink's website is sparse, one of the company's products, Pen-Proxy, also allows users to get "real-time call alerts" that provide notifications of a "wide variety of alert trigger criteria," including audio, SMS and email alerts.

Sanchez said that kind of tool would come in handy if an agent wanted to "set up a condition if they were, say, investigating a gang and a bunch of them all text each other at 3 a.m. in the morning, that agent could get immediately woken up...and respond immediately."

PenLink, which did not respond to a request for comment from *Newsweek*, also claimed to work with "various third-party databases" that match subscribers to phone numbers, and to operate a Cell Tower Database that lets users look up a cell tower and sector location for a "target" in real time as they collect live call data.

Sanchez said that while telecommunications companies are legally prohibited from providing certain types of information to the government without legal process, "the third-party angle throws a wrinkle into things." He explained that third parties are not legally prohibited to share such information with government bodies, but said they would likely be barred from doing so in contractual agreements with data providers.

ICE spokesperson Matthew Bourke confirmed to *Newsweek* that ICE "exercised" a contract with PenLink this week, but said that the deal was originally awarded to the company in June 2017, five months after President Donald Trump took office.

He said ICE has previously used the company for services related to "case management" and "case analysis" prior to signing the \$2.4 million contract.

The deal involved a 12-month period of performance, which included support for a "proprietary telecommunications analysis and intercept software suite related to Homeland Security investigations, according to a special notice published on the government's federal business opportunities website on June 22, 2017.

The notice stated that "only one source (PenLink) is capable of providing the supplies or services required because the supplies or services are unique or highly-specialized."

"During the course of conducting criminal investigations, ICE Homeland Security Investigations Special Agents gather evidentiary documents and electronic data containing transactional and non-transactional telecommunications and Internet Protocol (IP) records", it explains, adding: "The exploitation, analysis and linking of these records can be a key component of a successful criminal investigation."

According to a Bloomberg snapshot of PenLink, the surveillance company was founded in 1986 and is headquartered in Lincoln, Nebraska, with additional offices in Boulder, Colorado, and Washington, D.C.

The company's software was used in the high-profile murder case of Laci Peterson, a California woman who disappeared while eight months pregnant with her first child.

Wiretaps performed using a then-proprietary electronic surveillance system created by PenLink called LINCOLN helped convict her husband, Scott Peterson, in 2014 of first-degree murder for her death and second-degree murder for the death of the couple's prenatal son.

In 2005, Peterson was sentenced to death by lethal injection. His case is currently on appeal with the Supreme Court of California.

Sanchez said that while PenLink's software could be used to track and convict individual people, immigration enforcement would also likely be attracted to its big data services, which PenLink advertises as being "virtually limitless."

Director of Immigration and Senior Counsel at the Niskanen Center Kristie De Peña told *Newsweek* the deal represents a broader trend of cities and federal immigration authorities going to greater lengths to track people of interest.

"A bunch of cities across the U.S. have been buying up this kind of tracking/storage software, including the feds," she said.

Sanchez agreed that "there is at least a broader trend toward the use of big data analytics by law enforcement and immigration in particular, where the nature of this kind of analysis means you are making inferences based on connections, such as physical proximity or communications."

"But, that can lead to mistakes that amount to determining guilt by association," he warned.

"For example, one of the things we know that ICE is interested in is trying to assign gang membership based on both the judgment of local police departments and social connections, which we know is often not superaccurate," he said, referring to ICE's campaign cracking down on members of the notorious MS-13 gang.

"Connections and patterns can exist without someone being a member of a gang," Sanchez said.

"For example, a little while back several toddlers were mistakenly identified as gang members based on these kinds of analytics."

De Peña said that while she could only speculate about the use of information collected through PenLink's services, collection itself would still be subject to legal process and ICE would have to obtain a warrant to track any particular individual.

Last year, however, ICE demonstrated its ability to put such a warrant to use when it used a Stingray, also known as a cell site simulator, to track down an immigrant suspected of "unlawful reentry" into the country in May 2017.

Such warrants are typically only available in criminal investigations. In this case, the government alleged that the immigrant was wanted for the crime of unlawfully reentering the country after being deported, according to American Civil Liberties Union.

The case suggests that ICE would likely have grounds to justify a warrant to track anyone suspected of being in the U.S. unlawfully.

Sanchez said it would not be difficult to imagine scenarios in which ICE would be able to obtain bulk collection of data so long as the agency is able to justify that such data is relevant to a particular investigation.

He said Americans need to ask themselves if they are "comfortable with the idea of calling and location data being trawled through for the purpose of hunting down people who might not really be guilty of anything more serious than wanting to come here and work."

He added that the language used by ICE and PenLink "looks not that different from the language that the NSA used to do bulk collection of telephone records," referring to National Security Agency's use of global surveillance tactics revealed in a data leak by former Central Intelligence

Sanchez said Americans "might not think that this is the kind of tactic that is justified, that it involves too much broad invasion of privacy to be justified for that goal."

For example, he said, "you might think pot should be illegal but you might think using methods to hunt down suicide bombers to hunt down local pot dealers is not justified," he said.

With it still unclear "how broadly ICE is intending to ingest information," Sanchez said the agency could be tempted to "vacuum up a lot more data about a lot more people," adding that the "law as it is currently written will allow them to do that."

The agency has come under increasing scrutiny in recent months, with growing calls from protesters and a number of politicians demanding ICE be abolished.

Under the Trump administration, ICE has overseen a widespread crackdown on undocumented immigrants involving raids carried out across the country.

On Tuesday, the United Nations condemned a "zero tolerance" policy recently announced by the agency, which has seen hundreds of families separated at the border, with parents being taken to federal jail and children being transported by ICE to facilities operated by the Health and Human Services department.

The U.N. called on ICE to halt the practice immediately, declaring it an "unlawful interference in family life" and a "serious violation" of children's rights