The Washington Post
Democracy Dies in Darkness

ICE investigators used a private utility database covering millions to pursue immigration violations

Government agencies increasingly are accessing private information they are not authorized to compile on their own

By Drew Harwell
February 26, 2021 at 4:55 p.m. EST

U.S. Immigration and Customs Enforcement officers have tapped a private database containing hundreds of millions of phone, water, electricity and other utility records while pursuing immigration violations, according to public documents uncovered by Georgetown Law researchers and shared with The Washington Post.

ICE's use of the private database is another example of how government agencies have exploited commercial sources to access information they are not authorized to compile on their own. It also highlights how real-world surveillance efforts are being fueled by information people may never have expected would land in the hands of law enforcement.

The database, CLEAR, includes more than 400 million names, addresses and service records from more than 80 utility companies covering all the staples of modern life, including water, gas and electricity, and phone, Internet and cable TV.

CLEAR documents say the database includes billions of records related to people's employment, housing, credit reports, criminal histories and vehicle registrations from utility companies in all 50 states, D.C., Puerto Rico, Guam and the U.S. Virgin Islands. It is updated daily, meaning even a recent move or new utility sign-up could be reflected in an individual search.

CLEAR is run by the media and data conglomerate Thomson Reuters, which sells "legal investigation software solution" subscriptions to a broad range of companies and public agencies. The company has said in documents that its utility data comes from the credit-reporting giant Equifax. Thomson Reuters, based in Toronto, also owns the international news service Reuters as well as other prominent subscription databases, including Westlaw.

Thomson Reuters has not provided a full client list for CLEAR, but the company has said in marketing documents that the system has been used by police in Detroit, a credit union in California and a fraud investigator in the Midwest. Federal purchasing records show that the departments of Justice, Homeland Security and Defense are among the federal agencies with ongoing contracts for CLEAR data use.

On Friday, the House Committee on Oversight and Reform sent letters to the chief executives of Thomson Reuters and Equifax seeking documents and other information on how ICE has used the utility data in recent years.

“We are concerned that Thomson Reuters’ commercialization of personal and use data of utility customers and sale of broad access to ICE is an abuse of privacy, and that ICE’s use of this database is an abuse of power,” said the letters, which were signed by Rep. Jimmy Gomez (D-Calif.), the committee’s vice chair, and Rep. Raja Krishnamoorthi (D-Ill.), the chairman of a subcommittee on economic and consumer policy.

Thomson Reuters directed requests for comment to ICE, which declined to comment on its “investigative techniques, tactics or tools,” citing “law-enforcement sensitivities.” Equifax did not respond to requests for comment.

ICE has not shared how often it has used utility records to track people, saying such details should be confidential because they outline protected investigative techniques.

But an immigration-case investigator appeared to note the access last June in an email to officials at the Georgia Department of Driver Services. The email was revealed as part of a Freedom of Information Act request by Georgetown Law’s Center on Privacy & Technology and reviewed by The Post. In the heavily redacted email, the officer said immigration authorities are pursuing a “straight-up Pleasure Visitor” accused of overstaying a visa and that a search of unspecified utility records had showed that the target had “recently departed” from an address.

In a separate letter to a Texas sheriff’s office in 2019, also obtained by Georgetown researchers and shared with The Post, a Thomson Reuters specialist said CLEAR’s utility data offered investigators a powerful way to find “people who are not easily traceable via traditional sources.”

Nina Wang, a policy associate at the Georgetown center, said the database offered ICE officers a way to pursue undocumented immigrants who may have tried to stay off the grid by avoiding activities such as getting driver’s licenses but could not live without paying to keep the lights on at home.

“There needs to be a line drawn in defense of people’s basic dignity. And when the fear of deportation could endanger their ability to access these basic services, that line is being crossed,” she said. “It’s a massive betrayal of people’s trust. … When you sign up for electricity, you don’t expect them to send immigration agents to your front door.”

ICE has a $21 million contract with a Thomson Reuters subsidiary for the data, though the subscription is scheduled to expire on Sunday. ICE published a new solicitation for a “Law Enforcement Investigative Database Subscription” in November, but it is unclear whether the Biden administration will renew the deal or award a new contract.

Jacinta Gonzalez, a senior campaign organizer at the Latino civil rights group Mijente, said her group has been alarmed and “horrified” by how quickly ICE has expanded its surveillance network through the use of private databases, which members suspect have been used by ICE officers to plan raids on people’s homes.

“People would say to us, ‘How did ICE get my address? I’ve never had interactions with the police, I’ve never used this address publicly,’” she said. “It puts people in a tremendously difficult situation. They have to decide whether to have electricity or subject themselves to having ICE get access to this information.”

Equifax has said it gathers utility-bill records from the National Consumer Telecom & Utilities Exchange, a consumer-credit reporting bureau that gathers data on people's account and payment history with companies including Verizon and AT&T.

The data-exchange bureau has defended its data collection as "empowering" for the "underserved and underbanked community," because the records help big companies assess the creditworthiness of people by using "alternative data sources" beyond traditional credit reports.

It's unclear whether the utility data from Equifax comes from NCTUE or some other source, though the two firms have a long-standing data-sharing agreement. Speaking of the partnership in a letter to the Justice Department in 2001, a NCTUE representative wrote that Equifax had a "commitment to find and exploit appropriate opportunities for third-party access to exchange data."

Federal laws such as the Privacy Act of 1974 regulate how federal agencies can gather or use Americans' personal information, but they do not cover CLEAR or other private databases, and federal law enforcement has increasingly turned to them for information it otherwise is not allowed to collect without a court order.

Immigration agents have accessed information from a private database of license-plate readers holding billions of records related to vehicle locations from scanners on tow trucks, toll roads and speed-limit cameras. Agents have run facial recognition searches on people's photos to see if they match any of the millions of faces in state driver's license databases.

U.S. Customs and Border Protection officials also have used cellphone location data without warrants to track people inside the country. The data is gathered through a mix of weather, gaming and other apps, then bundled and resold by companies to marketers and federal agencies.

An inspector general for the Treasury Department said in a letter last week to Sens. Ron Wyden (D-OR) and Elizabeth Warren (D-Mass.), first reported by the Wall Street Journal, that similar uses of commercial location data by the Internal Revenue Service could conflict with a 2018 Supreme Court ruling that found such searches should require a warrant.

Lawyers for the IRS and other agencies have argued that they had not needed a warrant because phone users had "voluntarily granted access" to the data-sharing apps.