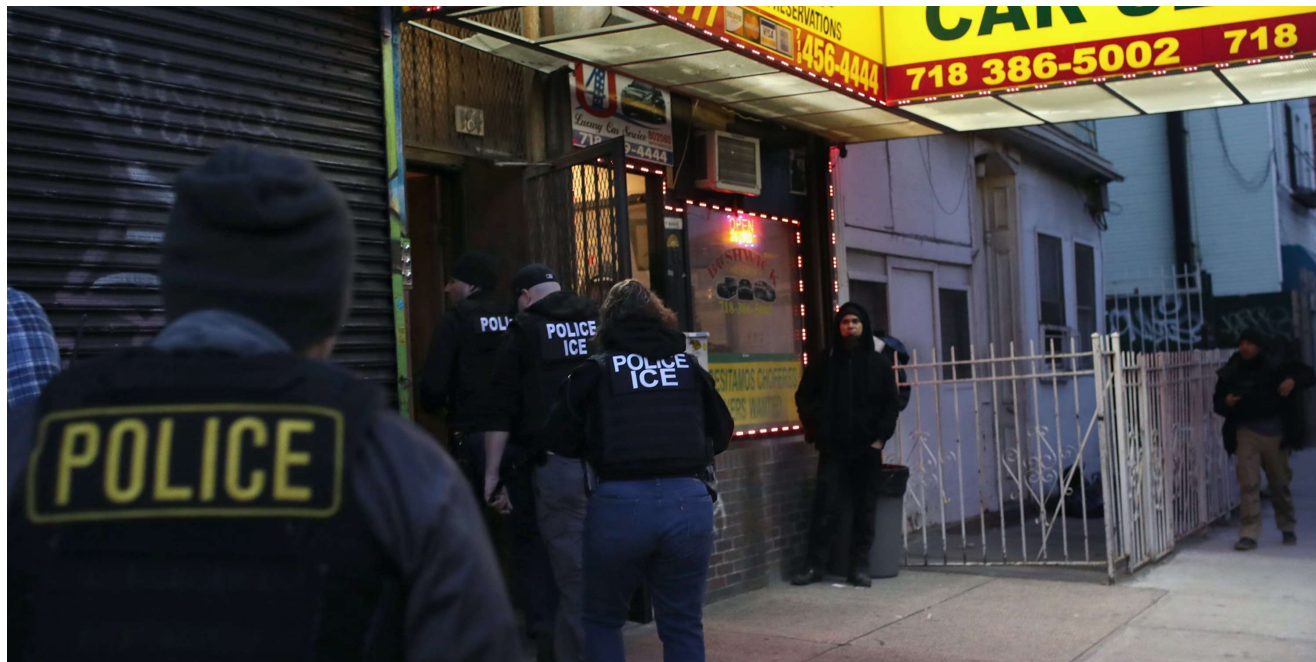


ICE Searched LexisNexis Database Over 1 Million Times in Just Seven Months

theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances

Sam Biddle



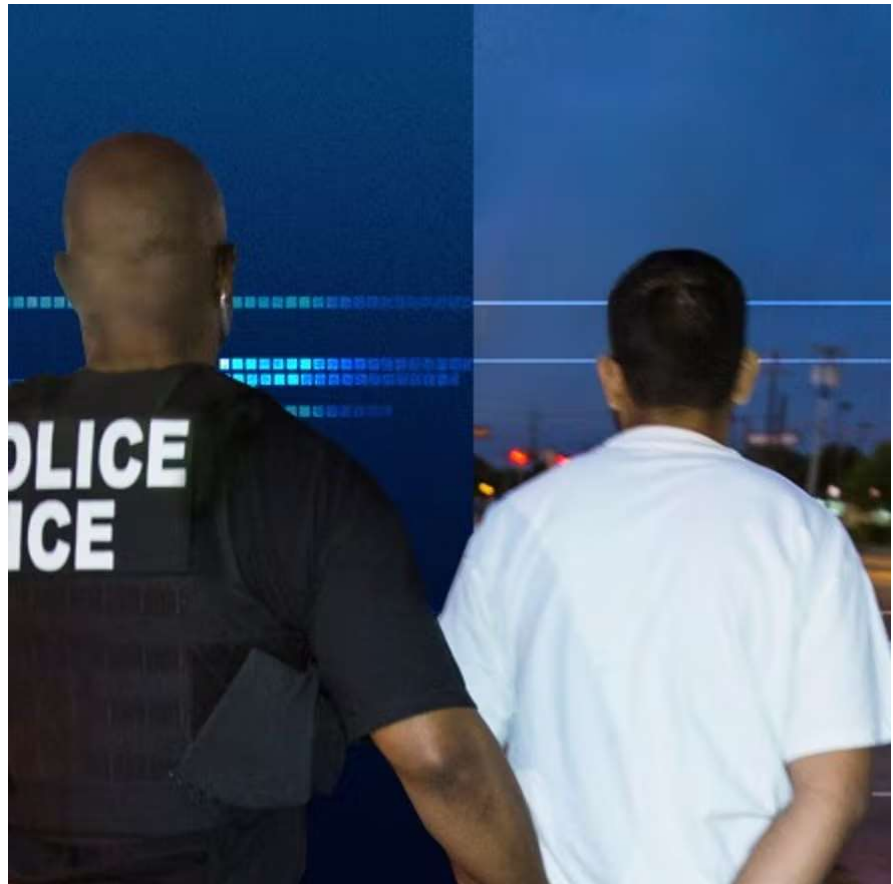
Immigration and Customs Enforcement searched a massive database of personal information provided by LexisNexis over 1.2 million times in just a seven-month period in 2021, according to documents reviewed by The Intercept. Critics say the staggering search volume confirms fears that the data broker is enabling the mass surveillance and deportation of immigrants.

The Intercept first reported last year that ICE had purchased access to LexisNexis Risk Solutions databases for \$16.8 million, unlocking an oceanic volume of personal information on American citizens and noncitizens alike that spans hundreds of millions of individuals, totaling billions of records drawn from 10,000 different sources. Becoming a LexisNexis customer not only provides law enforcement with instant, easy access to a wealth of easily searchable data points on hundreds of millions of people, but also lets them essentially purchase data rather than having to formally request it or seek a court order.

Internal documents now show that this unfathomably large quantity of data is being searched with a regularity that is itself vast. LexisNexis usage logs between March and September 2021 totaled 1,211,643 searches and 302,431 “reports,” information packages that provide an exhaustive rundown of an individual’s location, work history, family relationships, and many other data points aggregated by LexisNexis, a data broker better known for its legal research resources. Although the names were redacted, the logs show that

a single user conducted over 26,000 searches in that period.

Most of the queries were conducted through Accurint, a powerful LexisNexis tool that promises “cutting-edge analytics and data linking,” and touts its ability to provide a firehose of “investigative intelligence” to police on a national scale. “Criminals have no boundaries,” reads the Accurint homepage. “So neither can you when it comes to critical investigative intelligence and crime reporting. That’s why Accurint Virtual



Crime Center gives you visibility beyond your own jurisdictions into regional and nationwide crime data.”

The new documents, obtained by a Freedom of Information Act request by the immigrant advocacy organization Just Futures Law and shared with The Intercept, cast doubt on earlier assurances from LexisNexis that its sprawling database would be used only narrowly to target people with “serious criminal backgrounds.” In 2021, following widespread criticism of the ICE contract, LexisNexis published a brief FAQ attempting to downplay the gravity of the collaboration and dispel concerns their databases would facilitate dragnet surveillance and deportations. “The tool promotes public safety and is not used to prevent legal immigration,” reads the document, “nor is it used to remove individuals from the United States unless they pose a serious threat to public safety including child trafficking, drug smuggling and other serious criminal activity.”

However, the logs show that a sizable share of the usage — over 260,000 searches and reports — were conducted by ICE’s Enforcement and Removal Operations, a branch explicitly tasked with finding and deporting immigrants, often for minor infractions or no offense at all. An internal ERO memo obtained through the FOIA request and also shared with The Intercept contradicts the idea that Accurint’s use was to be narrowly focused on only the most dangerous criminal elements. In an email sent June 30, 2021, ERO’s assistant

director of enforcement wrote, “Please note this additional valuable resource should be widely utilized by ERO personnel as an integral part of our mission to protect the homeland through the identification, location, arrest, and removal of noncitizens who undermine the safety of our communities and the integrity of our immigration laws.” The email noted that LexisNexis would be directly providing ICE with educational seminars on how to most effectively use the data.

ICE’s long documented history of rounding up immigrants with no criminal history or those with only nonviolent offenses like traffic violations further undermines the notion that these hundreds of thousands of ERO searches all pertained to hardened, dangerous criminals. A breakdown of LexisNexis usage by individual ICE office shows that the single highest generator of searches and reports, with a total of 56,467, was ERO’s National Criminal Analysis and Targeting Center, a division tasked with locating immigrants who are merely deemed “amenable to removal,” according to agency documents. Though ICE and LexisNexis are both keen to couch these investigations as a bulwark against dangerous transnational terrorists and criminal syndicates, an analysis of 2019 ICE arrest data conducted by Syracuse University found that “exceedingly few detainees” had committed grave national security-related offenses like terrorism or election fraud, and that “the growth in detention by Immigration and Customs Enforcement (ICE) over the past four years has been fueled by a steady increase in the number of detainees with no criminal history.”

Read Our Complete Coverage The War on Immigrants

“LexisNexis is using the same type of scare tactics ICE tries to use to justify the brutality of their deportation mission,” said Just Futures Law attorney Dinesh McCoy, who worked on the FOIA request. “There’s no



indication, based on the huge number of searches conducted, nor from the records that we’ve seen, that ICE uses LexisNexis technology in a confined way to target ‘serious’ criminal activity. We know thousands of ICE employees are empowered to use this tech, and we know that officers are given significant discretion to make investigative and strategy decisions about how they locate immigrants.”

Though ICE arrests have fallen under the Biden administration, experts say they remain concerned by Accurant’s use and potential to snare people who’ve committed no crime beyond fleeing their home country. “We’re seeing a continuation of harmful surveillance

practices under this administration,” McCoy wrote via email. “We need real opposition to the constant expansion of ICE’s power and infrastructure, but by providing the agency with invasive tools like Accurint, the Biden Administration is just strengthening ICE’s institutional position for the future.” The marked decline in post-Trump ICE arrests presents an odd context for the massive scale of ICE’s searches: During roughly the same period tracked by the LexisNexis logs, ERO made 72,000 arrests after conducting over three times as many individual searches.



A Homeland Security Investigations special agent prepares to arrest alleged immigration violators at Fresh Mark meat processing plant in Salem, Ohio, on June 19, 2018.

Photo: Smith Collection/Gado/Getty Images

Over 630,000 of the searches and reports were run by Homeland Security Investigations, an ICE division tasked with investigating an expansive array of “threats,” from human trafficking and terrorism to “scams” and identity theft. But along with HSI’s broad mandate have come allegations of dragnet spy tactics and indiscriminate policing. In a letter to Homeland Security Inspector General Joseph Cuffari in March, Sen. Ron Wyden wrote that he’d learned HSI had “abused” its federal authority and “was operating an indiscriminate and bulk surveillance program that swept up millions of financial records about Americans.”

HSI also regularly assists with ERO's mass detention and deportation operations, including a 2018 workplace raid in Tennessee that separated children from their parents and left hundreds of students too afraid to return to school. In a March article for Just Security, Mary Pat Dwyer of the Brennan Center wrote that HSI "often uses its transnational crime mission to investigate immigrants of color who are not suspected of criminal activity," including investigations into naturalized citizens "looking for inconsistencies in their documents or old deportation orders as grounds to strip them of citizenship."

The logs provide a greater understanding of how ICE is making use of LexisNexis Risk Solutions, which provides a varied suite of search tools to navigate the company's voluminous store of government records and commercial data. The overwhelming majority of the searches, over 700,000 in total, were conducted using Accurint's "Advanced Person Search," which lets users enter fragments of data they might have on an individual — a relative, a former job, a nickname — and match it against a pool of millions of identities. Over 200,000 other searches were run against Accurint's database of phone provider records, more than 63,000 vehicle record searches, and nearly 10,000 different queries hunting for social media profiles. The logs also show nearly 6,000 searches for Accurint's index of jail booking activity, an ICE tactic recently reported by The Guardian as an explicit means of skirting "sanctuary city" laws that block local police from sharing such information with immigration agencies. With LexisNexis access, it is now trivial for an agency to essentially buy its way around such restrictions.

Neither ICE nor LexisNexis responded to a request for comment.

Used in concert, these searches grant ICE, an agency already charged with brutal and indiscriminate tactics against some of American society's most vulnerable members, with an immense technological advantage when seeking its targets. It's difficult to overstate the enormity of LexisNexis's databases, and equally difficult to imagine avoiding being absorbed into them. Financial records, property records, past jobs, former marriages, phone subscriptions, cable TV bills, car registrations — critics of LexisNexis's government work note that it's near impossible to exist today without leaving behind traces that are quickly vacuumed up into the company's colossal trove of public and proprietary data points, continuously indexed and rendered instantly searchable. Put in the hands of agencies like ICE, the mountains of digital paperwork one accumulates during ordinary civic and consumer lives can be easily turned against us. A 2021 report by the Washington Post found that ICE had previously tapped a database of utility records while searching for immigration offenses, leaving those who fear detention or deportation with a grim choice between the basic amenities of modern life and the perpetual risk of data broker-enabled arrest.

Despite the vastness of LexisNexis's data and the advertised sophistication of the tools it provides law enforcement to comb through that data, the company itself quietly warns that it may be providing inaccurate information, the consequences of which could upend a life or

entire family. “Due to the nature of the origin of public record information, the public records and commercially available data sources used in reports may contain errors. Source data is sometimes reported or entered inaccurately, processed poorly or incorrectly, and is generally not free from defect,” reads a small warning at the bottom of a marketing page for Accurint Virtual Crime Center, a tool used heavily by ICE according to the search logs. “Before relying on any data, it should be independently verified.”

It’s not just those individuals in ICE’s crosshairs who need to fear being implicated by a LexisNexis search. Accurint promotional and training materials make frequent mention of the software’s ability to not only locate people via the records they leave in their wake, but also trace real-life social networks, potentially drawing friends, family, neighbors, and co-workers under federal scrutiny. An Accurint training manual marked “Confidential and Proprietary” but publicly accessible via a LexisNexis website shows how users can obtain “information about a subject’s relatives, neighbors, and associates,” including “possible relative phones” two degrees removed from the target. The fact that a single search can yield results about multiple people or entire families suggests that the number of people subjected to LexisNexis-based surveillance could be far more than the already large 1.2 million figure might indicate. “We’re seeing that ICE is running a system of mass surveillance,” said Cinthya Rodriguez, a national organizer with the immigrant rights group Mijente. “What we’re really talking about is possibly upwards of three times that 1.2 million, perhaps upwards of 3 million searches happening in that period of time. ... What we’re saying is, perhaps 1 percent of the U.S. population was under ICE surveillance.”

That something as mundane as having heat or running water at home could draw the attention of the federal deportation machine, and that this machine could then turn its sights on one’s personal support network, has left immigrant communities in a state of perpetual fear, said Rodriguez. “Immigrants are forced to face impossible choices about what kind of services they need and the information they have to turn over in order to access those services, everything ranging from their electric bills to buying a car, to information about their children’s schools,” Rodriguez explained in an interview. “Everything we touch can have serious implications for building out ICE’s digital dragnet.”