12-Person Jury

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

MARIA FERNANDA CASTELLANOS RAMIREZ, ROSA CARRASCO, CLAUDIA MARCHAN TORRES, MIJENTE SUPPORT COMMITTEE, ORGANIZED COMMUNITIES AGAINST DEPORTATIONS,

Plaintiffs,

v.

LEXISNEXIS RISK SOLUTIONS,

Defendant.

Case No. 2022CH07984

JURY TRIAL DEMANDED

COMPLAINT FOR DAMAGES, DECLARATORY, AND INJUNCTIVE RELIEF

INTRODUCTION

1. LexisNexis Risk Solutions ("LexisNexis") is a multinational company that earns billions of dollars in annual revenue. LexisNexis makes much of this money by collecting and aggregating sensitive personal data from U.S. consumers, including Illinoisans, without their consent. It then sells that information to corporations, law enforcement, and government agencies, in violation of the privacy and consumer protection rights of Illinois residents.

2. LexisNexis sells consumers' data through an online platform it calls "Accurint." Accurint offers an encyclopedic summary of a person's existence; its database aggregates both public and non-public information and contains profiles on millions of people. This information includes names, addresses, emails, criminal histories, phone numbers, past jobs, former marriages, relatives, associates, motor vehicle information, bankruptcies, liens, judgements, real property records, social media information, and business and employment information. Much of this data is drawn from day-to-day consumer transactions, enabling LexisNexis' users, as

advertised in its brochures, to "locate people and discover associations," "uncover assets," "investigate businesses," and "visualize complex relationships." LexisNexis thus provides access to almost every aspect of consumers' lives.

3. LexisNexis has not just collected this data. On its website, it claims to have created 276 million "LexIDs" tied directly to individual U.S. identities. It also claims that LexIDs are 99% accurate in linking capabilities, which makes it remarkably easy to organize and use all the data collected about a person. In 2020, the U.S. Census Bureau counted 258.3 million adults, 18 years or older, living in the United States. What LexisNexis' technology really offers is a massive surveillance state with files on almost every adult U.S. consumer and more.

4. LexisNexis also markets its products to law enforcement agencies, offering information from third-party data brokers and other law enforcement agencies that are not available to the general public. This includes real-time booking information from thousands of facilities, up-to-date auto collision information, and license plate reader data. The latter can paint an intimate portrait of a driver's life, allowing Accurint customers to retrace a person's past movements and determine where they were at various points in time.

5. LexisNexis' technology poses a grave threat to civil liberties. Using Accurint, law enforcement officers can surveil and track people based on information these officers would not, in many cases, otherwise be able to obtain without a subpoena, court order, or other legal process. The officers who have access to this data include Immigration and Customs Enforcement (ICE) employees. Accurint enables ICE, which has a $22 million contract with LexisNexis, to rapidly aggregate data from millions of data points to build detailed dossiers on individuals whom it may be targeting for deportation. For example, ICE employees may use Accurint to search hundreds of millions of utility records (including cell phone, water, and

electricity records) while investigating putative immigration violations. All of this is done in the absence of warrants, subpoenas, or any court oversight. Because of these powerful tools, noncitizens who share their information while purchasing essential utilities or engaging in other common consumer transactions risk ICE enforcement action. Indeed, according to Freedom of Information Act (FOIA) records obtained by Plaintiffs, ICE used Accurint to conduct more than 1.2 million searches from March 2021 to September 2021.

6. Plaintiffs include three political activists who have, in both their personal and professional capacities, engaged in political speech critical of policing and immigration policy. Plaintiffs also include Mijente Support Committee ("Mijente") and Organized Communities Against Deportations ("OCAD"), two membership-based community organizations representing the interests of hundreds of Illinois residents, including undocumented immigrants. Accurint allows ICE, Cook County government officials, and countless other government entities to exercise enormous surveillance powers beyond the scope of what Congress and other lawmakers envisioned through the use of detailed dossiers. These dossiers include Plaintiffs' current addresses, cell phone numbers, and social security numbers, as well as private information about their relatives, neighbors, and associates. This deprives Plaintiffs (and their members) of the ability to control sensitive information about their identities and locations, placing them at significant risk of being targeted by law enforcement (and potentially others) for their political advocacy. The sharing and selling of Accurint data to private and public entities also subjects Plaintiffs to a heightened risk for identity theft, stalking, and other potential injuries.

7. Like Plaintiffs, millions of Illinoisans are harmed by LexisNexis' mass collection and sale of their data without consent or compensation. The Illinois' Consumer Fraud and Deceptive Business Practices Act (ICFA) restricts unfair business practices that offend public

policy, including the non-consensual collection and sale of consumer data. Illinois common law protects Illinoisans by prohibiting intrusion upon seclusion and unjust enrichment resulting from the capture and use of personal information without consent and compensation. LexisNexis ignores these consumer and privacy protections so it can profit from its use of personal information. Plaintiffs bring this action under Illinois Law to enjoin Defendant LexisNexis from collecting, aggregating, maintaining, and selling sensitive personal information without consent.

PARTIES

Plaintiffs

8. Plaintiff Maria Fernanda Castellanos Ramirez ("Plaintiff Castellanos") is a resident of Berwyn, Illinois, in Cook County. She is an organizer and part of the movement against deportations and the criminalization of immigrants and people of color in Chicago and surrounding areas. For over a year, Plaintiff Castellanos has coordinated healing justice initiatives while also working as a member of an anti-deportation team, where she directly supports individuals who are in deportation proceedings. Plaintiff Castellanos is an immigrant herself. She has engaged in political speech critical of the police, ICE, immigration policy, and government entities. She has active contracts for a cell phone, Internet, and cable TV and has provided her current home address as the service location for these contracts. LexisNexis has collected, used, and sold this consumer and other private information without her consent.

9. Plaintiff Rosa Carrasco ("Plaintiff Carrasco") is a resident of Chicago, Illinois. She is the Associate Director and Programs Manager at Chicago Community and Workers' Rights. Through her work and in her personal capacity, Plaintiff Carrasco advocates for immigrant justice and against deportations. She has spoken out at ICE offices on behalf of community members facing deportation, and she frequently posts about protests and other

awareness actions on her personal and organizational Facebook pages. Plaintiff Carrasco currently has a cell phone, and she purchases Internet, electricity, and gas services for her home. She has also purchased her home and registered her car. LexisNexis has collected, used, and sold Plaintiff Carrasco's consumer and other private information without her consent.

10. Plaintiff Claudia Marchan Torres ("Plaintiff Marchan") is a long-time resident of Chicago, Illinois. She is the Executive Director of Northern Illinois Justice for our Neighbors and is actively involved with the Illinois Coalition for Immigrant and Refugee Rights ("ICIRR"). Through her work and in her personal capacity, Plaintiff Marchan is a community organizer and advocates for immigrant justice. Her father endured terrible immigration detention conditions, and since then, Marchan has worked to raise awareness of detention-related issues by telling his story and speaking out at demonstrations. She also posts about immigrant justice and detention conditions on social media. Plaintiff Marchan currently purchases Internet, cable, electricity, and gas services for her home. She also currently has a mortgage on her home. LexisNexis has collected, used, and sold Plaintiff Marchan's consumer and other private information without her consent.

11. Plaintiff Mijente, an Arizona corporation, is a national digital and grassroots hub for Latinx and Chicanx movement building and organizing. It seeks to expand the profile of policy issues that matter to its communities and increase the participation of Latinx and Chicanx people in the broader movements for racial, economic, climate, and gender justice. Plaintiff Mijente organizes opposition to the mass surveillance of the immigrant community, particularly in the face of increasing technological capabilities of corporations and governments. It has a significant interest in halting data-sharing practices that result in the arrest, detention, and deportation of immigrants. Mijente has roughly 175 members in Cook County, many of whom

purchase utilities and other services from which Accurint's data tools likely collect their data. Mijente members are harmed by LexisNexis' collection, sale, and sharing of their sensitive personal information. Since many Mijente members are activists who are publicly critical of the police and government, they fear that LexisNexis' sale of their location information to law enforcement without the members' consent will make them targets for retaliation. Additionally, many Mijente members are immigrants and they fear that ICE could use non-consensually collected personal information to deport them. Mijente brings this action as an organizational representative. Mijente participates as a plaintiff only for purposes of securing declaratory and injunctive relief.

12. Plaintiff Organized Communities Against Deportations ("OCAD"), an Illinois corporation, is an immigrant justice group. It organizes as part of the movement against deportations and the criminalization of immigrants and of people of color in Chicago and surrounding areas. Through grassroots organizing, legal and policy work, direct action, education, and cross-movement building, OCAD supports its communities, builds collective power, and organizes to eliminate surveillance mechanisms. For example, it advocated for the elimination of the City of Chicago's gang database and produced the report entitled "The Digital Deportation Machine: How Surveillance Technology Undermines Chicago's Welcoming City Policy." OCAD coordinates support for its members and others in the community who face deportation or are otherwise targeted by police or ICE. OCAD has roughly 84 members in Cook County, many of whom purchase utilities and other essential services from which Accurint collects their data. LexisNexis' sale of Accurint and the data within it to ICE and other law enforcement causes substantial harm to OCAD members. OCAD members and their supporters fear the harsh consequences of arrest and deportation as a result of the up-to-date location

information ICE can, at a moment's notice, access from the Accurint platform. They not only fear for themselves, but also for identified family members, friends, and neighbors who may never have called attention to themselves or had prior contacts with ICE. They also fear misidentification and being denied opportunities—including when engaging in consumer transactions like purchasing a car or applying for a loan—due to the large swaths of inaccurate information contained in their Accurint profiles. OCAD brings this action as an organizational representative. OCAD participates as a plaintiff only for purposes of securing declaratory and injunctive relief.

13. Plaintiffs Castellanos, Carrasco, and Marchan, as well as members of Plaintiffs Mijente and OCAD did not consent to have their personal information collected, aggregated, or sold by LexisNexis. They did not understand that their personal information would be collected, aggregated, shared, or sold to private and public entities as a result of purchasing necessary utilities and services. Plaintiffs have been deprived of the economic value of their sensitive data and suffered invasions of their privacy and resulting mental distress. They also fear that they or their communities, families, and associates will be targeted for their political speech, associations, affiliations, and/or lack of immigration status.

Defendant

14. Defendant LexisNexis Risk Solutions is a multinational corporation with its headquarters in Alpharetta, Georgia.

JURISDICTION AND VENUE

15. This Court has jurisdiction over Defendant under Section 5/2-209 of the Illinois Code of Civil Procedure because Defendant is a corporation doing business within the State of Illinois (marketing and selling Accurint products to Illinois businesses and government

agencies), and because Defendant has committed tortious acts expressly aimed at Illinois residents, intentionally targeting them for the mass collection and sale of personal information without consent. According to its parent company's most recent annual report, Defendant has principal operations in Illinois. Further, Defendant regularly collects personal information about Illinois residents from Illinois service providers and government agencies, arising out of those residents' consumer transactions in Illinois.

16. Venue is proper in this Court under Section 5/2-101 of the Illinois Code of Civil Procedure because this Court is located in the county in which the transaction or some part thereof occurred out of which the cause of action arose.

FACTUAL ALLEGATIONS

I. LexisNexis's Collection and Sale of Consumer and Personal Information

17. LexisNexis collects and aggregates the private and sensitive data of hundreds of millions of individuals into searchable and detailed dossiers. It amasses these records from the most intimate corners of our lives. It then sells these exhaustive dossiers through its Accurint platform to 400,000 entities including private corporations, government agencies, and law enforcement agencies.

18. At no point during its process of collecting, aggregating, and selling an individual's information does LexisNexis inform or even try to inform the affected individual about its data-collection activities. Nor does LexisNexis attempt to obtain the individual's consent. Thus, in the vast majority of cases, consumers do not know that LexisNexis has collected their personal information and data, let alone that it is selling this information for profit.

19. In light of abuses from data broker companies like LexisNexis, in December 2021, Senator Ron Wyden wrote to the Consumer Finance Protection Bureau and advocated for more stringent oversight of these companies. He wrote, "[t]he data broker industry is out of control," adding that "selling personal information that people provide to sign up for power, water, and other necessities of life, and giving them no choice in the matter, is an egregious abuse of consumers' privacy."

A. LexisNexis draws consumers' personal and identifying information from billions of public and nonpublic records to build its Accurint database.

20. LexisNexis draws from over 34 billion "public and proprietary" records. According to the company, its "proprietary database combines data from hundreds of sources to create the most comprehensive collection of information about people in the United States."[1] While LexisNexis has revealed that it pulls from both public and non-public information to build its colossal trove of Accurint data, the company has not shared a comprehensive list of sources.

21. Public information about individuals is derived from public records such as voter registration rolls, property records, and motor vehicle registrations, as well as other public sources such as newspapers, magazine articles, and telephone directories. Non-public information comes from privately-owned sources and is unavailable to the general public, including utility accounts and cell phone records. According to LexisNexis, non-public information may include current and previous addresses, social security numbers, previously-used names (e.g., aliases, maiden names, or previous married names), birth dates, and/or telephone numbers.

[1] *Locating People Using Advanced Person Search*, Accurint, http://www.accurint.com/help/bps/v3/le/advanced_person_help.html [hereinafter *Locating People*].

22. With respect to public-record information, LexisNexis advertises its ability to search and analyze massive amounts of data that users (including law enforcement) cannot access on their own. For example, Accurint contains real-time motor vehicle registration search data, drawing from state DMV records. Accurint also contains real-time phone search data, which draws from a variety of public and non-public data, "including consumer bureaus, nationwide telephone companies, and phone networks like North American Numbering Plan, which includes the United States, all US territories (except Guam), and Canada address and name-change data from credit reports and to motor-vehicle registrations from 43 U.S. states plus the District of Columbia and Puerto Rico."[2] LexisNexis further claims that its data sources are updated instantaneously or "as often as every 15 minutes."

23. Non-public information that LexisNexis discloses also includes utility data and draws from the following categories of utilities and services: coal, electric, gas, oil, propane gas, water, paging, long distance calls, local phones, cellular phones, personal communication services, line leasing, Internet, satellite, cable TV, and cable equipment services.

24. On its website, Accurint also advertises its ability to map subjects' familial, social, and communal lives, as well as associational networks. A single search therefore has the potential to subject friends, family members, neighbors, and co-workers to scrutiny. The data for possible "relatives" and "associates" may include names and addresses, other residents at the address, phone numbers, social security numbers, and dates of birth. A subject's personal data, thus, could disturbingly be used for the purposes of locating their spouse or parent.

[2] *Real-Time Phones Search*, Accurint, https://www.accurint.com/help/bps/pdf/real_time_phone_help.pdf.

25. Additionally, LexisNexis advertises its ability to search for an individual and identify whether someone is on active-duty military. There is virtually nothing in U.S. law preventing LexisNexis from selling such information to foreign entities.

26. Accurint data reports about specific individuals are sometimes erroneous. For example, when LexisNexis does not have—or does not use—enough information about an individual when running a search, it can mistakenly use data pulled from multiple people in a single person's report. This can happen when the subject of a report has the same name as other subjects, thus confusing the LexisNexis data algorithms. This type of mistake has been documented. When these mistakes are made, misidentified individuals can be wrongly denied government benefits or be mistakenly identified as suspects in law enforcement investigations.[3] Because of the potential for such "errors and omissions" to result in lawsuits, in one instance, LexisNexis furnished a million-dollar insurance policy to cover the City of Denver and its officials, employees and volunteers in its use of LexisNexis data.

B. Through Accurint, LexisNexis sells the ability to easily and quickly search for a specific individual's personal and non-public information.

27. On its website, LexisNexis advertises Accurint as "the most widely accepted locate-and-research tool available to government, law enforcement and commercial customers...return[ing] search results in seconds to the user's desktop."

28. Accurint offers users the ability to conduct numerous types of searches for a targeted individual or entity, including a "Person Search" and "Advanced Person Search." According to LexisNexis, an Advanced Person Search "helps find individuals when only old or

[3] Sarah Mancini, Kate Lang & Chi Wu, *Mismatched and Mistaken: How the Use of an Inaccurate Private Database Results in SSI Recipients Unjustly Losing Benefits*, National Consumer Law Center (Apr. 2021), https://justiceinaging.org/wp-content/uploads/2021/04/SSADataReport.pdf.

fragmented data is available." It is a widely used function; for example, according to FOIA records obtained by Plaintiffs, it was the most used Accurint search function by ICE in 2021.

29. When a user conducts an Advanced Person Search, Accurint prompts that person to enter information such as an individual's name, address, social security number, or date of birth in order to locate a targeted individual. It also provides alternative search fields, including driver license number, driver license state, other state, other last name, other city, relative first name, and other relative first name.

30. The Advanced Person Search results bring the user to a landing page with personal identifying information. The page may include the target individual's full name, date of birth, age, gender, social security number, LexID, current address (along with the dates during which the individual resided at that address), prior addresses, and phone numbers (with the carrier name, location, and dates during which the individual used that number).[4]

31. The landing page also displays an "Indicators" column, which links to other data including Criminal Records, Motor Vehicles, Sexual Offenders, Concealed Weapons Permit, Property, and People at Work. Clicking on an indicator icon returns the relevant information. For example, if one clicks the "Motor Vehicles" icon, the results page will be filled with the subject's vehicle registration information. Or, if one clicks the "People at Work" icon, the search results will return the subject's place of employment and relevant address information.

32. The Advanced Person Search results page also features a "Further Research" panel, allowing a user to dive deeper into the targeted individual's profile. Selecting any data point (e.g., name, address, etc.) will automatically update the Further Research panel with links

[4] *Locating People*, *supra* note 1.

to additional searches that can be run. Also, if "a subject has any derogatory photos on file, those images are displayed in the Further Research panel."[5]

33. Users may also run more than thirty other types of searches on the subject and create several reports from the results of the Advanced Person Search, including a "Comprehensive Report" which purportedly "covers every aspect of the subject." It includes detailed information not only about the targeted individual, but also about that person's relatives, associates, neighbors, addresses, properties, vehicles, and businesses.

C. LexisNexis makes substantial profits from its sale of consumers' personal and identifying information through Accurint.

34. LexisNexis makes significant profits from the collection, aggregation, and sale of individuals' identities, identifying information, and personal data through its Accurint products.

35. LexisNexis charges users for each component of Accurint's search functions. It offers both flat rate and "pay-as-you-go" pricing models, with a minimum contract term of twelve months. LexisNexis also offers tailored subscription plans for law enforcement, government agencies, law firms, private investigators, insurers, healthcare organizations, and collections agencies, respectively.

36. Under Accurint's "pay-as-you-go" pricing models, a customer can choose to pay the lowest minimum monthly subscription fee and pay full price for each individual search. Alternatively, a customer could choose to pay higher levels of minimum monthly payments resulting in a commensurate discount on individual searches and reports. These pricing models demonstrate that the individual profiles in Accurint's database have concrete economic value.

[5] *Locating People*, *supra* note 1.

37. Using Accurint's "pay-as-you-go" pricing model, users pay for each component of a search and per report. Under one pricing schedule, LexisNexis charges $6.87 for a basic Person Search, with additional fees added for bankruptcy information and records. According to this schedule, users can pay for 58 different types of searches and reports, with the costs running from $8.00 for a "Social Media Locator" to $10.50 for "Phone Finder Ultimate" to $12.93 for a basic "Address Report." In many cases, users must also pay additional fees to generate reports from their searches. For example, a "basic report" for a person costs $13.73, with additional charges added respectively for "associates" or "relatives" data. In further customizing a basic report, a user may add on twenty other buckets of data, each with its own additional charge.

38. According to its parent company's annual report, LexisNexis Risk Solutions earned more than $2 billion in revenues in 2021. On information and belief, the sale of Defendant's Accurint products to private and public entities accounts for a significant percentage of those revenues.

II. Use of Accurint by ICE and Other Government Entities

39. According to LexisNexis' brochure, over 4,000 federal, state, and local law enforcement agencies have used Accurint technology.

40. Cook County government officials have access to Accurint and, according to their contract with LexisNexis, use it for purposes including location of persons and businesses, skip-tracing, address searches, bankruptcy checks for individuals and companies, driving records, associated persons and businesses, property ownership records, and public records (e.g., UCC records, liens, judgments, property records, lawsuit, or adverse filings, etc.).

41. In its website brochure, LexisNexis touts its ability to provide a vast source of "investigative intelligence" to police on a national scale. "Criminals have no boundaries," reads

the Accurint brochure, "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."

42. LexisNexis offers its services to law enforcement customers through several contractual models. Some service packages are offered on a per-user basis, and others are billed per search or use of the specific Accurint tool.

43. Law enforcement personnel who use Accurint are also able to access real-time incarceration and arrest records, including over 140 million booking records and 38 million offender images from more than 2,000 law enforcement databases nationwide. Local booking data is available from facilities in 43 states plus D.C., and state departments of corrections data is available from 27 states.

44. The terms and conditions for law enforcement users may stipulate that in exchange for access to the Accurint platform, local law enforcement agencies must submit their own agency data to the LexisNexis Public Safety Data Exchange so that other law enforcement customers may access it.

45. The contracts may also restrict customers from naming LexisNexis or referencing use of its products in press releases or in any third-party disclosures.

46. On February 25, 2021, LexisNexis entered into contracts with ICE to provide Accurint and potentially other database services. The contracts are valued at $22.1 million.

47. Plaintiffs' concerns about being targeted and misidentified due to ICE's use of Accurint are not abstract. According to documents produced by ICE in response to a FOIA request, ICE ran over 1.2 million searches and generated over 300,000 reports through Accurint from March 2021 through Sept. 2021. Thousands of these searches were run by the Chicago ICE

Field Office. Potential ICE uses of data broker technology include determining immigration status, determining current home address or location in order to conduct raids/arrests, and learning about immigrants' families through their associations. Upon information and belief, ICE has used Accurint for each of these purposes, and more.

48. Through Accurint, ICE also has access to Illinois driver license data. Indeed, in 2021, LexisNexis purchased over $20 million of data from the Illinois Department of Driver Services. Those records include name and address information, drivers' physical characteristics, and the type of license issued (for example, a Temporary Visitor Driver's License (TVDL)). Under Illinois law, a TVDL is available only to certain groups of immigrants, including undocumented immigrants. Access to this license data allows ICE to target Illinois drivers based on immigration status.

49. According to the FOIA records, in June 2021, ICE's Enforcement and Removal Operations (ERO) directorate stated that it had "available resources to bring over 4,200 users onto Accurint." LexisNexis' Education team offered ICE ERO employees training sessions related to the use of Accurint, and how to use the data most effectively.

50. In the contracting document related to its procurement of Accurint, ICE's Targeting Operations Division specified that the data service must allow ICE to "track daily address changes and credit activities of targeted persons" by providing access to data from sources including but not limited to the following:

a. Insurance
b. Phone
c. Employment
d. Utilities
e. Renter Information
f. Licenses

g. Credit Checks

51. Additionally, in the contracting document, ICE explained that it was expanding its contract with LexisNexis to obtain jail information that is restricted by sanctuary policies across the country: "Due to policy or legislative changes, [ICE] has experienced an increase in the number of law enforcement agencies and state or local governments that do not share information about real time incarceration of foreign-born nationals with ICE. Therefore, it is critical to have access to Justice Intelligence."

52. Justice Intelligence is a secure web portal that provides real-time jail incarceration data from hundreds of local jails and prisons across the country, including Illinois. This portal gives ICE agents real time alerts when people that it has targeted are booked into county jails, allowing the agency to identify and apprehend them upon their release. In ICE's contract with LexisNexis, the portal can be accessed by ICE only as an "add-on feature."

53. Pursuant to sanctuary laws and policies within the State of Illinois, including the Illinois TRUST Act, Cook County's Detainer Ordinance, and Chicago's Welcoming City Ordinance, law enforcement agencies in the state and county are required to deny ICE's requests to detain immigrants ("detainer requests"). For example, in the last year alone, Cook County law enforcement agencies rejected more than 1,000 detainer requests from ICE. When localities refuse to execute detainers, LexisNexis Justice Intelligence add-on serves as a backdoor, allowing ICE to obtain the real-time incarceration data necessary to identify and arrest immigrants as they are being released, and to thereby evade state and local policies designed to protect such information.

54. LexisNexis' efforts to help ICE circumvent state and local laws have raised serious concerns among the local officials responsible for enforcing those laws. For example, in April 2022, Cook County Commissioner Alma E. Anaya introduced a resolution to investigate

and take action against these practices as potential violations of local and state sanctuary laws and policies. On July 27, 2022, the Board of County Commissioners held a public hearing on the issue.

55. LexisNexis' data sharing with ICE and other government agencies is contrary to the Illinois TRUST Act and other local sanctuary policies intended to protect the privacy and civil rights of immigrant communities. Law enforcement surveillance and deployment against individuals based on aggregation of private data offends constitutional and basic notions of justice, equity, and good conscience. Participation in basic consumer behaviors should be free from suspicion and leave no question that such behaviors will not be used against the individual.

III. ICE's Abuse of Data to Illegally and Erroneously Target People

56. LexisNexis' collection, aggregation, and sale of personal data is unlawful under Illinois law regardless of how that data is subsequently utilized by the customer, but its contract with ICE is particularly troubling in light of ICE's history of misusing data against vulnerable populations. Since 2015, for example, ICE has performed thousands of faceprint searches on state DMV databases to identify, locate, and deport individuals. ICE has conducted these searches in at least three states that allow undocumented immigrants to obtain a license or driver privilege card. ICE runs these searches without notice to the license holders and without a warrant or any other official approval.

57. A unit of ICE was investigated for abusing its authority by operating "an indiscriminate and bulk surveillance program that swept up millions of financial records about Americans."[6] From 2019 to 2022, the agency unlawfully used its subpoena power to obtain approximately six million records involving money transfers to and from the border states of

[6] Letter from Senator Wyden to DHS Inspector General Joseph V. Cuffari (Mar. 8, 2022), https://www.wyden.senate.gov/imo/media/doc/DHS%20IG%20ICE_HSI%20data%20complaint%20final.pdf.

California, Texas, Arizona, and New Mexico. That information, which may have included the names, addresses, social security numbers, and identification numbers of senders, as well as the names and addresses of recipients was then sent to a database accessible by local and federal law enforcement, without any kind of court supervision.

58. ICE has also systematically surveilled, detained, and deported immigrant activists who publicly criticize immigration policies and practices.[7] For example, ICE has targeted Maru Mora-Villalpando, a member of both La Resistencia and Mijente, for her "anti-ICE protests." Ravi Ragbir was arrested at his ICE check-in meeting, after participating in protests that ICE characterized as an unwanted "display of wailing kids and wailing clergy." Daniela Vargas was arrested as she left a press conference supporting the DACA program. In response, a number of immigrant rights groups and immigrants have sued ICE for violating their First Amendment rights to speak, assemble, and associate.[8]

59. In light of that abuse, Accurint's partnership with ICE also poses a grave threat to First Amendment speech and association rights and chills Plaintiffs and others from participating in constitutionally-protected activity.

---

[7] Nick Pinto, *Across the U.S., Trump Used Ice to Crack Down on Immigration Activists*, The Intercept (June 17, 2021) (reporting on a law school-generated searchable map documenting a thousand examples of retaliatory actions against immigration activists by ICE, including several in Illinois), https://theintercept.com/2020/11/01/ice-immigration-activists-map/; Joel Rose, *Immigrant Activists Say ICE is Purposely Targeting Them. They're Urging Biden to Help*, NPR (Aug. 4, 2021) (describing a report prepared by the University of Washington School of Law documenting instances of ICE retaliation against immigrant activists nationwide), https://www.npr.org/2021/08/04/1024348198/immigrant-activists-ask-biden-administration-to-ban-ice-from-retaliating-against.

[8] *See, e.g.*, First Amended Complaint, *Migrant Just. v. Nielsen*, No. 5:18-cv-192 (D. Vt. Feb. 7, 2019) (alleging that after Plaintiff farmworker organization successfully campaigned for state driver's licenses for undocumented immigrants, ICE subsequently planted a civilian informant within the organization, and proceeded to arrest and detain, and in some cases deport, nearly two dozen Migrant Justice members); First Amended Complaint, *NWDC Resistance v. ICE*, No. C18-5860 (W.D. Wash. Dec. 20, 2019) (alleging a nationwide pattern and practice of ICE retaliation against immigrant activists engaging in protected political speech).

60. ICE also has a long history of using incomplete government records, biased data, and lax investigations to repeatedly target individuals for deportation by mistake. Indeed, ICE has unlawfully and mistakenly arrested hundreds of U.S. citizens in the last decade, holding them in detention centers for days, months, and, in some cases, years, even after some of these individuals presented their U.S. passports.[9]

61. Accurint allows ICE to conduct arbitrary digital searches of Plaintiffs, their members, and other Illinois residents, instantly accessing their sensitive personal data without privacy safeguards, warrants, or a showing of reasonableness. Further, inaccuracies plaguing the technology increase the risk of misidentification.

62. Given ICE's record of misusing data to target immigrant communities and protestors illegally and erroneously, Plaintiffs reasonably fear that ICE will indiscriminately use Accurint's database to target them, their organizational members, and their communities.

IV. Defendant Violates Plaintiffs' Rights

Individual Plaintiffs

63. LexisNexis has collected, stored, aggregated, and sold Plaintiffs Castellanos', Carrasco's, and Marchan's sensitive personal data in direct violation of the laws identified in this complaint.

64. Much of this personal and sensitive data has been collected and aggregated by LexisNexis directly from Plaintiffs' consumer transactions in Illinois.

[9] Paige St. John & Joel Rubin, *Must Reads: ICE held an American man in custody for 1,273 days. He's not the only one who's had to prove his citizenship*, L.A. Times (Apr. 27, 2018), https://www.latimes.com/local/lanow/la-me-citizens-ice-20180427-htmlstory.html.

65. LexisNexis never asked Individual Plaintiffs for their consent to sell, nor has it offered them compensation for selling, their personal information. Individual Plaintiffs have never agreed to permit LexisNexis to collect, store, or sell their personal information.

66. Nevertheless, LexisNexis sells access to its database containing Individual Plaintiffs' sensitive personal data to private and public entities for commercial gain. Accurint's "Comprehensive Report," for example, contains extensive information about each of the Individual Plaintiffs, some of which is private and not publicly available. This information includes a Social Security number that may or may not be partially redacted, current address, prior addresses, cell phone number, and details about one's current employers, licenses, and arrests. (The reports do not indicate that those arrests occurred in the context of civil disobedience.) The reports also identify Plaintiffs' neighbors, relatives, and "associates"—both current and past—and provide detailed information about them.

67. Plaintiff Castellanos purchases various utilities, including cell phone, cable, and Internet services. She takes steps to protect her data and private information by, for example, selecting paperless bills and setting up two-factor authentication for account access. Despite her wishes and her taking these measures, her dossier includes non-publicly available and private information associated with her accounts, including her present and prior addresses, phone number, and date of birth. The dossier also associates her with a former romantic partner, whom she has not seen in eleven years. She does not want to see or be affiliated with him. Furthermore, some of the information about her is inaccurate. For example, Plaintiff Castellanos' profile lists the wrong Social Security number, causing her to fear criminal allegations that she fraudulently used another's Social Security number. The profile also lists as "associates" several people she does not know or want to be associated with.

68. Plaintiff Carrasco currently owns a home and a cell phone. She purchases Internet, electricity, and gas services for her home. She has also registered her car. Because she wants to protect her personal and sensitive data, she takes security measures to protect those accounts by using online bill pay, shredding her bills, and using two-factor authentication for account access. Upon information and belief, the non-publicly available and private information in her dossier, including her present and prior addresses, social security number, phone number, and date of birth were taken from these utility accounts. Her cell phone accounts, which are private and non-publicly available information, are specifically listed in the dossier. Even more concerning is the inclusion of her full social security number. Furthermore, her dossier mischaracterizes her work experience and includes inaccurate information about one of her family member's date of birth.

69. Plaintiff Marchan currently has a mortgage on her home. She purchases various utilities, including gas, electric, cable, and Internet services for her home. She also takes steps to protect her data and private information. For example, after reviewing and paying her utility bills, she or other family members shred the bill statements so that no one will be able to access her data. This safeguard became especially important after her purse was stolen in late 2019. Using her identity documents and cards, someone began making transactions from her bank account. After her account was zeroed out, she called the police and filed a police report. Since that experience, Plaintiff Marchan has become more concerned about the protection of her data. For example, she will not give out her full social security number and will only provide the last four digits when prompted by service providers. Despite her wishes and despite these measures, her dossier includes non-publicly available and private information associated with her utility and service accounts, including her present and prior addresses, phone number, email address,

and date of birth. Even more concerning is the inclusion of her full Social Security number with no redactions, which she fears could be misused, especially given her prior experience. The sheer amount of information collected about Plaintiff Marchan causes her anxiety, particularly as someone who until recently lacked lawful immigration status.

70. This is an all-encompassing invasion of the individual Plaintiffs' privacy, as they are the owners of the information that LexisNexis collects, they have in many instances tried to keep this information private, and they have a reasonable expectation of privacy regarding this information. Defendant's collection of this personal data is cause for grave concern and highly offensive. There is a critical difference between the gathering of bits of personal information through publicly available resources (the Internet, court files, archives, etc.) and the collection of information through an encyclopedic dossier that compiles all the records, including ones that are *not* publicly available, into one easily accessible and computerized profile. That is, of course, why Accurint customers pay for access to these LexisNexis' dossiers.

71. Plaintiffs are immigrant activists who have exercised their constitutionally-protected right to publicly criticize the police, ICE, and immigration policy. The ability to protect their own identifying information–-as well as that of their families and their associates–-and to continue to exercise their right to free speech, free from the threat of clandestine and invasive surveillance and tracking of their locations, is vitally important. They do not want their information to be available to any stranger who is willing to pay for it.

Organizational Plaintiffs

72. Plaintiffs Mijente's and OCAD's members, like millions of other Illinois residents, have engaged in common consumer transactions from which LexisNexis captures sensitive private and personal data to create searchable dossiers. These transactions include the

purchase of essential services, including utilities, cell phones, driver's licenses, and car registrations, as well as the purchase of real property and motor vehicles. Upon information and belief, LexisNexis has captured the sensitive personal data of Plaintiffs Mijente's and OCAD's members. The sheer number of individuals whose personal information LexisNexis has captured—276 million in the United States—makes it a near certainty that anyone who has a consumer footprint in the United States is included in the searchable dossiers of LexisNexis' "locate-and-research tool."

73. Confidential Member 1 is a resident of Cook County and an active member of Mijente. Confidential Member 1 is also an immigrant. Through their work and in their personal capacity, they support workers who organize in the workplace and promote the development of worker cooperatives. They have been involved in the fight for the rights of workers and immigrants for more than twenty years. Over the years, they have advocated for immigrant justice and taken part in demonstrations against deportations and worker exploitation. Confidential Member 1 currently has a cell phone account. They have also purchased their home. LexisNexis has collected, stored, and aggregated their sensitive personal data into a searchable dossier. Confidential Member 1 has never given LexisNexis consent to do so. LexisNexis' aggregation of their private and sensitive data into an all-encompassing dossier for commercial sale has caused Confidential Member 1 to suffer an invasion of privacy and mental distress. Of particular concern to Confidential Member 1 is the detailed data on their daughters and their daughters' romantic partners and how that could be misused.

74. Similarly, Confidential Member 2 is a resident of Cook County and an active member of OCAD. They support other OCAD members and their families by participating in vigils for members who do not receive immigration bonds and by joining others in packing the

court at members' hearings. Confidential Member 2 purchases electricity services for their home. They take steps to protect their data and private information. For example, they do not disclose their social security number and have only revealed it when necessary—for example, to their bank and for their tax returns. As an additional security measure, they elect to receive paperless invoices for the electric bills and keep those secure in their electronic files. Despite these measures, LexisNexis has collected, stored, and aggregated their sensitive personal data, including private and non-publicly available information into a searchable dossier. This includes an unredacted social security number, date of birth, and "possible utility information," which includes the service address and phone number. Confidential Member 2 has never given LexisNexis consent to collect this information. LexisNexis' aggregation of Confidential Member 2's private and sensitive data into an all-encompassing dossier for commercial sale has caused Plaintiff to suffer an invasion of privacy and mental distress. Confidential Member 2 is particularly concerned that their profile includes an unredacted social security number, leaving them exposed to identity theft. This concern is exacerbated by the fact that Confidential Member 2 was the victim of a robbery earlier this year, and their identification documents were stolen.

75. Through its unauthorized collection, storage, aggregation, and sale of Plaintiffs' sensitive personal data, LexisNexis infringes on Plaintiffs' legitimate interests in data security and the ownership and control of their identities and personal data. LexisNexis deprives Plaintiffs of the economic value of their sensitive information. Additionally, the unauthorized collection and aggregation of Plaintiffs' sensitive personal data has caused them mental anguish and suffering over the safety of their personal and sensitive data.

76. Because LexisNexis sells its Accurint products to thousands of law enforcement entities and ICE, Plaintiffs have suffered additional mental distress. They are concerned that,

because they have publicly criticized the police and immigration policies, they will be subject to retaliation for exercising their constitutionally-protected right to free speech. They fear surveillance and the tracking of their immigrant communities. As immigrants themselves, some of whom are undocumented, they fear being indiscriminately and erroneously targeted for arrest and deportation.

77. LexisNexis provides only limited opt-out measures to those whose records it has collected, aggregated, and sold. LexisNexis will only consider (but not necessarily approve) an individual's request to opt-out of having personal information about themselves made available through LexisNexis' products if they can provide written documentation confirming they are victims of identity theft or are facing a substantial risk of physical harm. Even if LexisNexis agrees to suppress an individual's personal data, it will only do so for certain products—that is, it will in no instance suppress personal data from (a) databases used by law enforcement customers or from products containing information regulated by the Fair Credit Reporting Act (except as required by law), (b) third party data available through real time gateway, (c) news outlets, and (d) legal documents.

78. LexisNexis will continue to capture Individual Plaintiffs' and Organizational Plaintiffs' members' data in the future as its Accurint product has real-time data searching capabilities and its data sources are updated regularly, and sometimes as often as every fifteen minutes.

79. Each day that LexisNexis is allowed to continue its illegal activities, Plaintiffs suffer immediate and irreparable injuries, including the chilling of their core constitutional rights of freedom of association and freedom of speech, violations of their rights to privacy,

deprivations of the economic value of their own personal data, and injuries to their peace of mind and well-being.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
Consumer Fraud and Deceptive Business Practice Act, 815 ILCS 505, Injunctive and Monetary Relief (On behalf of Organizational and Individual Plaintiffs)

80. Plaintiffs repeat and incorporate by reference each preceding paragraph as if fully stated herein.

81. The Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/2 ("ICFA"), prohibits any unlawful, unfair, or fraudulent business acts or practices.

82. Defendant is a "person" as defined by 815 ILCS § 505/1(c).

83. By collecting, aggregating, using, and selling Plaintiffs' personal information to private and public entities without consent and compensation, as described above, LexisNexis has engaged in unfair acts and practices prohibited by the ICFA.

84. LexisNexis' practices constitute unfair business practices under the ICFA because these practices offend established Illinois and local public policy protecting personal information and consumer data, as well as the Illinois TRUST Act and local county and city sanctuary policies, which protect the civil and privacy rights of immigrant communities; are otherwise immoral, unethical, oppressive, unscrupulous; and cause substantial injury to Plaintiffs.

85. LexisNexis knowingly collected and aggregated—and continues to collect and aggregate—Plaintiffs' sensitive identifying information for the purpose of selling access to products linked to the Accurint database. LexisNexis' use of this information is central to its Accurint products.

86. At no time has LexisNexis affirmatively sought consent from Plaintiffs before collecting, aggregating, and selling their personal data, nor does it have a process for doing so.

87. Plaintiffs received no compensation for LexisNexis' use of their personal identifying information and data.

88. Defendant's practice of using and selling Plaintiffs' data without their consent and without giving them an opportunity to opt-out entirely of its Accurint products is oppressive because it "leaves the consumer with little choice except to submit to it." *Newman v. Metropolitan Life Insurance Co.*, 885 F.3d 992, 1002-03 (7th Cir. 2018).

89. Defendants know their practices are unfair to Illinois consumers because they neither provide them with any notice that they are collecting and selling their private and sensitive data, nor any choice to opt-out entirely of their Accurint products.

90. LexisNexis' unfair conduct occurred in the course of marketing, distributing, and selling its Accurint products to corporations, government agencies, and law enforcement agencies in the state of Illinois. Therefore, these activities were performed in the conduct of trade and commerce.

91. Much of Plaintiffs' personal and sensitive data has been collected, aggregated, and used by LexisNexis as a direct result of Plaintiffs' consumer transactions in Illinois. Such transactions include their purchases of cell phone, Internet, and cable services, utility services, driver's licenses, auto registrations, and homes or property. Therefore, they are "consumers" as defined under section 505/1(e) of the ICFA. Alternatively, Defendant's unfair business practices have a consumer nexus because they address the general public (including the consumers of its Accurint product). The sheer volume of identities that LexisNexis has captured—276 million in the United States—makes it a near certainty that anyone who has a consumer footprint in the

United States is included in Defendant's searchable dossiers. Further, consumer protection concerns are inherently implicated in the sale of a database that aggregates both public and non-public *consumer* information about hundreds of millions of people from credit agencies, DMV records, cellphone registries, property records, and utility accounts, among many other sources.

92. The Plaintiffs were injured and have suffered damages as a direct and proximate result of Defendant's unfair acts and practices.

93. As a result of LexisNexis' unfair business practices, Plaintiffs lost money. Plaintiffs' personal data has economic value. But for its violation of law, LexisNexis would have either paid Plaintiffs for consent to sell their information or ceased the sale of their information. By selling their data, LexisNexis has deprived them of the economic value of their sensitive information.

94. Further, Plaintiffs have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, mental anguish, loss of privacy, threats to public safety, and other economic and non-economic losses.

95. Plaintiffs seek all monetary and non-monetary relief allowed by law.

SECOND CAUSE OF ACTION
Unjust Enrichment (On behalf of Individual Plaintiffs)

96. Plaintiffs repeat and incorporate by reference each preceding paragraph as if fully stated herein.

97. Defendant LexisNexis obtained a monetary benefit from Plaintiffs to their detriment. LexisNexis did so by using and profiting from the collection and aggregation of the Plaintiffs' personal and sensitive data without their consent and without providing them any compensation.

98. Plaintiffs did not authorize LexisNexis to collect, aggregate, store, and sell or otherwise profit off their personal data.

99. LexisNexis appreciated, accepted, and retained the benefit bestowed upon them under inequitable and unjust circumstances arising from LexisNexis' conduct toward Plaintiffs described in this complaint.

100. By engaging in the conduct described in this complaint, LexisNexis has been unjustly enriched at the expense of the Plaintiffs, and the company has unjustly retained the benefits of its unlawful and wrongful conduct.

101. Under the circumstances, it would be inequitable and unjust for LexisNexis to be permitted to retain any of the unlawful proceeds resulting from its unlawful and wrongful conduct.

102. The Plaintiffs accordingly are entitled to equitable relief, including restitution and disgorgement of all revenues, earnings, and profits that LexisNexis obtained as a result of its unlawful and wrongful conduct.

THIRD CAUSE OF ACTION
Intrusion Upon Seclusion (On behalf of Individual Plaintiffs)

103. Plaintiffs repeat and incorporate by reference each preceding paragraph as if fully stated herein.

104. Plaintiffs have a reasonable expectation of privacy in their personal and sensitive data, including non-public data. They can reasonably expect that this information will not be compiled into an encyclopedic dossier, easily accessible and available to anyone willing to pay.

105. LexisNexis intentionally intruded on the seclusion of Plaintiffs by collecting, storing, aggregating, and selling their sensitive personal and private data to private and public entities without notice or consent for commercial purposes.

106. LexisNexis' misuse of personal information reveals private facts over which a reasonable person would expect privacy. It maintains, sells, and advertises a surveillance database using records that reveal intimate details about subjects' private lives, including family history, current addresses, phone numbers associated with non-public utility accounts, unredacted social security numbers, biographical details, as well as erroneous information that is misleading and/or embarrassing. The collection and aggregation of this information that Plaintiffs are trying to protect and keep private is highly offensive to a reasonable person because it is an all-encompassing invasion of their privacy. The ease of access to this private data for law enforcement surveillance and deployment against individuals is also highly offensive as it upsets constitutional and basic notions of justice, equity, and good conscience where participation in basic consumer behaviors should be free from suspicion that those behaviors will be used against the individual.

107. LexisNexis' intrusion upon the Plaintiffs' seclusion caused Plaintiffs mental anguish and suffering in the form of anxiety and concern for the safety of their personal and sensitive data.

FOURTH CAUSE OF ACTION
Declaratory Relief (On behalf of Organizational and Individual Plaintiffs)

108. Plaintiffs repeat and incorporate by reference each preceding paragraph as if fully stated herein and reallege claims in the first cause of action for purposes of this action.

109. Pursuant to 735 ILCS 5/2-701, this Court "may make binding declarations of rights, having the force of final judgments . . . including the determination . . . of the construction

of any statute, municipal ordinance, or other governmental regulation . . . and a declaration of the rights of the parties interested."

110. Such a declaration of rights "may be obtained . . . as incident to or part of a complaint . . . seeking other relief as well." 735 ILCS 5/2-701(b).

111. As described above, this Court has jurisdiction over this matter, and therefore may declare the rights of Plaintiffs.

112. Organizational and Individual Plaintiffs seek a judgment declaring that Defendant has violated their rights under the ICFA and Illinois common law.

PRAYER FOR RELIEF

For all of these reasons, Plaintiffs request that this Court grant the following relief:

a. An order declaring that Defendant's actions, as set out above, constitute a violation of the ICFA, Intrusion upon Seclusion, and unjust enrichment;

b. An order for injunctive relief, enjoining Defendant from collecting, aggregating, and selling Plaintiffs' (and members of Plaintiff organizations') personal data without their consent;

c. An award of actual damages;

d. An award of punitive damages;

e. Restitution and disgorgement of the defendant's profits from its unlawful and unfair business practices and conduct;

f. An award and judgment granting costs and reasonable attorneys' fees; and

g. Such other and further relief that the Court deems reasonable and just.

JURY DEMAND

Plaintiffs demand a trial by jury for all issues so triable under the law.

Dated: August 16, 2022

Respectfully submitted,

/s/ Daniel Schneider
One of the Plaintiffs' Attorneys

Sejal R. Zota*
sejal@justfutureslaw.org
Dinesh McCoy*
dinesh@justfutureslaw.org
Daniel Werner*
daniel@justfutureslaw.org
JUST FUTURES LAW
95 Washington Street, Suite 104-149
Canton, MA 02021
(617) 812-2822

Daniel Schneider
Legal Action Chicago
Attorney No. 100037
120 S. LaSalle St., Suite 1000
Chicago, IL 60603
(312) 423-5941
dschneider@legalactionchicago.org

**Application for admission pro hac vice forthcoming*