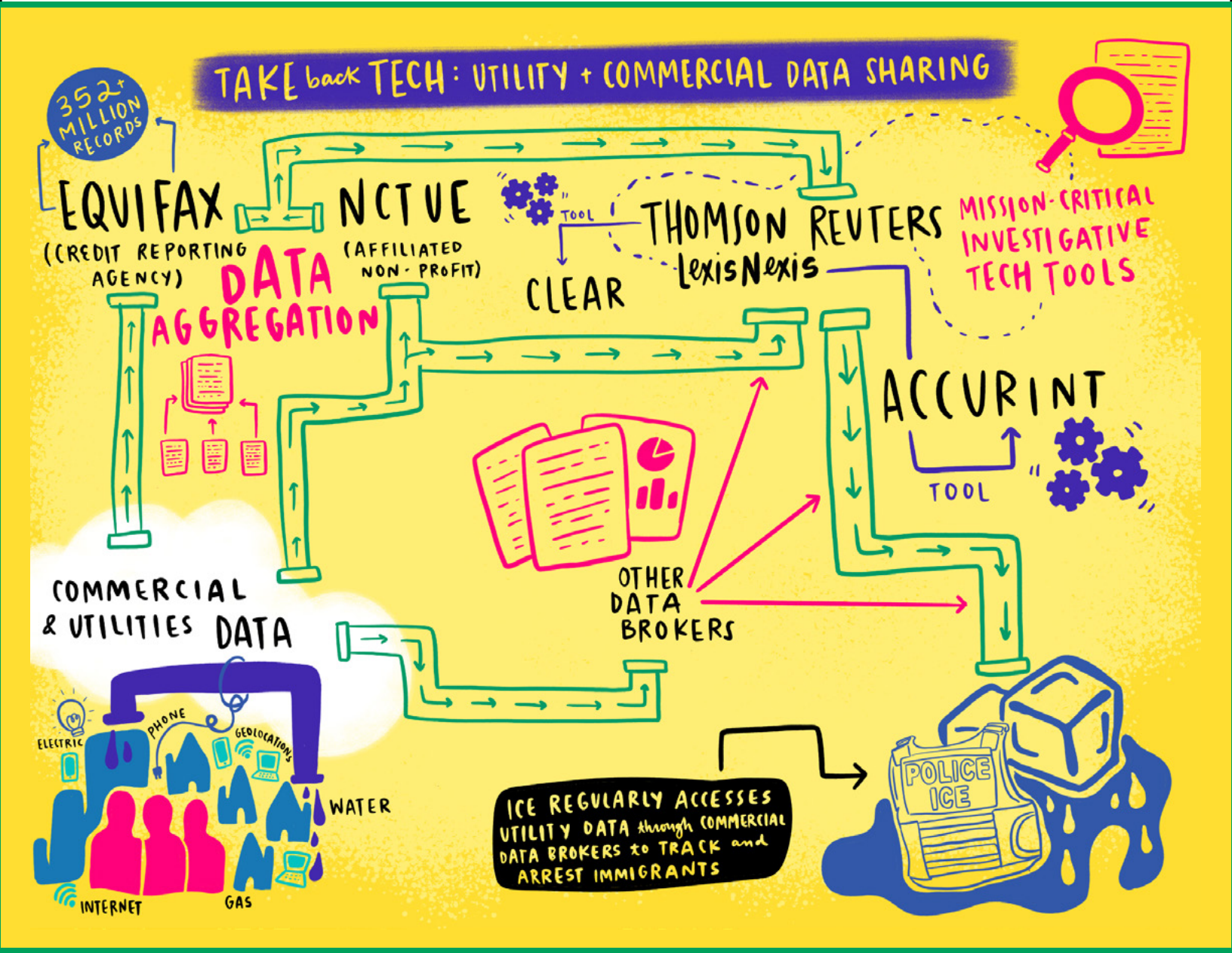
The Data Broker to Deportation Pipeline:

How Thomson Reuters & LexisNexis Share Utility & Commercial Data with ICE



JUST FUTURES LAW

mijente

Contents

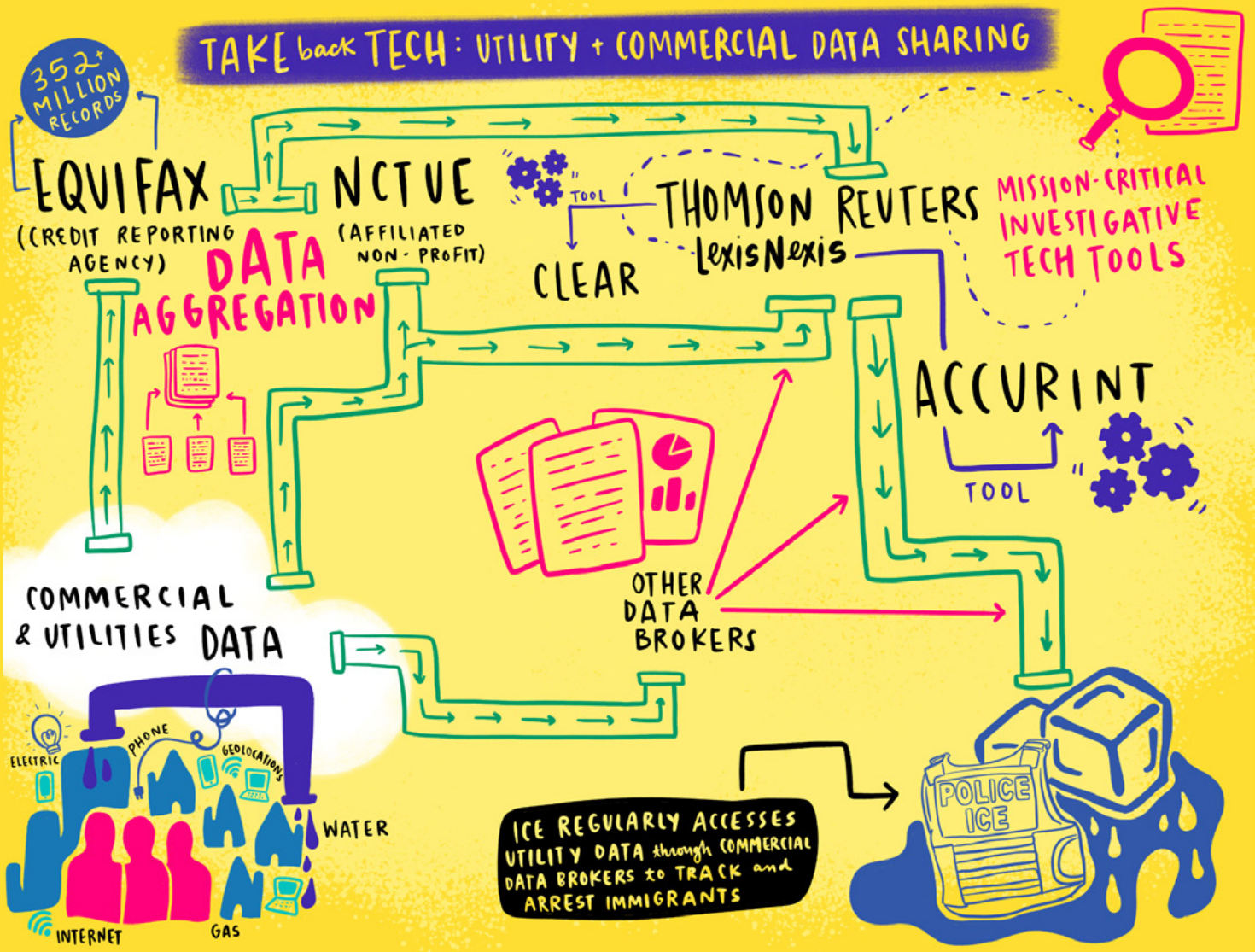
I. Introduction

Over the past year, public reporting has revealed how law enforcement entities are increasingly turning to surveillance data sources, such as smartphone applications, to collect sensitive personal information about marginalized communities.[1] This list of unconventional sources is only growing. Through several multi-million dollar contracts with data brokers, Immigration and Customs Enforcement (ICE) has gained access to unprecedented levels of utility and commercial data as well as advanced technological tools that enable more efficient and ruthless deportation operations. The data broker industry is composed of companies that aggregate, analyze, and share personal data extracted from online and offline activities, and there are few to no safeguards or consumer protections. Thomson Reuters and LexisNexis are two data brokers that have provided extensive data and operational capacity to ICE.[2]

Commercial and utility data includes information generated from gas, electricity, water, telephone, cable television, and internet services, as well as property records, geolocation information from mobile phones, and much more. When this information is aggregated and regularly updated, it can provide an intimate overview of a person's life, including where an individual has been, who their relatives and friends are, and where they work. Most people have no reason to expect that basic purchases for these essential services can be weaponized to surveil and criminalize communities. But by purchasing data sets and search tools from data brokers, ICE and other law enforcement entities amass enormous searchable databases and avoid democratic accountability for mass surveillance.

Without political mobilization against these intrusive and drastic surveillance measures, the data broker industry will continue to profit from large-scale data-sharing with ICE. This report maps the pipeline of data-sharing to unveil possible points of intervention. Specifically, we focus on the following:

- Equifax and NCTUE: How this credit reporting corporation and its non-profit affiliate NCTUE collect and aggregate consumer and utility data from millions of people.
- LexisNexis and Thomson Reuters: How consumer and utility data from Equifax and other sources flow into Accurint and CLEAR, the investigative technology tools of the two companies.
- ICE collaboration: How Accurint and CLEAR supercharge ICE's detention and deportation machine.



Commercial and utility data ends up in ICE's control through a series of little-known data-sharing agreements and practices.

II. Equifax and the National Consumer Telecom & Utilities Exchange (NCTUE)

Commercial and utility information gets caught up in ICE's surveillance dragnet via data-sharing by Equifax, one of the three nationwide credit reporting agencies in the United States. Equifax collects data about credit history and produces credit reports to help lenders determine individual risk and creditworthiness. Equifax is also the sole manager of the National Consumer Telecom & Utilities Exchange (NCTUE), a credit bureau whose members share consumer information and commercial history with each other.

A total of 95 internet, television, telephone, electricity, and gas companies contribute data to NCTUE for data coverage on 218 million unique consumers. Among these companies are AT&T, DISH Network, Verizon Wireless, Frontier Communications, Georgia Power, and Pacific Gas & Electric.[3] Anyone who has purchased basic utility services from these companies may show up in the aggregated NCTUE database. The data exchange aims to help member companies pool data and evaluate consumer risk based on credit history.[4] We do not know exactly how deep the relationship between Equifax and NCTUE goes, but we do know that Equifax servers store NCTUE data and agreements between the two allow for third-party data-sharing.[5] As discussed below, Equifax has many data agreements with third parties, including Thomson Reuters and LexisNexis, to share utility data. Utility data from NCTUE and Equifax is likely accessed by ICE via Thomson Reuters and LexisNexis tools.

III. Thomson Reuters & LexisNexis sell investigative technology tools that make commercial and utility data accessible to ICE.

As of May 2021, Thomson Reuters and LexisNexis have ongoing contracts with ICE with potential award values of over $16 million and $27 million, respectively. Public records show that these contracts give ICE access to Accurint from LexisNexis, an RELX subsidiary.[6] ICE previously relied heavily on Thomson Reuters for similar services from its Consolidated Lead Evaluation and Reporting (CLEAR) tool until late February 2021, when it entered into a large contract with LexisNexis intended to replace that functionality.[7] These tools enable ICE to rapidly search millions of data points across many datasets and leverage complex technological capabilities to compose personal profiles with an unprecedented level of detail. Both companies are equipped and clearly willing to offer investigative data tools to ICE and have similar data and functionality.

Below we discuss the two investigative tools from LexisNexis and Thomson Reuters in more detail and explain their access to Equifax's consumer and utility data.

A. LEXISNEXIS: ACCURINT

Accurint is an investigative technology tool that aggregates and organizes over 37 billion public and proprietary records.[8] LexisNexis claims that Accurint has the largest database of linked public and proprietary information. Its features include up-to-date phone numbers, addresses, vehicle information, property records, social networking information, license plate reader information, business records, criminal records, bankruptcies, and case management, comparison, and mapping tools.

To build full profiles on individuals, Accurint uses proprietary linking technology to find intersecting data points and pull together partial information for over 276 million U.S. consumers.[9] Given Accurint's description of this technology, it would be possible to automatically associate property records and criminal record information from different datasets if they connect to the same unique identifying information, such as phone numbers, addresses, or IDs.[10] This linking technology makes it more difficult for people to maintain privacy. For example, even if a set of purchases or activities are under different names, ICE can hypothetically use Accurint to associate the set together and find personally identifiable information if there are common data points.

B. THOMSON REUTERS: CLEAR

CLEAR is a similar investigative software tool that offers historical and current public records data, including cell phone records, real-time incarceration data, jail booking photos, home addresses, property listings, motor vehicle registration, and utility information.[11] Additionally, CLEAR provides access to content from the three large credit bureaus - Equifax, Experian, and TransUnion.

Notable datasets accessible in CLEAR are Appriss Safety's Justice Intelligence, a real-time jail booking database, and Motorola Solutions' Vigilant PlateSearch, a license plate reader database. Justice Intelligence is exclusively shared with CLEAR and includes 40 million booking photos and over 160 million records on jail and DOC booking data from 2,000 separate law enforcement databases.[12,13] This database was previously shared with LexisNexis' Accurint.[14] Vigilant PlateSearch offers easy access to at least 7 billion records of license plate data[15] and adds 150 million more scans every month.[16] This set of historical records potentially allows ICE agents to find all locations a car has been, placing entire neighborhoods and workplaces at risk.

C. EQUIFAX PARTNERSHIP WITH THOMSON REUTERS & LEXISNEXIS

We know that CLEAR uses credit header content from Equifax, which includes more than 350 million records on former and last known addresses, social security numbers, and birth dates. CLEAR has also accessed utility data through Equifax. Thomson Reuters' communications describe how "CLEAR's utility data is updated daily and provides more than 30 million utility data records (e.g., names, addresses, service information) from more than 80 national and regional electric, cable, gas, and telephone companies."[17] Based on the number of data records and existing agreements on data-sharing between Equifax and NCTUE, it is very likely that NCTUE is the original source of this utility data.[18]

Equifax and LexisNexis are also collaborating and sharing data. PowerView Score, a credit scoring product provided by LexisNexis, leverages "credit bureau and NCTUE telecom/utility payment data from Equifax" for over 300 million consumer accounts. LexisNexis boasts that PowerView Score is "capable of evaluating over 240 million consumers including more than 80% of thin/no file and other 'emerging' populations (i.e., Millennial & Hispanic)."[19] While it is unclear whether law enforcement officials can access this utility data via Accurint, Equifax and LexisNexis have laid the foundation for this expansive government surveillance.

IV. Why should we be concerned about these data broker contracts with ICE?

Both CLEAR and Accurint are representative of the growing ecosystem of unregulated data brokers with unparalleled access to personal data. As commercial high-tech engineering products, both merge many data points to offer comprehensive information profiles on individuals and enable easier, faster search of records. They offer analyst services to help organizations use their tools and batch processing capabilities, which allow users to send many searches at once and receive results faster. They also have continuous monitoring and alerting services to automatically inform users of new data and activities for people of interest.

These tools go far beyond the use cases of a simple database. Without data analytics tools like CLEAR and Accurint, ICE would need to gain access to dozens of different databases that may not be compatible and then manually search them over and over to find information and connections in a case. CLEAR and Accurint streamline and greatly enhance this process. They likely relate various datasets together by standardizing and connecting disparate data fields and using automated algorithmic processing to identify relationships that would take humans longer to find manually. Additionally, algorithmic processing can find patterns and connections between people and things that might be difficult to spot. These tools make it much easier to find and target personal assets like homes and cars for seizure and to start surveilling family members, friends, and workplaces.
As an example, an Accurint case study discusses how an Advanced Persons Search using an individual's first name, a relative's first name, and a street name can surface the individual's information quickly.[20] Tools like Accurint and CLEAR market this type of complex search as their competitive advantage over other products. Because of this sweeping aggregation of personal data and these high-tech search capabilities, ICE can locate individuals for detention and deportation at a mass scale.

V. Recommendations

Given the dangers posed by the data-sharing practices of NCTUE, Equifax, Thomson Reuters, and LexisNexis, it is imperative that we regulate the data broker industry and continue to call for accountability from companies that collaborate with ICE, alongside protecting immigrant communities that are already surveilled and criminalized by ICE. We recommend the following actions.

A. CONGRESS AND FEDERAL AGENCIES SHOULD REGULATE THE DATA BROKER INDUSTRY AND PROTECT UTILITY DATA.

Congress should pass a comprehensive federal privacy law that prevents the data broker industry from facilitating immigrant mass surveillance and criminalization. We propose implementing legislation that defines "utility data" as a protected class of personal data comprising all information derived from a consumer's use of water, electricity, gas, Internet, landline, cell phone, license, banking, education, and cable services. This legislation should prohibit data brokers from sharing and selling utility data with corporate affiliates and all law enforcement entities outside of industry regulators and auditors.

Policymakers should also examine and strengthen existing legislation such as the Gramm-Leach-Bliley Act (GBLA) and Fair Credit Reporting Act (FCRA) as well as proposed legislation such as the Data Broker Accountability and Transparency Act, to require data brokers to receive consumer consent before collecting sensitive data, mandate opt-outs, and create a data broker registry managed by the FTC.[21]

B. STATES SHOULD PROVIDE GREATER AUTHORITY TO THEIR PUBLIC UTILITIES COMMISSIONS.

At the state level, lawmakers should expand the purview of Public Utilities Commissions (PUCs), which often regulate state gas, electricity, and telephone companies, to include all modern utilities. Activists can push to make the protection of utility data a core issue for gubernatorial and PUC commission candidates. Additionally, state lawmakers should prohibit the selling and sharing of utility data with law enforcement and data brokers. California passed a similar law in September 2020.[22] To strengthen this type of legislation, we propose that utility data should not be subject to data sharing absent a criminal warrant, given its essential nature.

C. CONSUMERS, LEGAL PROFESSIONALS, AND SHAREHOLDERS SHOULD URGE COMPANIES TO DISCONTINUE THESE ABUSIVE DATA PRACTICES.

We also recognize that communities cannot wait for legislative protection. Collective action to pressure policymakers and corporations can help reduce the scope of surveillance and data-sharing. For instance, the legal community can act as responsible consumers and change their case research tools from LexisNexis and WestLaw (owned by Thomson Reuters) to alternative legal research resources (e.g., Bloomberg Industry Group/BNA, Fastcase, and Casemaker). Additionally, shareholders of the companies that provide data to Equifax and NCTUE could protest these companies' data practices through public shareholder votes. While shareholder activism is historically difficult and expensive, public awareness can motivate change.[23]

D. COMMUNITIES CAN TAKE STEPS TOWARD IMMEDIATE HARM REDUCTION.

Below are practical tips that individual community members may consider to mitigate against data sharing:

- Provide an alternate person, such as a housemate, or alternate address to utility companies for billing purposes.
- Ask your utility company to opt you out of data-sharing where possible.
- Opt out of smart meter usage from your electricity provider where possible — the meters can reveal when you are home and how many people are in your home.

These recommendations are the first steps for protecting immigrant communities and reducing the power and scope of ICE. Ultimately, the strongest community response is an organized one. We are encouraged and hopeful that the growing energy around bringing accountability to data brokers and fighting against mass surveillance and criminalization will lead to a safer and more just world for everyone.

12 Acknowledgments

TAKE BACK TECH FELLOWS
Archana Ahlawat
Ana Ortiz

WRITERS
Archana Ahlawat, Ana Ortiz, and Anuj Shah

EDITORS & PROOFREADERS
Dinesh McCoy, Julie Mao, & Ellen Kemp, Just Futures Law

RESEARCH SUPPORT
Aaron Lackowski, Empower LLC

ILLUSTRATION
Laura Chow Reeve, Radical Road Maps

REPORT LAYOUT DESIGN
Summer Rose Wood

Mijente and Just Futures Law are joint sponsors of the Take Back Tech Fellowship program.

13 Endnotes

1 Byron Tau and Michelle Hackman, Federal Agencies Use Cellphone Location Data for Immigration Enforcement, The Wall Street Journal (February 7th, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600; Joseph Cox, How the U.S. Military Buys Location Data from Ordinary Apps, Vice (November 16th, 2020), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x; Charlie Savage, Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says, The New York Times (January 22nd, 2021), https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html

2 Hannah Beckler, Thomson Reuters Analysts Process Data to Help ICE Agents Make Arrests, Documents Show, Documented (May 20th, 2020), https://documentedny.com/2020/05/20/thomson-reuters-analysts-process-data-to-help-ice-agents-make-arrests-documents-show/; Crime and Criminal Investigations, LexisNexis (Accessed May 4th, 2021), https://risk.lexisnexis.com/law-enforcement-and-public-safety/crime-and-criminal-investigations

3 About Us, NCTUE https://www.nctue.com/about-us

4 Id.

5 History, NCTUE https://www.nctue.com/history

6 Active ICE Contracts with Thomson Reuters & LexisNexis, https://tinyurl.com/icecontracts (updated as of May 16, 2021).

7 Drew Harwell, ICE investigators used a private utility database covering millions to pursue immigration violations, The Washington Post (February 26th, 2021), https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data/

8 Case Studies: LexisNexis Accurint for Law Enforcement, LexisNexis (Accessed May 13th, 2021), https://risk.lexisnexis.com/products/accurint-for-law-enforcement

9 LexID, LexisNexis (2021), https://risk.lexisnexis.com/our-technology/lexid

10 Case Studies: LexisNexis Accurint for Law Enforcement, LexisNexis (Accessed May 13th, 2021), https://risk.lexisnexis.com/products/accurint-for-law-enforcement

11 Thomson Reuters CLEAR, www.thomsonreuters.com/content/dam/openweb/documents/pdf/legal/fact-sheet/clear-brochure.pdf

12 Justice Intelligence Product Sheet, https://apprissinsights.com/wp-content/uploads/sites/9/2018/06/SFTY-JI-Investigations-PS-FINAL-WEB.pdf

13 Sole Source Justification: Thomson Reuters Special Services, U.S. Department of Homeland Security (2018), https://tinyurl.com/thomsonreuters-dhs

14 LexisNexis Federal Contract Price List, http://www.lexisnexis.com/gsa/76/gsasched76_pricelist.pdf

15 CLEAR for Law Enforcement, Thomson Reuters (Accessed May 14th, 2021), https://legal.thomsonreuters.com/en/products/clear-investigation-software/law-enforcement

16 Vigilant ® License Plate Recognition (LPR), WirelessUSA (Accessed May14th, 2021), https://www.wirelessusa.com/motorola/vigilant/

17 Kyle Keene, Sole Source Letter - Thomson Reuters (January 17th, 2018), https://www.prorfx.com/Storage/110S34471_051/ProRFx/Upload/Attachments/General/Sole%20Source%20Letter%20-Thomas%20Reuters.pdf

18 Nina Wang, Is your utility company telling ICE where you live?, Center on Privacy & Technology at Georgetown Law (February 26th, 2021), https://medium.com/center-on-privacy-technology/is-your-utility-company-telling-ice-where-you-live-ae1c7d187eff

19 PowerView Score, LexisNexis Risk Solutions (Accessed May 13th, 2021), https://risk.lexisnexis.com/products/powerview-score

20 Case Studies: LexisNexis Accurint for Law Enforcement, LexisNexis Risk Solutions (Accessed May 13th, 2021), https://risk.lexisnexis.com/products/accurint-for-law-enforcement

21 Data Broker Accountability and Transparency Act of 2020, H.R. 6675, 116th Congress, https://www.congress.gov/bill/116th-congress/house-bill/6675

22 Public utilities: cooperation with immigration authorities, AB-2788, Assembly Session 2019-2020, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB2788

23 Morgan Stelly, Shareholder Activism: The Success of Few for the Few, The Race to the Bottom (August 20th, 2019), https://www.theracetothebottom.org/rttb/2019/8/20/shareholder-activism-the-success-of-few-for-the-few