WHEN WESTLAW FUELS ICE SURVEILLANCE: ETHICS IN THE ERA OF BIG DATA POLICING

SARAH LAMDAN[∞]

ABSTRACT

Legal research companies are selling surveillance data and services to U.S. Immigration and Customs Enforcement ("ICE") and other law enforcement agencies. This Article discusses ethical issues that arise when lawyers buy and use legal research services sold by the same vendors responsible for building ICE's surveillance systems. As the legal profession collectively pays millions of dollars for computer assisted legal research services, lawyers should consider whether doing so in the era of big data policing compromises their confidentiality requirements and their obligation to supervise third party vendors. With new companies developing legal research services, lawyers have more legal research options than ever. Lawyers can choose to purchase legal research services from socially responsible vendors.

[∞] Sarah Lamdan is a professor at CUNY School of Law with a master's degree in legal information management. She would like to thank her colleagues at CUNY School of Law for their support and feedback, and to the editorial team at the NYU Review of Law and Social Change for their editing work. Sarah would also like to thank Eyal, Benjamin, Evelyn, and Kansas Lamdan.

TABLE OF CONTENTS

INTRODUCTION

Imagine that you are an immigration attorney with a client who was just arrested and detained by ICE. Days after receiving a ticket for driving without a license, your client is dropping their children off at school when ICE agents suddenly descend, separating your client from their family, job, and community without warning. Upon investigation, you learn that ICE located your client through a database that tracks license plate locations. Digging deeper, you find that the license plate data comes from Thomson Reuters,[1] the company whose

1. In 2017, Thomson Reuters teamed up with Vigilant Solutions to integrate license plate recognition data into its CLEAR investigation platform, one of the services that ICE uses for surveillance. *See* Press Release, Thomson Reuters, Thomson Reuters Brings Vigilant License Plate Recognition Data to CLEAR Investigation Platform (June 18, 2017), https://www.thomsonreuters.com/en/press-releases/2017/june/thomson-reuters-brings-vigilant-license-plate-recognition-data-to-clear-investigation-platform.html [https://perma.cc/ADZ8-8DQT] [hereinafter *License Plate Recognition Data Press Release*]. The CLEAR database contract with ICE is discussed *infra* notes 138–146 and accompanying text.

legal research product, Westlaw, you use every day to research client matters and for which your employer pays thousands of dollars each month.[2] In fact, the money that you and your colleagues pay for the legal research service is padding Thomson Reuters' balance sheets at the same time that the company is purchasing and aggregating surveillance databases and technologies to sell them to law enforcement agencies like ICE.[3]

Contemporary law enforcement is a technology-driven enterprise that incorporates vast amounts of information, machine-learning algorithms, and artificial intelligence into identifying and tracking potential law-breakers.[4] This "big data policing"[5] depends on a broader range of data than ever before—including "crime data, personal data, gang data, associational data, locational data, [and] environmental data"—gleaned from a "growing web of sensor and surveillance sources."[6] Like other areas of policing, "immigration control has rapidly become an information-centered and technology-driven enterprise"[7] that depends on data collected and curated by private "data brokers."[8]

2. Daniel Fisher, *The Law Goes Open Source*, FORBES (June 12, 2018), https://www.forbes.com/forbes/2008/0630/070.html#50f288091d3e [https://perma.cc/ER23-JJAH] ("Big law firms pay as much as $4 million a year for access to Westlaw and Lexis.").

3. *See* THOMSON REUTERS, ANNUAL REPORT 2017, 34, 47 (Mar. 16, 2018), https://ir.thomsonreuters.com/static-files/dd5b380d-7e0e-4316-b693-bec293daaece [https://perma.cc/9WYS-7C3H] [hereinafter THOMSON REUTERS 2017 ANNUAL REPORT]. The company's legal research products pulled in $ 3.39 billion in revenue in 2017, 30 percent of the company's revenues. *Id*. According to the company's annual report, the CLEAR surveillance product is considered one of "Legal's major brands," but it is unclear exactly how much revenue is generated from each of its legal products. *Id*. at 7–8. While it is unclear how Thomson Reuters distributes its profits among new research and development efforts, the company is actively working to eliminate "product silos" and seemingly combines revenues from its various products, making it possible that lawyers' Westlaw subscriptions help fund research & development for its surveillance products. *See* Bob Ambrogi, *As Thomson Reuters Readies Layoffs of 3,200, What's it Mean for Customers?*, LAWSITES (Dec. 10, 2018), https://www.lawsitesblog.com/2018/12/thomson-reuters-readies-layoffs-3200-whats-mean-customers.html [https://perma.cc/XD4S-G4X3].

4. *See* ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 18–19 (2017).

5. "Big Data Policing" is a term from Andrew Guthrie Ferguson's 2017 book on the subject. *Id*. at 2 n.1 ("'Big data' is used here as a shorthand term for growing data sets and large quantities of digital information. . . . In the context of law enforcement, the concept of big data policing encompasses a host of emerging technologies involving predictive analytics, mass surveillance, data mining, and other digital tracking capabilities.").

6. *Id*. at 2.

7. Anil Kalhan, *Immigration Surveillance*, 74 MD. L. REV. 1, 6 (2014).

8. *See* FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 68 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/5XNA-X4XM] ("Data brokers are companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud."); *see also* FERGUSON, *supra* note 4, at 12–14 (explaining private data brokers).

Private data brokers play a critical role in government surveillance.[9] While intelligence and law enforcement agencies certainly conduct their share of direct online surveillance,[10] they have become hungry consumers of the data profiles sold by private companies, a method of indirect data collection which allows these agencies to evade privacy protections.[11] Legal publishers have seized the opportunity created by this demand and become data brokers: Thomson Reuters and RELX Group,[12] the companies that supply lawyers with the legal research products Westlaw and Lexis, respectively, are building and maintaining surveillance tools for local, state, and federal law enforcement entities, including U.S. Immigration and Customs Enforcement ("ICE").[13] Surveillance—including immigration surveillance—offers Thomson Reuters and RELX Group new sources of income as selling print resources and online case databases becomes less lucrative.[14] ICE is using more personal data than ever to track immigrants, and increasingly depends on companies like Thomson Reuters and RELX for datasets.[15] Recognizing the potential for profit, Thomson Reuters and RELX are researching and developing new ways to use artificial intelligence, cognitive computing, and big data collections to assist immigration enforcement.[16]

9. ROBERT GELLMAN & PAM DIXON, WORLD PRIVACY FORUM, DATA BROKERS AND THE FEDERAL GOVERNMENT: A NEW FRONT IN THE BATTLE FOR PRIVACY OPENS 8 (2013), http://www.worldprivacyforum.org/wp-content/uploads/2013/10/WPF_DataBrokersPart3_fs.pdf [https://perma.cc/8AM5-24HH] ("The U.S. federal government uses data brokers extensively for a wide variety of governmental activities.").

10. *See, e.g.*, U.S. DEP'T OF HOMELAND SEC'Y, ANALYST'S DESKTOP BINDER 20–23 (2011), https://www.scribd.com/doc/82701103/Analyst-Desktop-Binder-REDACTED [https://perma.cc/767G-3EXG] (listing key words and search terms for agency analysts to monitor on social media sites like Facebook and Twitter).

11. Amitai Etzioni, *Reining in Private Agents*, 101 MINN. L. REV. HEADNOTES 279, 279 (2016) (presenting evidence that restraints on governmental power to surveil individuals "are circumvented, on a very large scale, by private agents carrying out—for the government—activities that government is banned from undertaking.").

12. RELX Group was formerly known as Reed Elsevier. In 2015, the company rebranded itself to "reflect the company's transformation in recent years from a publishing group to a 'technology, content and analytics driven business.'" Robert Cookson, *Reed Elsevier to Rename Itself RELX Group*, FINANCIAL TIMES (Feb. 26, 2015), https://www.ft.com/content/4be90dbe-bd97-11e4-9d09-00144feab7de [https://perma.cc/WRH7-JGJL].

13. *See infra* notes 100, 140–148 and accompanying text.

14. *See id*.

15. *See* MIJENTE, THE NATIONAL IMMIGRATION PROJECT & IMMIGRANT DEFENSE PROJECT, WHO'S BEHIND ICE?: THE TECH AND DATA COMPANIES FUELING DEPORTATIONS (Aug. 23, 2018), https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf [https://perma.cc/9FCY-QC3E]. The Mijente report describes the ever-growing network of technology companies feeding data to DHS and ICE, tracing the web of technology companies, such as Palantir and Amazon, that help DHS track immigrants, explaining that "[i]mmigration enforcement and detention is now big business for Silicon Valley" *Id*. at 1. The report describes Thomson Reuters and its subsidiary, West Publishing, as a "data broker with large ICE contracts that interfaces with Palantir and Forensic Logic" to share data sets of personally identifiable information. *Id*. at 11. Forensic Logic owns COPLINK, "the most widely used corporate platform for law enforcement information sharing with DHS." *Id*. at 10.

16. *See infra* notes 131–135 and accompanying text.

Policing technology is not value neutral.[17] U.S. immigration authorities rely on big data technology to employ increasingly cruel and invasive techniques as they accelerate arrests, detentions, and deportations of immigrants without legal status.[18] ICE agents arrest immigrants at their homes,[19] in courthouses,[20] at work,[21] and while dropping their children off at school.[22] Agents pursue immigrants in car chases, leading on one occasion to multiple deaths.[23] In another instance, immigration enforcement officers stopped and arrested a man while he was driving his pregnant wife to the hospital for a C-section, leaving her to drive herself to the procedure.[24]

These callous enforcement tactics are facilitated by surveillance technology. The technology is used to track and locate noncitizen targets, undermining city

17. Bryan Menegus & Kate Conger, *Microsoft Employees Pressure Leadership to Cancel ICE Contract*, GIZMODO (June 19, 2018), https://gizmodo.com/microsoft-employees-pressure-leadership-to-cancel-ice-c-1826965297 [https://perma.cc/9GYH-B7RS] ("It would be easy to think of coding as neutral—we solve puzzles…. It's important, though, to consider the bigger picture for the things we help to build—how can it be misused, who am I supporting with it, who benefits from it and who bears the costs?").

18. MIJENTE, *supra* note 15, at 1.

19. *See, e.g.*, Tanvi Misra, *Lessons From New York's Immigration Raids*, CITYLAB (July 23, 2018), https://www.citylab.com/equity/2018/07/lessons-from-new-yorks-immigration-raids/565847/ [https://perma.cc/U6GB-8ZBD] (finding after a recent study on immigrant raids in New York City that Trump's "unshackled" ICE forces are entering homes without consent, using "misleading ruses," and even force to get inside, "gaining access to its targets through surveillance of immigrant communities").

20. *See* U.S. IMMIGRATION AND CUSTOMS ENF'T, No. 11072.1, CIVIL IMMIGRATION ENFORCEMENT ACTIONS INSIDE COURTHOUSES 1 (2018), https://www.ice.gov/sites/default/files/documents/Document/2018/ciEnforcementActionsCourthouses.pdf [https://perma.cc/5S95-NNHS]; Akilah Johnson, *ICE Arrests at Courthouses Disrupt Justice, Lawsuits Claim*, BOS. GLOBE (Mar. 16, 2018), https://www.bostonglobe.com/metro/2018/03/15/ice-arrests-courthouses-are-disrupting-justice-two-lawsuits-claim/N7IhXiHlEuw3Qdz1XDlt4I/story.html [https://perma.cc/TXE2-5ME2].

21. *See, e.g.*, John Minchillo & Elliot Spagat, *Immigration Agents Arrest 114 in Sting at Ohio Landscaping Company*, PBS NEWS HOUR (June 5, 2018), https://www.pbs.org/newshour/politics/immigration-agents-arrest-114-in-sting-at-ohio-landscaping-company [https://perma.cc/9E3U-ZJQC]; N'dea Yancey-Bragg, *Pizza Delivery Man Facing Deportation After Delivering to Brooklyn Military Base*, USA TODAY (June 6, 2018), https://www.usatoday.com/story/news/nation-now/2018/06/06/ice-pizza-delivery-man-military-base/678479002/ [https://perma.cc/C6LR-Y4SL].

22. *See, e.g.*, Christie Duffy, *2 Dads Nabbed by ICE as They Drop Off Kids at NJ School; 3rd Takes Shelter in Church*, PIX11 (Jan. 25, 2018), https://pix11.com/2018/01/25/2-dads-nabbed-by-ice-as-they-drop-off-kids-at-nj-school-3rd-takes-shelter-in-church/ [https://perma.cc/EA5P-336K].

23. Amy B. Wang, *A Couple Died in a Car Crash While Fleeing ICE Agents in California, Authorities Say*, WASH. POST (Mar. 15, 2018), https://www.washingtonpost.com/news/post-nation/wp/2018/03/15/a-couple-died-in-a-car-crash-while-fleeing-ice-agents-in-california-authorities-say/?utm_term=.0a94256de062 [https://perma.cc/5DA4-MUD6] (describing a deadly car crash that occurred after ICE agents misidentified a man and attempted to pull over his vehicle, causing its inhabitants to flee).

24. Wynne Davis, *ICE Detains Man Driving his Wife to Hospital for Planned C-Section*, NPR (Aug. 19, 2018) https://www.npr.org/2018/08/19/640022683/ice-detains-man-driving-his-wife-to-hospital-for-planned-c-section [https://perma.cc/N2KG-WX6S].

and state level "sanctuary" policies.[25] Mijente, a national organization that advocates for immigrants' rights, reports that surveillance tools help ICE agents "scour regional, local, state, and federal databases across the country, build profiles of immigrants and their friends and family based on both private and public information, and use those profiles to surveil, track, and ultimately deport immigrants."[26]

The sophisticated, invasive surveillance products developed by companies like Thomson Reuters and RELX directly contribute to the increase in immigration enforcement.[27] ICE agents rely on a plethora of records to learn about and track immigrants, from utility bills to law enforcement databases.[28] Agents sift through various data points to find targets, "tap[ping] into local law enforcement and drivers' license databases," and tracking immigrants from home addresses to churches and workplaces.[29] Aristides Jimenez, a former ICE agent, explains that the agency uses brokered data and analytical tools from private companies to "discover connections between individuals, their addresses, and their property."[30]

When Thomson Reuters and RELX develop products for ICE and other law enforcement agencies, lawyers are contributing, albeit indirectly, to the surveillance of their clients. The fees lawyers pay for legal research contribute significantly to the profit margin of companies developing surveillance products. Both companies make millions of dollars selling your personal data, and the data of millions of other people, to law enforcement and selling sophisticated research tools that transform our data into invasive surveillance dossiers with real-time tracking updates. This places lawyers in problematic ethical territory.

In addition to their financial conflict, lawyers must also consider how their profession's ethical standards mesh with the vendors they rely upon. While the ABA Model Rules of Professional Conduct and accompanying guidance materials demand that lawyers make efforts to hold parties they "directly supervise" to their own professional obligations, the ABA has not specifically addressed ethical issues related to legal research vendors.[31] Nevertheless,

25. *See* MIJENTE, *supra* note 15, at 2–3 (explaining that ICE's collection of mass personal information from private vendors has "enormous implications for protective policies in cities and states by making separation of information impossible, granting full access to Trump's federal police force"); Misra, *supra* note 19 (describing ways ICE subverts local protective policies).

26. MIJENTE, *supra* note 15, at 3.

27. *Id*. at 1 (pointing to tech companies and data brokers as "playing an increasingly central role in facilitating the expansion and acceleration of arrests, detentions, and deportation").

28. George Joseph, *Where ICE Already Has Direct Lines to Law-Enforcement Databases with Immigrant Data*, NPR (May 12, 2017), https://www.npr.org/sections/codeswitch/2017/05/12/479070535/where-ice-already-has-direct-lines-to-law-enforcement-databases-with-immigrant-d [https://perma.cc/FTF9-THU9].

29. *Id*.

30. *Id*.

31. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 08-451, at 1 (2008), https://www.americanbar.org/content/dam/aba/migrated/2011_build/ethics_2020/ethicsopinion084

Thomson Reuters and RELX's surveillance products should spark discussions about lawyers' ethical duties regarding their legal research products. The legal industry must ask: Should lawyers use products that are linked to the surveillance of their clients? And more concretely, is it possible that these products are sharing lawyers' research data with law enforcement?

Lawyers should follow the lead of other consumer groups that have focused on supply chain ethics to ensure that the products and services they consume as part of their legal practice comply with ethical standards.[32] In an era where consumers can research purchasing choices with more ease than ever before, ethical priorities have become a key consideration in consumer decision-making.[33] Buyers can trace the corporate roots and supply chains for their goods and services while shopping from home or standing in a store. The increased availability of information to consumers online has exposed unethical supply chains, driving consumers to insist on ethical manufacturing practices for products ranging from clothing to coffee beans.[34] Similarly, legal professionals can harness their power as consumers to hold legal research companies

51.authcheckdam.pdf [https://perma.cc/CZZ7-22LA] (A lawyer "should make reasonable efforts to ensure that the conduct of the lawyers or nonlawyers to whom tasks are outsourced is compatible with her own professional obligations as a lawyer with 'direct supervisory authority' over them."); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 483, at 15–16 (2018), https://www.americanbar.org/content/dam/aba/images/news/formal_op_483.pdf [https://perma.cc/9HWX-G68F] (requiring attorneys to "properly supervise […] third-party electronic-information storage vendors" and to notify clients about data breaches). The ABA, mirroring the legal profession, is not the fastest to adopt and react to new technology. For instance, the legal blog *Above the Law* recently assailed the ABA for waiting until 2018 to create professional responsibility guidelines for blogging. Robert Ambrogi, *In New Ethics Ruling on Blogging, ABA Opines Like it's 1999*, ABOVE THE LAW (Mar. 12, 2018), https://abovethelaw.com/2018/03/in-new-ethics-ruling-on-blogging-aba-opines-like-its-1999/ [https://perma.cc/MR7P-CZWP].

32. For instance, manufacturing supply chains are managed to guarantee sustainable environmental practices. *See generally* Cristina Giminez & Vicenta Sierra, *Sustainable Supply Chains: Governance Mechanisms to Greening Suppliers*, 116 J. BUS. ETHICS 189 (2013). Apparel and footwear supply chains are managed to guarantee fair labor practices. *See generally* Haesun Park-Poaps & Kathleen Rees, *Stakeholder Forces of Socially Responsible Supply Chain Management Orientation*, 92 J. BUS. ETHICS 305 (2010). Mineral supply chains are managed to avoid social strife. *See generally* Rita O. Koyame-Marsh & Debra Perkins, *Supply Chain Management of Conflict Minerals: Case of the Democratic Republic of Congo*, PROC. OF THE 6TH INT'L BUS. AND SOC. SCI. RES. CONF. (2013).

33. NIELSEN, THE SUSTAINABILITY IMPERATIVE: NEW INSIGHT ON CONSUMER EXPECTATIONS 10 (Oct. 2015), https://www.nielsen.com/content/dam/nielsenglobal/dk/docs/global-sustainability-report-oct-2015.pdf [https://perma.cc/GTQ5-3Z5B] (finding that 66 percent of surveyed consumers were willing to pay extra for products and services from companies who are committed to positive social and environmental impact).

34. *See* Amrou Awaysheh & Robert D. Klassen, *The Impact of Supply Chain Structure on the Use of Supplier Socially Responsible Practices*, 30 INT'L J. OF OPERATIONS & PRODUCT MGMT. 1246, 1247 (Nov. 2010). Software company supply chains have also been scrutinized: for example, Apple has been held accountable for human rights violations of its upstream suppliers, at plants that manufacture iPhones. *See* Kirsten E. Martin, *Ethical Issues in the Big Data Industry*, 14:2 MIS Q. EXEC. 67, 71 (June 2015), http://kirstenmartin.net/wp-content/uploads/2013/11/Martin-MISQE-Big-Data-Ethics-2015.pdf [https://perma.cc/DCC6-7V3T].

accountable for providing an ethical supply chain.

Because lawyers are bound to an ethical code, they must remain vigilant and actively ensure that the products they use in their work comports with their ethical principles. While LexisNexis and Westlaw continue their decades-long grip on the legal research market, new companies have emerged that provide attorneys with less problematic alternatives. Lawyers should explore using other legal research companies like Casetext, which promises not to sell or provide user data to third parties,[35] or products that are not owned by data brokerage services.

This Article explores the ethical issues raised by legal research companies selling surveillance services to ICE and other law enforcement. Part II reviews the U.S. government's extensive history of tracking immigrants and U.S. immigration enforcement's gradual incorporation of sophisticated surveillance technologies, demonstrating how today's immigration enforcement uses more data-based surveillance than ever before in new, ethically fraught ways. Part III describes legal research companies' expansion into the surveillance market, and Part IV examines the ethical issues that expansion raises. As legal research companies enter the surveillance market, they provide a test case to explore ethical issues related to big data policing and the legal profession.

I.
THE EVOLUTION OF ICE SURVEILLANCE: AN OVERVIEW

A. The Origins of Immigrant Surveillance

The current immigrant surveillance scheme may seem shocking, with its layers of intrusive digital probes that reach into almost every aspect of immigrants' lives, from where their cars are driving to who they "friend" on Facebook. However, immigration surveillance is a centuries-old practice in the United States. As far back as 1798, the Alien and Sedition Acts called for the collection of information about immigrants' political beliefs,[36] ordering shipmasters to report noncitizen passengers upon arrival in U.S. ports in order to prevent those with undesirable political views from remaining in the country.[37]

Through the decades, the federal government gradually recorded more and more information about the nation's newcomers. In the late 1800s, spurred by the "hysteria [of] a civilizational threat," Congress authorized creating registries to identify and track Chinese immigrants by recording their names, dates, ages,

35. *Casetext Privacy Policy*, CASETEXT, https://casetext.com/privacy [https://perma.cc/6GYS-EYPE] (last modified Mar. 15, 2015) (stating the company will not sell your personal information to third parties).

36. Naturalization Act of 1790, ch.20, 1 Stat. 414 (1795); An Act to Establish a Uniform Rule of Naturalization, ch.54 1 Stat. 566 (1798); An Act Concerning Aliens, ch.58, 1 Stat. 570 (1798); An Act Respecting Alien Enemies, ch.66, 1 Stat. 577 (1798).

37. An Act Concerning Aliens, ch.58, 1 Stat. 570 (1798).

occupations, addresses, and even physical "peculiarities."[38] In 1893, the U.S. Supreme Court clarified that plenary power authorizes Congress to create legislation allowing for the deportation of resident noncitizens who had failed to obtain identification proving lawful residency.[39] Just a decade later, Congress passed a law requiring prospective immigrants to answer questions about their political backgrounds.[40] Similar laws, like the Alien Registration Act of 1940,[41] increased the scope of immigration surveillance in the pre-internet era by requiring noncitizens to be registered and fingerprinted.

Although many contemporary academics and policy-makers decry the discriminatory immigration policies of early America,[42] similar and even more intrusive modes of surveillance remain ingrained in our laws.

B. The Development of Contemporary Immigrant Surveillance

Since the 1990s, and the beginning of the digital era, immigration surveillance databases have grown far more complex. Computers are capable of storing large quantities of personal data for software programs to mine, allowing ICE to track immigrants more easily than ever. For instance, the Department of Homeland Security's E-Verify program, first implemented in the 1990s, mines government citizenship data and checks it against the information that employees working for government contractors and vendors provide in their I-9 forms.[43] Every federal contractor must use the E-Verify system to examine all newly-hired employees as well as existing employees assigned to the contract, and any employees that are deemed not to be in compliance with U.S. immigration laws are ineligible for government contractor jobs.[44]

After the September 11, 2001 terrorist attacks, national security concerns trumped due process considerations and the U.S. surveillance regime exploded from individualized to mass surveillance.[45] Congressional investigations linked

38. Margaret Hu, *Crimmigration-Counterterrorism*, 2017 WIS. L. REV. 955, 967 (2017) (quoting the Chinese Exclusion Act § 4 (1882) (repealed 1943)).

39. Fong Yue Ting v. United States, 149 U.S. 698, 728–29 (1893), *overruled in part on other grounds by* Yamataya v. Fisher, 189 U.S. 86, 101 (1903).

40. An Act to Regulate the Immigration of Aliens into the United States, ch. 1012, 32 Stat. 1213, 1222 (1903).

41. The Alien Registration Act of 1940, ch. 439, 54 Stat. 670 (1940).

42. *See e.g.*, David B. Oppenheimer, Swati Prakash, and Rachel Burns, *Playing the Trump Card: Racism and Immigration Law*, 26 LA RAZA L.J. 1 (2016), https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1264&context=blrlj [https://perma.cc/UR3Y-N64T].

43. NATIONAL IMMIGRATION LAW CENTER, THE HISTORY OF E-VERIFY 1–2 (Sept. 2011), https://www.nilc.org/wp-content/uploads/2015/12/e-verify-history-rev-2011-09-29.pdf [**https://perma.cc/63L7-NU4J**]. The E-Verify program was authorized by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 ("IIRIRA"), Pub. L. 104-208, 8 U.S.C. § 1101 et seq.

44. HISTORY OF E-VERIFY, *supra* note 43, at 2.

45. *See, e.g.*, Marc Rotenberg, *Privacy and Secrecy After September 11*, 86 MINN. L. REV. 1115, 1115–16 (2002); ELIZABETH GOITEIN & FAIZA PATEL, BRENNAN CTR. FOR JUSTICE, WHAT

the terrorists' success to poor agency coordination,[46] so Congress expanded the scope of permissible surveillance and inter-agency coordination. The Patriot Act, passed shortly after the attacks, amended the Foreign Intelligence Surveillance Act of 1978 ("FISA") and empowered federal agents to use new, more invasive surveillance tactics.[47] Subsequent amendments, including the FISA Amendments Act of 2008—containing the controversial Section 702[48]—further broadened the scope of surveillance.[49]

FISA also established a system of judicial review to oversee foreign intelligence surveillance through the Foreign Intelligence Surveillance Court ("FISC").[50] Before 2001, the FISC focused on reviewing and issuing individualized warrants where foreign intelligence was sought to protect the U.S. from external threats, avoiding the "dragnet" surveillance techniques that the Fourth Amendment was designed to prevent.[51] That changed in the years following 9/11.[52] Today, the government can get a FISA warrant for any "tangible things" it has "reasonable grounds" to believe may be related to a terrorism investigation.[53] The term "tangible things" has been construed broadly,

WENT WRONG WITH THE FISA COURT 21–22 (2015), https://www.brennancenter.org/sites/default/files/analysis/What_Went_%20Wrong_With_The_FISA_Court.pdf [https://perma.cc/2ZXT-R5EL].

46. RICHARD A. BEST, JR., CONG. RESEARCH SERV., THE INTELLIGENCE COMMUNITY AND 9/11: CONGRESSIONAL HEARINGS AND THE STATUS OF THE INVESTIGATION 7–9 (2003), https://fas.org/irp/crs/RL31650.pdf [https://perma.cc/E44F-ZKX8] (discussing the need to remove "walls" between the intelligence community and law enforcement to improve information collection and sharing and more effectively fight terrorism).

47. *See generally* 50 U.S.C. §§ 1801–1813 (2012); Presidential Statement on Signing the Foreign Intelligence Surveillance Act of 1978, 14 WEEKLY COMP. PRES. DOC. 1853 (Oct. 25, 1978).

48. 50 U.S.C. §§ 1881a. The most controversial surveillance authority, Section 702 of the Foreign Intelligence Surveillance Act, was reauthorized on January 19, 2018. FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, 132 Stat. 3 (2018). The law authorizes the U.S. government to surveil non-U.S. citizens with any information relevant to any foreign intelligence objective abroad. *Id*. The 2018 reauthorization expands the surveillance authority to include collecting communications "about" targets even when they are not party to the communication. *Id*. For instance, any communication that includes the term ISIS or the name of a political activist may be surveilled and is collected from cell phone providers, social media companies, etc., through warrantless "backdoor searches" that risk disproportionately impacting immigrants. *See* Robyn Greene, *Americans Wanted More Privacy Protections. Congress Gave Them Fewer.*, SLATE (Jan. 26, 2018), https://slate.com/technology/2018/01/congress-reauthorization-of-section-702-of-the-fisa-is-an-expansion-not-a-reform.html **[**https://perma.cc/8GTH-EJQH].

49. FISA Amendments Act of 2008, Pub. L. No. 110-261, §403, 122 Stat. 2463, 2473 (2008).

50. 50 U.S.C. §§ 1803–1805.

51. GOITEIN & PATEL, *supra* note 45, at 9 (describing the court's original mandate), at 11 (citing U.S. v. U.S. District Court, 407 U.S. 297 (1972)).

52. *Id*. at 22–28 (detailing a series of new court interpretations and statutory amendments to FISA that shifted the role of the FISA court).

53. 50 U.S.C. § 1861 (2012) (allowing the FBI to collect "any tangible things (including books, records, papers, documents, and other items)"). This broad language can be read to include almost anything. The reasonable grounds standard is similarly permissive, including instances where known facts and circumstances are sufficient for a prudent person to believe that contraband

allowing the government to engage in bulk collection of personal data, including call detail records.[54] The government also uses its FISA authority to collect user data from giant technology companies like Facebook, Skype, Apple, and Google.[55]

A powerful tool for law enforcement, post-9/11 FISA warrants have raised red flags for skirting constitutional protections and thwarting civil rights: Individual lawyers and groups from the ACLU to the ALA have criticized the U.S. government's post-9/11 "surveillance society" as threatening civil liberties and privacy rights.[56] In 2013, Eric Snowden leaked government records revealing that the National Security Administration ("NSA") has invoked Section 702 far beyond its intended scope and collected detailed personal data with no connection to investigations of potential terrorism.[57] A coalition of thirty-two groups decried the expansion of FISA warrants in 2017, pointing to the litany of surveillance abuses and citing due process concerns.[58]

---

or evidence of a crime will be found. *See* GOITEIN & PATEL, *supra* note 45, at 4 (explaining that "under current law, the FISA court does not provide the check on executive action that the Fourth Amendment demands"), at 19 ("the safeguard of judicial review…has eroded to near-nothingness"). AM. LAW DIV., CONG. RESEARCH SERV., PROBABLE CAUSE, REASONABLE SUSPICION, AND REASONABLENESS STANDARDS IN THE CONTEXT OF THE FOURTH AMENDMENT AND THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (Jan. 30, 2006), https://fas.org/sgp/crs/intel/m013006.pdf [https://perma.cc/KV7S-WXHQ].

54. *See, e.g.*, In re Application of the FBI for an Order Requiring the Production of Tangible Things from [redacted], No. BR 08-13, 1 (FISA Ct. Dec. 12, 2008) (ordering production of "telephony metadata"); David S. Kris, *On the Bulk Collection of Tangible Things*, 7 J. NAT'L SEC. L. & POL'Y 209, 211 (2014).

55. Barton Gellman & Lauren Poitras, *Documents: U.S. Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 6, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.c39dd00b03f7 [https://perma.cc/FT8D-U2BK] (reporting on the NSA's PRISM surveillance program, where the NSA collects communications from U.S. internet companies).

56. *See* Hina Shamsi & Alex Abdo, *Privacy & Surveillance Post-9/11*, ABA HUMAN RIGHTS MAGAZINE (2011), https://www.americanbar.org/publications/human_rights_magazine_home/human_rights_vol38_2011/human_rights_winter2011/privacy_and_surveillance_post_9-11.html [https://perma.cc/36Y4-TGM3]; AMER. LIB. ASSOC., RESOLUTION ON THE USA PATRIOT ACT AND LIBRARIES (2005), http://www.ala.org/aboutala/sites/ala.org.aboutala/files/content/wo/reference/colresolutions/PDFs/062905-CD20.6.pdf [https://perma.cc/JEQ5-9XBM].

57. Timothy B. Lee, *Here's Everything We Know About PRISM to Date*, WASH. POST (June 12, 2013), https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/?utm_term=.e43f202d4685 [https://perma.cc/LE3L-K36F] (explaining the NSA's PRISM system, which taps into private communications on various online services under the auspices of FISA's Section 702).

58. When Section 702 was up for reauthorization in 2017, a coalition letter was signed by dozens of lawyer and advocacy organizations to protest H.R. 4478, the bill reauthorizing and broadening the scope of the surveillance law. Coalition Letter on Section 702 Legislation to House Representatives (2017), https://www.aclu.org/letter/coalition-letter-section-702-legislation [https://perma.cc/ZL5M-QEK2]. H.R. 4478 was later advanced as S. 139 and passed in January of 2018. FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, 132 Stat. 3 (2018).

Finally, while FISA is administered by the NSA rather than the Department of Homeland Security ("DHS"), the agency under which ICE operates, there is evidence that ICE has access to FISA surveillance data.[59]

C. ICE's Current Surveillance Apparatus

Whether or not it has access to FISA surveillance data, ICE is gradually accruing its own surveillance program to rival the NSA's. In 2017, ICE entered into a $2.4 million contract with PenLink,[60] a software company whose products help law enforcement track people using "real-time" "live monitoring" through phone data analysis and geolocation data mining and tracking.[61] Julian Sanchez, a surveillance expert at the Cato Institute, said that PenLink's deal with ICE "looks not that different from the language that the NSA used to do bulk collection of telephone records" under the PRISM program.[62] This comparison signals the troubling expansion of immigration policing into surveillance realms previously reserved for tracking suspected international terrorism.

How will ICE use this more robust surveillance technology? If what's past is prologue, ICE will use software like PenLink, as well as biometric recognition technology, to track immigrants and implement policing schemes that profile entire classes of people under the guise of gang affiliation or drug trafficking rather than focusing on individual instances of criminal activity.[63] In 2005, ICE launched "Operation Community Shield," an initiative in which the agency's

59. *See* HOMELAND SECURITY INVESTIGATIONS: NATIONAL SECURITY INVESTIGATIONS HANDBOOK, U.S. IMMIGRATION AND CUSTOMS ENF'T 37–41 (Apr. 26, 2013) (containing a chapter overview of NSA FISA warrants and FISC orders); Betsy Woodruff, *Exclusive: Read the ICE Agent's Guide to NSA Surveillance*, DAILY BEAST (Sept. 28, 2018), https://www.thedailybeast.com/exclusive-read-the-ice-agents-guide-to-nsa-surveillance [https://perma.cc/L2NR-28CG] ("The document strongly suggests that private information obtained using the government's secret spying tools is bleeding into certain ICE investigations." (quoting Patrick Toomey, an attorney for the ACLU's National Security Project)).

60. *Contract Summary for Award HSCETC16C00002*, USASPENDING.GOV, https://www.usaspending.gov/#/award/23844482 [https://perma.cc/CZ4J-LBJX].

61. *PLX Collection and Analysis*, PENLiNK, https://www.penlink.com/plx/ [https://perma.cc/EB6C-WSJ2]; Chantal Da Silva, *ICE Just Launched a $2.4M Contract with a Secretive Data Surveillance Company that Tracks You in Real Time*, NEWSWEEK (June 7, 2018), https://www.newsweek.com/ice-just-signed-24m-contract-secretive-data-surveillance-company-can-track-you-962493 [https://perma.cc/T7VN-TRWS].

62. Da Silva, *supra* note 61.

63. *See* Hannah Rappleye & Lisa Riordan Seville, *Does High-Tech Dragnet to Deport Immigrants Go Too Far?*, NBC (Feb. 28, 2014), https://www.nbcnews.com/news/investigations/does-high-tech-dragnet-deport-immigrants-go-too-far-n40306 [https://perma.cc/WR7H-ZLJZ] (describing the use of biometric data to profile and surveil immigrants); Ali Winston, *Vague Rules Let ICE Deport Undocumented Immigrants as Gang Members*, INTERCEPT (Feb. 17, 2017), https://theintercept.com/2017/02/17/loose-classification-rules-give-ice-broad-authority-to-classify-immigrants-as-gang-members/ [https://perma.cc/58DU-W56J] (describing how ICE uses its ICEGangs database as an arrest and deportation tool, despite the fact that the database mistakenly includes many people with no gang affiliation as a result of flawed criteria).

National Gang Unit[64] combines information gathered by the federal government, third-party data like that sold by Thomson Reuters and RELX, and data from gang databases shared through partnerships with state and local police to identify and crack down on noncitizen "gang members."[65]

The gang databases ICE uses to identify and track noncitizens raise due process concerns due to their notoriously inaccurate information, and the inability of individuals to challenge their inclusion in the stigmatizing databases.[66] Gang databases are riddled with errors that result in law enforcement targeting and criminalizing people with no gang affiliation.[67] The results of Operation Community Shield reveal the accuracy issues inherent to big data policing: as of 2006, 70 percent of immigrants deported under the Operation were never found guilty of a crime.[68] Moreover, these opaque databases give authorities an opportunity to effectively criminalize whoever they please. A federal judge in Washington state recently found that ICE agents who arrested one DACA recipient had lied to two different immigration courts when they asserted that the man was "gang-affiliated."[69] Indeed, false claims of gang involvement are a "routine" part of ICE's deportation strategy.[70]

64. *See National Gang Unit: Operation Community Shield Overview*, U.S. IMMIGRATION AND CUSTOMS ENF'T https://www.ice.gov/national-gang-unit [https://perma.cc/8HFX-TEK8] (last updated June 15, 2017).

65. *Frequently Asked Questions on "Gang Related" Immigration Enforcement*, NAT'L IMMIGR. PROJECT (Oct. 25, 2017), https://www.nationalimmigrationproject.org/PDFs/community/2017_Oct_FAQ-ICE-gang-enforcement.pdf [https://perma.cc/K23Q-DS8Z] (providing a breakdown of data types and sources funneled through the Operation Community Shield program); *see also* Jennifer M. Chacon, *Whose Community Shield?: Examining the Removal of the "Criminal Street Gang Member"*, 2007 U. CHICAGO LEGAL F. 317, 327–30 (2007).

66. *See* Joshua D. Wright, *The Constitutional Failure of Gang Databases*, 2 STAN. J. C.R. & C.L. 115, 115 (2005); NAT'L IMMIGR. PROJECT, *supra* note 65, at 2–3; Winston, *supra* note 63.

67. NAT'L IMMIGR. PROJECT, *supra* note 65, at 3 ("Gang labeling practices by local law enforcement commonly operate with little training, quality control, or uniform standards" with common reasons for designating gang affiliation including tattoos, clothing color, and residence in a high-crime neighborhood.). The CalGang database even contained toddlers' names, listing babies as purported gang members. *See Beware of Gangster Babies: California Database Slammed*, CBS NEWS (Aug. 15, 2016), https://www.cbsnews.com/news/calgang-california-gang-database-slammed-listing-babies-privacy-concerns/ [https://perma.cc/86LL-7N28].

68. AARTI KOHLI & DEEPA VARMA, CHIEF JUSTICE EARL WARREN INST. ON RACE, ETHNICITY, & DIVERSITY, BORDERS, JAILS, AND JOBSITES: AN OVERVIEW OF FEDERAL IMMIGRATION ENFORCEMENT PROGRAMS IN THE U.S. 19 (Feb. 2011), https://www.wilsoncenter.org/sites/default/files/WI_Enforcement_Paper_final_web.pdf [https://perma.cc/CED6-RGAC] (explaining that "the broad discretion allowed in identifying such individuals … may therefore lead to discriminatory practices by law enforcement agencies[,] for example, in the absence of due process requirements or definitions of gang association, police may rely on profiling and stereotyping as a means to identify suspects").

69. Mark Joseph Stern, *Bad Liars*, SLATE (May 16, 2018), https://slate.com/news-and-politics/2018/05/federal-judge-accused-ice-of-making-up-evidence-to-prove-that-dreamer-was-gang-affiliated.html [https://perma.cc/BA2S-ENZX].

70. *See id*. ("ICE routinely alleges that Latinx immigrants with no indication of gang affiliation are members of a gang in order to detain and deport them.").

ICE's reliance on inaccurate data and a lack of proper investigation has regularly led to mistaken arrests, and even deportation, of people with legal status. One recent investigation found that 1,488 immigrants have been wrongly detained by ICE agents since 2012 "based on incomplete government records, bad data and lax investigations."[71] It is particularly troublesome that big data collected and sold by brokers like Thomson Reuters and RELX often contains many errors[72] that unfairly place individuals in legal limbo. Despite these alarming shortcomings, ICE continues to practice big data policing, claiming the tactics are necessary to prevent terrorism, drug trafficking, and other crimes.[73]

Bad data in databases used by ICE is all the more worrisome as concern mounts over ICE's mission.[74] ICE is a controversial vestige of the September 11th attacks: the Homeland Security Act of 2002, which authorized ICE's creation, was passed in tandem with the Patriot Act, as part of a reflexive effort to prevent terrorism.[75] To create ICE, Congress melded the investigative and intelligence resources of the U.S. Customs Service with the investigative, detention, and deportation resources of the Immigration and Naturalization Service ("INS").[76] ICE's mission focused on preventing terrorism and not on

71. Paige St. John & Joel Rubin, *ICE Held an American Man in Custody for 1,273 Days. He's Not the Only One Who Had to Prove His Citizenship*, L.A. TIMES (Sept. 17, 2018), https://www.latimes.com/local/lanow/la-me-citizens-ice-20180427-htmlstory.html [https://perma.cc/JK9T-ASE8**]**.

72. Studies of data brokers' data finds that it is often riddled with errors. In one such study, 71 percent of participants judged that the data about them in different categories and contained in a data broker system were 0 to 50% correct, and in some cases, people found that their data was entirely switched with the data points of another person. John Lucker, Susan K. Hogan & Trevor Bischoff, *Predictably Inaccurate: The Prevalence and Perils of Bad Big Data*, DELOITTE REVIEW (July 31, 2017), https://www2.deloitte.com/insights/us/en/deloitte-review/issue-21/analytics-bad-data-quality.html [https://perma.cc/LC32-XJNV**]**. One reporter found that 50 percent of a data broker report about her was incorrect. Caitlyn Renee Miller, *I Bought a Report on Everything That's Known About Me Online*, ATLANTIC (June 6, 2017), https://www.theatlantic.com/technology/archive/2017/06/online-data-brokers/529281/ [https://perma.cc/8LDS-VWRB].

73. George Joseph, *Where ICE Already Has Direct Lines to Law Enforcement Databases with Immigrant Data*, NPR (May 12, 2017), https://www.npr.org/sections/codeswitch/2017/05/12/479070535/where-ice-already-has-direct-lines-to-law-enforcement-databases-with-immigrant-d [https://perma.cc/8746-XBS3] ("Local and federal law enforcement leaders argue that such data is crucial in carrying out criminal investigations that pose national security or public-safety threats.").

74. Ella Nilsen, *The List of Democrats Calling to Abolish ICE Keeps Growing*, VOX (June 30, 2018), https://www.vox.com/policy-and-politics/2018/6/29/17518176/democrats-to-abolish-ice-movement-gillibrand-de-blasio-ocasio-cortez [https://perma.cc/6VJK-U9VU] (listing politician's criticisms of ICE's mission and actions); Sean McElwee, *It's Time to Abolish ICE*, THE NATION (Mar. 9, 2018), https://www.thenation.com/article/its-time-to-abolish-ice/ [https://perma.cc/PP9Y-MKPA] (arguing for the complete abolition of ICE and insisting "that the core of the agency is broken").

75. *See* Homeland Security Act, Pub. L. No. 107-296, 116 Stat. 2135, 2177–78 (2002); McElwee, *supra* ("ICE was a direct product of the post-September 11 panic culture . . . [b]y putting ICE under the scope of DHS, the government framed immigration as a national security issue rather than an issue of community development, diversity or human rights.").

76. Homeland Security Act, Pub. L. No. 107-296, 116 Stat. 2135, 2177–78 (2002).

wide-scale surveillance of immigrants.[77] But where previous administrations had directed ICE to focus on "serious criminals" who threaten national security and public safety, in 2017 the Trump Administration issued an executive order directing the agency to instead prioritize all undocumented immigrants for removal, including those with no criminal history.[78] The executive order shifted ICE's focus to the interior of the country, empowering them to seek out unauthorized immigrants in their communities rather than simply stopping unauthorized passage at the border.[79]

ICE's controversial mission to target all undocumented immigrants makes it particularly unsettling that the agency is building an invasive surveillance system as the backbone of its "deportation machine."[80] A surveillance system built up during the Obama administration is now being deployed with animus:[81] Under Trump, ICE agents are a "bullying squad," rounding up immigrants and engaging in ethically fraught practices fueled by surveillance.[82] This surveillance data supplements the information that the U.S. government collects through visa petitions[83] and immigration forms.[84] These traditional visitor and immigration

77. CHAD C. HADDAL, CONG. RESEARCH SERV., BORDER SECURITY: KEY AGENCIES AND THEIR MISSIONS 3 (Jan. 26, 2010), https://fas.org/sgp/crs/homesec/RS21899.pdf [https://perma.cc/MW6F-7SWJ] ("ICE's mission is to detect and prevent terrorist and criminal acts by targeting the people, money, and materials that support terrorist and criminal networks"); Brian A. Reaves, *Federal Law Enforcement Officers, 2004*, BUREAU OF LABOR AND MANAGEMENT STATISTICS BULLETIN, at 2 (July 2006) ("The primary mission of ICE is to prevent acts of terrorism by targeting the people, money, and materials that support terrorist and criminal activities.").

78. Exec. Order No. 13768, 82 Fed. Reg. 8799, 8800 (Jan. 25, 2017).

79. *Summary of Executive Order "Enhancing Public Safety in the Interior of the United States,"* AMERICAN IMMIGRATION COUNCIL (May 19, 2017), https://www.americanimmigrationcouncil.org/immigration-interior-enforcement-executive-order [https://perma.cc/Z9NM-AGXM].

80. As ICE ramps up its immigration enforcement efforts, the phrase "deportation machine" has been used to describe the new form and function of the agency. *See* AMERICAN IMMIGRATION LAWYERS ASSOCIATION, COGS IN THE DEPORTATION MACHINE 2 (Mar. 12, 2018), https://www.aila.org/infonet/aila-report-cogs-in-the-deportation-machine [https://perma.cc/4XUR-5VEG].

81. Alvaro M. Bedoya, *Deportation is Going High-Tech Under Trump*, ATLANTIC (June 21, 2017), https://www.theatlantic.com/technology/archive/2017/06/data-driven-deportation/531090/ [https://perma.cc/454G-P5R9] ("Under Barack Obama, ICE went high-tech. At the heart of that shift were biometrics: precise, digitized measurements of immigrants' bodies. Obama ramped up a Bush-era program, Secure Communities, which sent booking fingerprints from local jails to the Department of Homeland Security, shunting hundreds of thousands of undocumented and *legal* immigrants, many arrested for minor offenses, into federal deportations").

82. Michael Gerson, *ICE Has Become Trump's Personal Bullying Squad*, WASH. POST (Apr. 23, 2018), https://www.washingtonpost.com/opinions/ice-has-become-trumps-personal-bullying-squad/2018/04/23/5197541e-472d-11e8-8b5a-3b1697adcc2a_story.html?utm_term=.97855a8cc818 [https://perma.cc/AA5H-VXLC]; Bedoya, *supra* note 81.

83. *See generally* 8 U.S.C. §§ 1201–1202 (requiring collection of data along with visa application, including documents and physical examination of applicants).

84. *See generally* 8 U.S.C. §§ 1301–1306 (regarding registration of noncitizens, including fingerprinting); 8 U.S.C. §§ 1421–1458 (including provisions requiring applications for citizenship and investigations of prospective citizens as well as prerequisite tests and oaths and certifications).

forms already collect copious personal data including addresses, education levels, and even fingerprints.[85]

Predictably, the combination of ICE's sweeping new directive to arrest any unauthorized immigrant and its enhanced surveillance capacities has led to soaring immigration enforcement numbers. ICE arrests increased 30 percent from 2016 to 2017,[86] and increased another 11 percent in 2018.[87] More troubling still, ICE contracts signed during the Trump administration indicate that surveillance will play an even larger role in future ICE enforcement efforts.[88]

To help fund more ICE surveillance initiatives, the federal government is funneling money into the ICE deportation machine. Funds are being redirected to ICE from other DHS offices like FEMA and the Coast Guard.[89] Flush with

85. *See, e.g.*, 8 U.S.C. § 1187 (requiring transmission of passenger data for people entering the U.S. under the visa waiver program); Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. 107-173, 116 Stat. 543 (codified at 8 U.S.C. §§ 1701–1778) (establishing, among other programs, a reporting requirement for universities accepting foreign students). Even these routine form processes have become more invasive in recent years. In 2014, U.S. Customs and Border Patrol added data requirements to the Visa Waiver Form requirements so that people visiting the U.S. under that program must provide even more personal data for an advanced authorization before they can cross the border. *Strengthening Security of the VWP Through Enhancements to ESTA*, U.S. Customs & Border Prot. (Nov. 4, 2014), https://www.cbp.gov/travel/international-visitors/esta/enhancements-to-esta-faqs [https://perma.cc/7TQH-QY6J]. Refugees must also undergo strenuous background checks. *See* Kalhan, *supra* note 7, at 15, 42–43.

86. Kristen Bialek, *ICE Arrests Went Up in 2017, with Biggest Increases in Florida, Northern Texas, Oklahoma*, PEW RESEARCH CTR. (Feb. 8, 2018), http://www.pewresearch.org/fact-tank/2018/02/08/ice-arrests-went-up-in-2017-with-biggest-increases-in-florida-northern-texas-oklahoma/ [https://perma.cc/78Z8-4GJL].

87. Ron Nixon, *Immigration Arrests and Deportations Are Rising, I.C.E. Data Show*, N.Y. TIMES (Dec. 14, 2018), https://www.nytimes.com/2018/12/14/us/politics/illegal-immigrant-arrests-deportations-rise.html?login=email&auth=login-email [https://perma.cc/QVU5-WKKA].

88. For example, one Thomson Reuters contract with ICE requires Thomson Reuters to supply "subscription data services" containing a variety of personal records ranging from employment and credit, to vehicle registration and wireless phone account data. *Notice of Intent to Sole Source TRSS Subscription Data Services*, FED. BUS. OPP. (2018) https://www.fbo.gov/index?s=opportunity&mode=form&id=71911de5fa638ed0a391f01f520c0e2a&tab=core&_cview=1 [https://perma.cc/XX8S-AWF9] (containing a link to the SOW Subscription, which details the type of data to be provided); AJ Dellinger, *It Turns Out All Kinds of Tech Companies Are Working With ICE*, GIZMODO (June 20, 2018), https://gizmodo.com/turns-out-all-kinds-of-tech-companies-are-working-with-1827006046 [https://perma.cc/DR5H-AT28]. Thomson Reuters data and technology are only a part of ICE's growing surveillance "ecosystem" that collects and connects massive amounts of data. *See* Joan Friedland, *Information Vacuuming: The Trump Administration is Collective Massive Amounts of Data for Its Immigrant Surveillance and Deportation Machine*, NATIONAL IMMIGRATION LAW CENTER (Aug. 22, 2018), https://www.nilc.org/2018/08/22/information-vacuuming-immigrants-and-citizens/ [https://perma.cc/JA2M-36VV]. ICE's surveillance system exploits extremely powerful national security surveillance tools to find nonthreatening immigrants and arrest them. For example, ICE used a Stingray—a foreign intelligence technology that simulates a cell tower in order to track an individual by their cell phone—to find a 23-year-old restaurant worker from El Salvador to deport him, not to locate a terrorism suspect, as the tool is intended to be used. Bedoya, *supra* note 81.

89. *See* Tal Kopan, *It's Not Just FEMA: ICE Quietly Got an Extra $200 Million*, CNN (Sept. 12, 2018), https://www.cnn.com/2018/09/12/politics/ice-more-money-fema-dhs/index.html

government funding and support, ICE is on a surveillance shopping spree, spending tens of millions of dollars on the most invasive technology available.[90] For instance, ICE is paying Palantir, a data technology firm, over $50 million to create a system that will sift through data from intelligence platforms, allowing "agents to access a vast 'ecosystem' of data to facilitate . . . in both discovering targets and then creating and administering cases against them."[91]

In practice, ICE's surveillance technology and police powers in immigration enforcement create scenes that could be found in a dystopian novel. Since its inception in 2003, ICE has evolved from an organization focused on the targeted policing of serious crimes to one implementing a surveillance dragnet that uses technology to indiscriminately surveil, target, arrest, and detain immigrants in their communities regardless of their criminal history, in accordance with Trump's executive order.[92] For example, in 2017, ICE officers stopped at a

[https://perma.cc/4636-ZM7X].

90. *See, e.g.*, *Who Supplies the Data, Analysis, and Tech Infrastructure to U.S. Immigration Authorities?* PRIVACY INT'L (Aug. 9, 2018), https://privacyinternational.org/feature/2216/who-supplies-data-analysis-and-tech-infrastructure-us-immigration-authorities [https://perma.cc/3XBU-P2UL]; Dellinger, *supra* note 88; Chantal Da Silva, *ICE Just Launched a $2.4 Million Contract with a Secretive Data Surveillance Company That Tracks You In Real Time*, NEWSWEEK (June 7, 2018), https://www.newsweek.com/ice-just-signed-24m-contract-secretive-data-surveillance-company-can-track-you-962493 [https://perma.cc/Z4V2-C49L]; Thomas Brewster, *Trump's Immigration Cops Just Spent $3 Million on These Ex-DARPA Social Media Miners*, FORBES (Sept. 27, 2017), https://www.forbes.com/sites/thomasbrewster/2017/09/27/trump-immigration-social-media-surveillance-giant-oak-penlink-palantir/#6e5f07ee3e3b [https://perma.cc/6JA5-G6R6].

91. Sam Biddle & Spencer Woodman, *These are the Technology Firms Lining Up Build ICE's 'Extreme Vetting' Program*, INTERCEPT (Aug. 7, 2017), https://theintercept.com/2017/08/07/these-are-the-technology-firms-lining-up-to-build-trumps-extreme-vetting-program/ [https://perma.cc/7VTX-5N5Y]; Dellinger, *supra* note 88.

92. Daniel Oberhaus, *ICE Modified its "Risk Assessment" Software So It Automatically Recommends Detention*, MOTHERBOARD (June 26, 2018), https://motherboard.vice.com/en_us/article/evk3kw/ice-modified-its-risk-assessment-software-so-it-automatically-recommends-detention [https://perma.cc/5BHK-6FAK] (reporting on new settings in ICE's Risk Classification Assessment program which now automatically recommends detention conforming to Trump's "zero tolerance" stance and leads to an increase in the detention of people with little or no criminal history); Nick Miroff & Maria Sacchetti, *Trump Takes "Shackles" Off ICE, Which is Slapping Them on Immigrants Who Thought They Were Safe*, WASH. POST (Feb. 11, 2018), https://www.washingtonpost.com/world/national-security/trump-takes-shackles-off-ice-which-is-slapping-them-on-immigrants-who-thought-they-were-safe/2018/02/11/4bd5c164-083a-11e8-b48c-b07fea957bd5_story.html?utm_term=.f6ef0b26d0dc [https://perma.cc/KM6Z-8373] (reporting that ICE arrests have surged 40% under the Trump administration, and claiming that ICE made 37,734 "noncriminal" arrests in the 2017 fiscal year, more than twice the number from the previous year); Caitlin Dickerson, *Immigration Arrests Rise Sharply as a Trump Mandate is Carried Out*, N.Y. TIMES (May 17, 2017), https://www.nytimes.com/2017/05/17/us/immigration-enforcement-ice-arrests.html [https://perma.cc/JC77-M6WS]. The mandate referred to in the title is the rescinding of Obama era rules that prioritized arrests of "serious criminals," rather than applying ICE enforcement across all undocumented populations, regardless of the seriousness of crimes, opening enforcement to people committing minor infractions and misdemeanors. *Id*. *See also* Memorandum from John Kelly, Secretary, Department of Homeland Security (Feb. 20, 2017), https://www.dhs.gov/sites/default/files/publications/17_0220_S1_Enforcement-of-the-Immigration-Laws-to-Serve-the-National-Interest.pdf [https://perma.cc/Y6TA-Y955] (mandating changes in immigration enforcement priorities).

Michigan restaurant, ate breakfast, complimented the chef on their meals, and then proceeded to arrest three restaurant employees.[93] In another case, a 10-year old girl with cerebral palsy, who had lived in the U.S. since she was three months old, was detained immediately after she had surgery—ICE agents tracked and located her at 2 a.m. as an ambulance transported her between hospitals.[94] In New York, ICE agents arrested a high schooler hours before his senior prom,[95] as well as a couple visiting their son-in-law, a sergeant in the U.S. Army, on the Fourth of July.[96] ICE's inhumane tactics have led many to believe the agency is out of control.[97]

As ICE's role creeps beyond its original mission of securing the public safety into the detainment and removal of noncitizens who do not pose a threat to the public and who are on a pathway to legal citizenship, people have decried the agency's actions on legal and ethical grounds.[98] Lawyers have condemned instances of ICE enforcement as unconstitutional and unethical, and as shaping a national immigration policy that violates common decency.[99] What many of these attorneys do not know is that ICE enforcement is bolstered by an ever-growing big data surveillance structure, and that their legal research

93. Associated Press, *ICE Agents Eat Breakfast, Compliment Chef, then Arrest Three Workers at Michigan Restaurant*, CHI. TRIB. (May 27, 2017), http://www.chicagotribune.com/news/nationworld/midwest/ct-michigan-restaurant-immigration-arrests-20170525-story.html [https://perma.cc/4YJ9-V5JX].

94. Lia Eustachewich, *Girl with Cerebral Palsy Detained by Immigration Agents After Surgery*, N.Y. POST (Oct. 26, 2017), https://nypost.com/2017/10/26/girl-with-cerebral-palsy-detained-by-ice-agents-after-surgery/ [https://perma.cc/YT86-FYAX].

95. Michael P. McKinney & Jorge Fitz-Gibbon, *ICE Agents Arrest High Schooler Hours Before Prom*, USA TODAY (June 9, 2017), https://www.usatoday.com/story/news/nation-now/2017/06/09/high-school-student-immigration-arrest/385457001/ [https://perma.cc/JA7J-YUQ7].

96. Samantha Schmidt, *A Couple Visited Their Soldier Son-In-Law on July 4. The Army Turned Them Over to ICE.*, WASH. POST (July 10, 2018), https://www.washingtonpost.com/news/morning-mix/wp/2018/07/10/a-couple-visited-their-soldier-son-in-law-on-july-4-the-army-turned-them-over-to-ice/?noredirect=on&utm_term=.322e768c6639 [https://perma.cc/635A-586T].

97. Trevor Timm, *Ice Agents Are Out of Control. And They Are Only Getting Worse.*, THE GUARDIAN (May 31, 2017), https://www.theguardian.com/commentisfree/2017/may/31/ice-agents-out-of-control-immigration-arrests [https://perma.cc/ZR4M-QDG4]; Sean McElwee, *The Power of 'Abolish ICE'*, N.Y. TIMES (Aug. 4, 2018), https://www.nytimes.com/2018/08/04/opinion/sunday/abolish-ice-ocasio-cortez-democrats.html [https://perma.cc/5E49-8645].

98. *See, e.g.*, Stern, *supra* note 69.

99. *See, e.g.*, Chantal Da Silva, *Cuomo to ICE: No More "Reckless" Immigration Raids In New York, Or We'll Sue*, NEWSWEEK (Apr. 26, 2018), http://www.newsweek.com/cuomo-ice-no-more-immigration-raids-new-york-or-well-sue-901812 [https://perma.cc/B8NV-3TZH]; Press Release, Am. Immigration Lawyers Assoc., Missouri-Kansas Immigration Attorneys Condemn ICE Officer's Actions (June 27, 2018), https://www.aila.org/infonet/missouri-kansas-immigration-attorneys-condemn-ice [https://perma.cc/7XXS-W6UG]; Nora Flaherty, *Dozens of Maine Lawyers Condemn ICE Arrest at Courthouse*, MAINE PUBLIC RADIO (Apr. 10, 2017), http://www.mainepublic.org/post/dozens-maine-lawyers-condemn-ice-arrest-courthouse [https://perma.cc/FLL2-L8BP].

subscriptions may be facilitating the very same ICE practices they condemn.

II.
LEGAL RESEARCH COMPANIES' ROLES IN ICE SURVEILLANCE

Both Thomson Reuters and RELX Group, the companies that provide the legal research tools Westlaw and Lexis, respectively, contract with ICE to supply the agency with vast quantities of personal data and analytic tools to mine that data.[100] The companies' eagerness to support immigration enforcement surveillance should raise an ethical red flag for lawyers, and especially for those who work in defense of clients targeted by law enforcement.

A. Corporate Models Shift Toward Information Sales

Westlaw and LexisNexis have invested in keeping their legal product lines ahead of the pack, incorporating artificial intelligence into their search functions[101] and creating new modes of analyzing case law.[102] Yet, even with these updates, their expensive products must now compete with a proliferation of new, improved, free or low-cost online research resources.[103] At the same time,

100. Woodman, *supra* note 91; Ben Collins & Meghan Sullivan, *Tech Companies Quietly Work with ICE as Border Crisis Persists*, NBC NEWS (June 20, 2018), https://www.nbcnews.com/tech/tech-news/tech-companies-quietly-work-ice-border-crisis-continues-n885176 [https://perma.cc/9R4H-V2Q4]. Thomson Reuters and its subsidiary, West Publishing, have already made tens of millions of dollars from ICE contracts. *See, e.g.*, *Contract Summary for Award ID HSCEMD17F00008*, USASPENDING.GOV, https://www.usaspending.gov/#/award/23831008 [https://perma.cc/5M68-BN87] (CLEAR contract); *Contract Summary for Award ID HSBP1015P00702*, USASPENDING.GOV, https://www.usaspending.gov/#/award/23779955 [https://perma.cc/VG5H-PSEU] (Thomson Reuters Database Access); *Contract Summary for Award ID HSCEDM16P00082*, USASPENDING.GOV, https://www.usaspending.gov/#/award/23822745 [https://perma.cc/76GG-9FJW] (TRSS database access); *Contract Summary for Award ID 70CDCR18P00000048*, USASPENDING.GOV, https://www.usaspending.gov/#/award/62503110 [https://perma.cc/KK73-B3WV] (TRSS subscription service); DHS, Office of Acquisition Management Investigations & Operations Support Dallas, *Limited Source Justification*, http://www.mediafire.com/file/y2e3vk65z6v3k6x/LSJ_Final.pdf [https://perma.cc/BC93-6ASL] (Thomson Reuters system to system connection between CLEAR database and Palantir). RELX Group also contracts with ICE. Its LexisNexis Accurint databases are "mission-critical" to ICE's Fugitive Operations Support Center, which tracks "fugitive and other high priority" targets for arrest and deportation. William Quigley, *ICE Will Utilize LexisNexis Databases to Track Down Fugitive Aliens*, GOVERNMENT SEC. NEWS (Sept. 11, 2013), https://www.gsnmagazine.com/article/33053/ice_will_utilize_lexisnexis_databases_track_down_f [https://perma.cc/XFT9-NVZB]. *See infra* note 133 for current Lexis contracts with ICE.

101. Press Release, Thomson Reuters, Thomson Reuters Reveals New Legal Research Platform with Advanced AI: Westlaw Edge (July 12, 2018), https://www.thomsonreuters.com/en/press-releases/2018/july/thomson-reuters-unveils-new-legal-research-platform-with-advanced-ai-westlaw-edge.html [https://perma.cc/VR9K-T3V7] (introducing Westlaw's foray into AI-driven legal research).

102. Bob Ambrogi, *Putting a "Stake in the Ground" to Claim the Legal Analytics Space*, LAWSITES (July 13, 2018), https://www.lawsitesblog.com/2018/07/lexisnexis-launches-lexis-analytics-putting-stake-ground-claim-legal-analytics-space.html [https://perma.cc/3J7Q-UGVJ].

103. Legal technology incubators and government initiatives are developing low cost and

the print products that lawyers formerly relied on, like case reporters and digests, are waning in popularity.[104] Law libraries across the nation are tossing their print collections, especially volumes of primary legal sources like cases and statutes which have historically been the cornerstones of LexisNexis and Westlaw's legal publishing empires.[105] Many law firm libraries are shrinking their book collections[106] and switching from pricey electronic databases to cheaper alternatives.[107] Reflecting this trend, both RELX Group[108] and Thomson Reuters have shifted their business models away from traditional publishing and into the provision of digital data services.[109] Their former profit sources—print resources and the proprietary ownership of legal and academic materials—are being outmoded by online and open access resources as scholars who provide Thomson Reuters and RELX Group with proprietary materials push back on companies profiting off of their unpaid labor.[110] These companies' profit models

open access alternatives to the Wexis duopoly. Jobst Elster lists legal research as one of the startup technologies being developed in legal tech incubators. *See* Jobst Elster, *Start Me Up…I'll Never Stop*, LEGAL IT TODAY (June 10, 2015) https://insidelegal.typepad.com/files/2015/06/Legal%20Technology%20Startups%20Article-Legal%20IT%20Today-June%202015-Jobst%20Elster.pdf [https://perma.cc/6LY7-X7BV**]**.

104. Law librarians predict that print resources will be replaced by online resources within the decade. Sarah Gotschall, *The Year 2027: The Future of Academic Law Libraries/Librarians*, RIPS LAW LIBRARIAN BLOG (Jan. 16, 2018), https://ripslawlibrarian.wordpress.com/2018/01/16/the-year-2027-future-of-academic-law-libraries-librarians/ [https://perma.cc/Y7SR-GM8R].

105. Kimberly Mattioli, *Access to Print, Access to Justice*, 110 LAW L. J. 31, 35 (2018) (citing PRIMARY RESEARCH GROUP, LAW LIBRARY PLANS FOR THE PRINT MATERIAL COLLECTION (2015)).

106. Mark Giagrande, *Study Examines the Shrinking Print Collection in Law Libraries*, LAW LIBRARIAN BLOG (Aug. 31, 2015), https://llb2.com/2015/08/31/study-examines-the-shrinking-print-collection-in-law-libraries/ [https://perma.cc/93LV-YHH4] (describing a study projecting law firm spending on print resources to drop 22.6% from 2014-2016).

107. Lisa Needham, *Lexis Legal Research Comes Out Swinging Against Lower Cost Legal Research Services*, LAWYERIST.COM (May 2, 2017), https://lawyerist.com/lexis-legal-research-services-lashes-out/ [https://perma.cc/4X25-HBTL] (noting that Lexis and Westlaw are fighting to maintain consumer loyalty as new low-cost alternatives emerge).

108. In 2017, RELX reported that it had to offset the declining print products market by evolving into "information analytics" and moving away from the traditional publishing industry. Katherine Cowdrey, *Elsevier Profits up 3% Despite 'Steeper' Print Declines*, THE BOOKSELLER (Feb. 23, 2017), https://www.thebookseller.com/news/elsevier-profits-3-despite-steeper-print-declines-493781 [https://perma.cc/G7F9-MN6R]. RELX's 2017 Annual Report shows that print revenue decreased by 53% from 2000-2017. RELX GROUP, ANNUAL REPORTS AND FINANCIAL STATEMENTS 2017, at 6 (2018), https://www.relx.com/~/media/Files/R/RELX-Group/documents/reports/annual-reports/relx2017-annual-report.pdf [https://perma.cc/M4ZQ-RJ5B] [hereinafter RELX ANNUAL REPORT].

109. Thomson Reuter's similarly reported declining print sales:

As expected, we have also continued to experience a decline in U.S. Legal's print revenues as customers increasingly migrate to our online offerings…Technology is also changing how lawyers work and the evolving regulatory landscape is enabling new types of legal services," so the company is "allocating greater amounts of capital to our solutions offerings within the Legal business that [the company] believe[s] present the highest growth opportunities…" THOMSON REUTERS 2017 ANNUAL REPORT, *supra* note 3, at 18.

110. The writers of legal treatises and secondary sources do not profit from their work when

have also contributed to worsening customer relations with their legal customers.[111] Still, legal professionals rely so heavily on Westlaw and Lexis for their work that law librarians, the gatekeepers for these products in law schools and many law firms, have refused to discuss controversial Westlaw and LexisNexis practices for fear of upsetting the companies.[112] For instance, even as LexisNexis was widely criticized for engaging in coercive sales practices, legal professionals continued to use the product and the company's profit margins remained strong.[113]

As the traditional legal publication market shrinks, the market for big data policing services is quickly growing.[114] Indeed, Thomson Reuters and RELX Group have found a new cash cow in law enforcement surveillance.[115] The

Thomson Reuters and Reed Elsevier publish it. Over the last decade, academic writers have fought against these publishers and turned to open access publishing options, and large academic institutions are pushing back on Reed Elsevier's publishing model, refusing to sign contracts with the company. *See* Holly Else, *Europe's Open-Access Drive Escalates as University Stand-offs Spread*, NATURE (May 17, 2018), https://www.nature.com/articles/d41586-018-05191-0 [https://perma.cc/3UJS-2SQ5]; Peter W. Martin, *Possible Futures for the Legal Treatise in an Environment of Wikis, Blogs, and Myriad Online Primary Sources*, 108 L. LIB. J. 7, 32 (2016).

111. *See, e.g.*, Jean O'Grady, *The Law Librarians Revolt: AALL Accuses LexisNexis of Engaging in Unfair Business Practices – Possible Antitrust Violations*, DEWEY B STRATEGIC (June 17, 2018), https://www.deweybstrategic.com/2018/06/law-librarians-revolt-aall-accuses-lexisnexis-engaging-unfair-business-practices.html [https://perma.cc/PGV7-FBK8] (detailing law librarians' dissatisfaction with LexisNexis' growing use of product bundling, a practice wherein LexisNexis forces law libraries to purchase subscriptions to expensive unwanted services in order to gain access to essential traditional legal news sources and print books and treatises).

112. When I first learned about the surveillance issue, I brought it to the attention of the legal research community through a post published on an American Association of Law Libraries ("AALL") blog. Within hours of posting, it was taken down, censored by AALL for fear of upsetting LexisNexis, and law library professionals were prohibited from discussing the surveillance issue on any AALL forums. Joe Hodnicki agreed to publish the commentary on his Law Library Blog, but the topic has been a sensitive one among law librarians, who fear that speaking out may harm their Westlaw and Lexis contracts or get them in trouble with the academic institutions and law firms where they work. *See* Sarah Lamdan & Joe Hodnicki, *Surveillance and Legal Research Providers: What You Need to Know*, LAW LIB. BLOG (July 9, 2018), https://llb2.com/2018/07/09/surveillance-and-legal-research-providers-what-you-need-to-know/ [https://perma.cc/LJF5-E5P7].

113. *See* RELX ANNUAL REPORT, *supra* note 108, at 5 (2018), https://www.relx.com/~/media/Files/R/RELX-Group/documents/reports/annual-reports/relx2017-annual-report.pdf [https://perma.cc/M4ZQ-RJ5B] (Chief Executive Officer Erik Engstrom noted that "[w]e achieved good underlying revenue growth in 2017, and continued to generate underlying operating profit growth ahead of revenue growth.").

114. RELX Group touts its "big data" initiatives and a growing demand for RELX solutions to "combat criminal activities." *Id*. at 22. It's Public Safety Data Exchange already serves over 1,300 law enforcement agencies and RELX has created an "Accurint Virtual Crime Center" policing platform to "accelerate criminal investigations." *Id*. at 21.

115. *See id*. at 10–11, 42 (touting the success of RELX's "High Performance Computer Cluster"—its big data technology). RELX Group's 2017 Annual Report also shows that their risk and business analytics products brought in 2.1 billion pounds, or about 2.7 billion dollars. *Id*. at 23. It also touts its contributions to big data policing through its LexisNexis Accurint Crime Analysis tool as part of its corporate responsibility. *Id*. at 42. *See also* THOMSON REUTERS 2017 ANNUAL REPORT, *supra* note 3, at 14 (describing Thomson Reuters Labs as an R&D effort to build better AI, Machine Learning, and Cognitive Computing systems). RELX Group does separate its big data

companies have both turned to data brokering from traditional legal and academic publishing.

As commercial data brokers, RELX Group and Thomson Reuters aggregate and resell individualized data. At the beginning of the information supply chain, individuals provide their personal information to various government entities[116] and share their online consumer data and location data with software companies, who sell the bundled data to firms specializing in data tracking.[117] Powerful data aggregators like Thomson Reuters and RELX Group then purchase and consolidate the information held by individual data tracking firms, along with further data gleaned from public records, to create an informational mosaic describing millions of different people in great detail.[118] Through this supply chain, Thomson Reuters and RELX Group hold stores of personal data including public records held by local, state, and federal governments, online data including individuals' use of social networks, blogs, chat rooms, lists of relatives and associates, and any other data they can purchase or collect.[119] These brokers then sell these detailed individualized databases to businesses and law enforcement.

RELX Group and Thomson Reuters have been gradually pivoting towards the law enforcement data market for over a decade. In 2004, RELX Group, LexisNexis's parent company, then called Reed Elsevier, purchased Accurint, one of the country's largest public records databases.[120] With the addition of Accurint to LexisNexis services, law students could use Lexis's public records

surveillance product revenues from legal product revenues, reporting 2.1 billion pounds in profit from its surveillance data products compared to 1.7 billion pounds in profit from RELX legal products. RELX ANNUAL REPORT, *supra* note 116, at 23, 31. RELX Group risk analytics "big data" products' revenue grew 8 percent from 2016-2017, and the legal product growth was only 2 percent. *Id*.

116. Data that federal, state, and local governments collect through various programs end up in data brokers' collections. Records from state departments of motor vehicles, voting records, and other points of contact between individuals and government entities are bought and sold by data brokers. Lois Beckett, *Everything We Know About What Data Brokers Know About You*, PROPUBLICA (June 13, 2014), https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you [https://perma.cc/HY3V-N5FP].

117. Kirsten E. Martin, *Ethical Issues in the Big Data Industry*, MIS Q. EXECUTIVE 70–71 (June 2015), http://kirstenmartin.net/wp-content/uploads/2013/11/Martin-MISQE-Big-Data-Ethics-2015.pdf [https://perma.cc/M3WV-XN95] (describing the "big data" supply chain).

118. *Id*.

119. Meghan Koushik, *Data Brokers Know a Lot About You, But What Do you Know About Them?*, BRENNAN CTR. FOR JUSTICE (Oct. 31, 2014), https://www.brennancenter.org/blog/data-brokers-know-lot-about-you-what-do-you-know-about-them [https://perma.cc/8AX7-R7FH]; *see also Public Records Privacy Statement*, THOMSON REUTERS (Jan. 15, 2019), https://legal.thomsonreuters.com/en/legal-notices/privacy-records?CID=TRSite [https://perma.cc/CX3N-HW78] (last updated Jan. 15, 2019) (identifying Thomson Reuters' data sources broadly as a collection of data from public records and non-public information from government agencies and third party private data providers).

120. *Reed Elsevier's LexisNexis Acquires Seisint for $775 Million*, SPECTRUM EQUITY (July 2004), https://www.spectrumequity.com/news/reed-elseviers-lexisnexis-acquires-seisint-for-775-million [https://perma.cc/M4AW-3CUK].

search to check up on old friends and love interests. In 2005, one legal scholar described the ease with which one could use systems like Accurint to covertly acquire information about people without any sort of legal authorization: "[t]he easiest way to get useful data is to contact one of the many companies, usually called commercial data brokers ("CDBs"), that use computers and the internet to dig up 'dirt' from public and not-so public records."[121]

Today, RELX Group has amassed over 78 billion public records from over 10,000 diverse sources.[122] In 2015, Reed Elsevier officially rebranded itself as RELX Group,[123] and in 2018 it purchased ThreatMetrix, a cybersecurity company that specializes in tracking and authenticating people and their online activities.[124] Technology reporters called RELX Group's cyber-tracking company purchase "an interesting development, considering the company's roots in educational and scientific publishing,"[125] but an RELX representative characterized the acquisition as "in line with our organic growth driven strategy, supported by acquisitions of targeted data sets and analytics that are natural additions to our existing business."[126]

Thomson Reuters, Westlaw's parent company, has similarly positioned itself to compete in the surveillance data and technology market. Thomson Reuters Special Services was created to market Thomson Reuters' surveillance products, and it has worked to create a positive relationship with ICE. This branch of Thomson Reuters employs several former ICE officials in high-ranking positions[127] and its CEO, Stephen Rubley, is a board member of the ICE Foundation, a nonprofit organization that "supports the men and women of ICE."[128]

In 2008, Reed Elsevier had created such a powerful data empire that the

121. Christopher Slobogin, *Transaction Surveillance*, 75 MISS. L. J. 142, 143–44 (2005).

122. *Cast a Wider Net with our Powerful Public Records Search*, LEXISNEXIS, https://www.lexisnexis.com/en-us/products/public-records/powerful-public-records-search.page [https://perma.cc/56VQ-PV76].

123. Jamie Dunkley, *Reed Elsevier Rebrands as RELX and Overhauls Corporate Structure*, EVENING STANDARD (Feb. 26, 2015), https://www.standard.co.uk/business/business-news/reed-elsevier-rebrands-as-relx-and-overhauls-corporate-structure-10072098.html [https://perma.cc/3HJT-43L5].

124. Ingrid Lunden, *Relx Acquires ThreatMatrix for $817M to Ramp Up in Risk-Based Authentication*, TECHCRUNCH (Jan. 29, 2018), https://techcrunch.com/2018/01/29/relx-threatmetrix-risk-authentication-lexisnexis/ [https://perma.cc/C4U3-7MU3].

125. *Id*.

126. *RELX Group Announces Definitive Agreement to Acquire ThreatMatrix*, BUSINESSWIRE (Jan. 29, 2018), https://www.businesswire.com/news/home/20180128005093/en/RELX-Group-Announces-Definitive-Agreement-Acquire-ThreatMetrix [https://perma.cc/27GD-UF9D].

127. Patrick Michels, *ICE Plans to Outsource Data Collection on 500,00 People a Month*, REVEAL (Aug. 25, 2017), https://www.revealnews.org/article/ice-plans-to-outsource-data-collection-on-500000-people-a-month/ [https://perma.cc/Y5KP-GEU2] (reporting that TRSS employs former ICE officials "including James Dinkins, a vice president and general manager, and its general counsel, Peter Vincent").

128. Ben Collins & Meghan Sullivan, *supra* note 108; ICE Foundation, *What We Do*, https://icefoundation.org/what-we-do/ [https://perma.cc/J6VL-A4ES] (last visited July 1, 2018).

Federal Trade Commission ("FTC") was compelled to intervene, splitting the data giant's holdings to prevent the creation of a monopoly. First acknowledging that Thomson Reuters and Reed Elsevier had already formed a duopoly on surveillance data brokering,[129] the FTC forced Reed Elsevier to divest assets related to ChoicePoint's AutoTrack XP and Consolidated Lead Evaluation and Reporting (CLEAR) electronic public records services to Thomson Reuters to comply with anti-trust laws.[130] Thomson Reuters took CLEAR and ran with it, building a powerful investigation tool that links together millions of databases brimming with public and proprietary records.[131]

B. Contracting with ICE

Both Thomson Reuters and RELX Group contract directly with ICE to provide the agency with their informational services. RELX operates as both a direct and indirect source of information for ICE operations. As early as 2013, ICE has purchased direct access to RELX databases to help track immigrants as part of its Fugitive Operations program.[132] Notably, the size of ICE's contract with RELX increased between 2017 and 2018, a shift that ICE attributed to the executive order expanding the scope of immigration enforcement.[133] In addition to its direct arrangement with ICE, RELX retains over 1,300 contracts with other law enforcement agencies.[134] These relationships likely serve as an indirect source of RELX data for ICE, as ICE's law enforcement information sharing initiative draws data from law enforcement entities across the nation.[135]

129. Press Release, FTC, FTC Challenges Reed Elsevier's Proposed $4.1 Billion Acquisition of ChoicePoint, Inc. (Sept. 16, 2008), https://www.ftc.gov/news-events/press-releases/2008/09/ftc-challenges-reed-elseviers-proposed-41-billion-acquisition [https://perma.cc/WB5W-8QXA].

130. *Id*. Before it was purchased, Choicepoint was already a widely-depended-on commercial data broker for law enforcement agencies, who could use it "to obtain a comprehensive dossier on almost any adult." Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 595–96 (2003).

131. *CLEAR System-to-System*, THOMSON REUTERS, https://legal.thomsonreuters.com/en/products/clear-investigation-software/system-to-system [https://perma.cc/V43L-2Y5K].

132. The collaboration between ICE and LexisNexis began prior to the Trump administration and is renewed annually, according to yearly ICE Budget Overviews. Dave Larsen, *Feds to Hire LexisNexis to Track Immigrants*, DAYTON DAILY NEWS (Sep. 14, 2013), https://www.daytondailynews.com/news/feds-hire-lexisnexis-track-immigrants/XcV1Sl48kuCBmHmRrohRHK/ [https://perma.cc/2FVN-UTX3]; Dep't of Homeland Sec., U.S. Immigr. & Customs Enf't, Budget Overview – FY 2018 – Congressional Justification 160 (2018), https://www.dhs.gov/sites/default/files/publications/ICE%20FY18%20Budget.pdf [https://perma.cc/LTQ2-LXCA] (detailing current LexisNexis surveillance data subscription).

133. Budget Overview – FY 2018 – Congressional Justification, *supra* note 146, at 160 ("The increase [in the LexisNexis contract] from FY 2017 to FY 2018 is due to additional contract services required related to EO 13768.").

134. RELX ANNUAL REPORT, *supra* note 108, at 21.

135. ICE, *Law Enforcement Information Sharing Initiative*, https://www.ice.gov/le-information-sharing [https://perma.cc/TP9U-QJQV] (last visited Feb. 11, 2019).

Thomson Reuters has been even more successful than RELX in profiting from ICE surveillance. Thomson Reuters has signed at least three contracts to provide ICE with surveillance services totaling over $46 million.[136] Among those services is the CLEAR system, which "allows ICE access to a 'vast collection of public and proprietary records' including phone records, consumer and credit bureau data, healthcare provider content, utilities data, DMV records, World-Check listing, business data, data from social networks and chatrooms, and 'live access' to more than seven billion license plate detections.'"[137] These ICE contracts have come under fire from civil liberties groups concerned that the surveillance tools and data Thomson Reuters is selling violate peoples' rights.[138]

The first contract is a 2015 agreement giving ICE access to Thomson Reuters' CLEAR system. Under that contract, ICE enjoys access to millions of databases containing both public records from government entities and proprietary data collected from smaller data firms, which it uses to, according to the contract, "identify criminal suspects, businesses and assets of targets of investigations for potential arrest, seizure and forfeiture."[139] The contract specifies that Thomson Reuters will provide the data and the technology firm Palantir will conduct the real-time analysis to determine who to target through system-to-system communication.[140] Together with a host of law enforcement agency databases provided by Thomson Reuters, Palantir's controversial "automated policing" system will determine whether people should be targeted for investigations[141] in support of ICE's increasingly aggressive scheme to arrest

136. MIJENTE, *supra* note 15, at 56.

137. Privacy International, *Thomson Reuters Selling US Immigration and Customs Enforcement (ICE) Access to Data*, MEDIUM (June 28, 2018), https://medium.com/@privacyint/thomson-reuters-selling-ice-access-to-data-e4e7e6230614 [https://perma.cc/84TW-FCH2].

138. Using license plate tracking software to track people and AI to predict future criminals are both practices that have been condemned by civil liberties groups and shunned by some state governments. *See You Are Being Tracked*, ACLU, https://www.aclu.org/issues/privacy-technology/location-tracking/you-are-being-tracked [https://perma.cc/ZX9A-QXHS] (condemning the use of automated license plate readers); Russell Brandom, *ICE Contract Sparks License Plate Reader Backlash from Cities*, THE VERGE (Feb. 7, 2018), https://www.theverge.com/2018/2/7/16988058/ice-license-plate-reader-backlash-alameda-deportation-aclu [https://perma.cc/WZD6-QNFX]; s*ee generally* Dan Robitzki, *The LAPD's Terrifying Palantir-Powered Policing Algorithm Was Just Uncovered and Yes It's Basically 'Minority Report'*, FUTURIST (May 10, 2018), https://futurism.com/lapd-documents-show-their-policing-algorithms-continue-to-target-minorities-and-past-offenders/ [https://perma.cc/RGK4-5584].

139. Tracy Rosenberg, *Thomson Reuters $13 Million Contract with HSI*, OAKLAND PRIVACY (Oct. 14, 2017) https://oaklandprivacy.org/2017/10/14/thomson-reuters-13m-contract-with-hsi/ [https://perma.cc/34XF-M3NY]; *CLEAR System-to-System*, *supra* note 131; *see also CLEAR System-to-System*, THOMSON REUTERS, https://legal.thomsonreuters.com/en/products/clear-investigation-software/system-to-system [https://perma.cc/V43L-2Y5K].

140. *Id*.

141. *Id.*; FERGUSON *supra* note 4, at 1–2, 91–92; Sarah Brayne, *Big Data Surveillance: The Case of Policing*, 82 AM. SOC. REV. 977, 990–991 (2017) (describing the shift from query-based systems, submission of a request for information, for instance, a police officer running a license

noncitizens.

The second contract integrates license plate recognition ("LPR") data into the CLEAR system that Thomson Reuters supplies to ICE.[142] LPR data comes from systems of roadside cameras that photograph passing license plates and convert the images into a computer-readable format, creating a "massive vehicle-tracking network generating as many as 100 million sightings per month, each tagged with the date, time, and GPS coordinates of the sighting."[143] CLEAR subscribers can enter a license plate number and get insights such as the vehicle's make and model, state of registration, the best locations to find a vehicle, and set up a virtual stakeout for the vehicle.[144] The system simultaneously allows ICE to query historical license plate data (for instance, search for every time a given license plate was spotted in the last five years) to construct a detailed record of a target's movements, and can provide ICE with instant alerts whenever a new image of a particular license plate is found.[145] This forward- and backward-looking system gives ICE the power to "drill down into the data to build a detailed picture of your private life, including where you work, where you live, when you go to the doctor, and what political demonstrations you attend," and even who you associate with.[146]

Finally, a five-year contract between Thomson Reuters and ICE Enforcement and Removal Operations, a division of ICE that tracks hundreds of thousands of noncitizen U.S. residents each month, will give ICE a "continuous monitoring and alert system" that supplies "FBI numbers; State Identification Numbers; real time jail booking data; credit history; insurance claims; phone number account information; wireless phone accounts; wire transfer data; driver's license information; vehicle registration information; property information; pay day loan information; public court records; incarceration data; employment address data; Individual Taxpayer Identification Number (ITIN)

plate during a traffic stop, to alert-based systems where officers are notified in real time whenever particular variables coalesce in the data, and Palantir's role in the system as an RSS-feed of sorts, sorting and tracking data-points automatically, in real-time).

142. *ICE Acquires License Plate Tracking Data Through Sole Source Contract*, HOMELAND SEC. TODAY (Jan. 29, 2018), https://www.hstoday.us/uncategorized/ice-acquires-license-plate-tracking-data-through-sole-source-contract/ [https://perma.cc/Q5CA-2KKH]; DHS & ICE, PRIVACY IMPACT ASSESSMENT UPDATE FOR THE ACQUISITION AND USE OF LICENSE PLATE READER DATA FROM A COMMERCIAL SERVICE, DHS-ICE-PIA-039 (Dec. 27, 2017), https://www.dhs.gov/publication/dhs-ice-pia-039-acquisition-and-use-license-plate-reader-data-commercial-service [https://perma.cc/KQT3-HZG6]; *License Plate Recognition Data Press Release*, *supra* note 1.

143. Russell Brandom, *ICE is About to Start Tracking License Plates Across the US*, VERGE (Jan. 26, 2018), https://www.theverge.com/2018/1/26/16932350/ice-immigration-customs-license-plate-recognition-contract-vigilant-solutions [https://perma.cc/627Z-SSYE].

144. *License Plate Recognition Data Press Release*, *supra* note 1.

145. *Id*.

146. Matt Cagle, *A California City Fights Off ICE's Digital Deportation Machine*, ACLU (Feb. 13, 2018), https://www.aclu.org/blog/privacy-technology/location-tracking/california-city-fights-ices-digital-deportation-machine [https://perma.cc/UR4F-WXEZ]; Brandom, *supra* note **Error! Bookmark not defined.**.

data; and employer records."[147] This broad swathe of data is pulled from all sorts of local, state, federal, and private databases and consolidated by Thomson Reuters for ICE's convenience.[148]

C. Looking Ahead: The Future of ICE's Big Data Policing Program

The last contract also hints at things to come, demanding that the data services be "flexibly structured to adapt to changing priorities in the law enforcement continuum," allowing for possible increases in the amount of services and data types required by the agency.[149] Other ICE surveillance proposals reveal the types of surveillance projects legal information vendors will support in the future. When ICE held an investor day program related to the administration's proposed Extreme Vetting Program,[150] both Thomson Reuters and RELX Group representatives attended.[151] ICE wanted a data company to

147. U.S. Immigration and Customs Enforcement, *Notice of Intent to Sole Source TRSS Subscription Data Services*, FEDBIZOPPS.GOV (Feb. 7, 2017), https://www.fbo.gov/index?s=opportunity&mode=form&id=71911de5fa638ed0a391f01f520c0e2a&tab=core&_cview=1 [https://perma.cc/DE7U-B7VQ]. The Statement of Work Justification explains that before awarding the contract to Thomson Reuters, Enforcement and Removal Operations relied on subscriptions to commercial database aggregators supplied by the Federal Library and Information Network, managed by the U.S. Library of Congress. ICE, DATA SUBSCRIPTION SERVICES STATEMENT OF WORK 2 (Feb. 2018), https://www.fbo.gov/index?tab=documents&tabmode=form&subtab=core&tabid=8d8d10f190196f1ad88533d371f215b6 [https://perma.cc/HU85-PABX]. The Statement of Work states "however, the growing need for more criminal information and for more accuracy in the batch process prompted the [Targeting Operations Division] to seek alternatives to data service products currently available through the DHS Library." *Id.* Note that LexisNexis also bid for this contract. *See* DHS, SOLE SOURCE JUSTIFICATION, at 4 (Mar. 2018), https://www.fbo.gov/index?tab=documents&tabmode=form&subtab=core&tabid=42012dc0ffcf5f38adfaa8dae5d2f750 [https://perma.cc/8J7R-NW3H].

148. SOLE SOURCE JUSTIFICATION, *supra*, at 1 (describing the technology ICE requires as database aggregators that provide continuous access and alerts on people and that "leverage technology to share secure law enforcement data between Federal, State, and local law enforcement agencies").

149. DATA SUBSCRIPTION SERVICES STATEMENT OF WORK, *supra* note 147, at 2.

150. Donald J. Trump (@realdonaldtrump), TWITTER (Oct. 31, 2017, 6:26 PM), https://twitter.com/realdonaldtrump/status/925534445393928199?lang=en. [https://perma.cc/28WX-VNYQ] (demonstrating that "extreme vetting program" was coined after Trump's tweet reacting to a truck attack that killed 8 people in NYC and ordering Homeland Security "to step up our already Extreme Vetting Program. . . [b]eing politically correct is fine, but not for this!").

151. Both Thomson Reuters and Reed Elsevier sent representatives to the informational investor day for the Extreme Vetting Program. *The Intercept* published PDFs of the sign-in sheets where each company is signed in as TRSS (Thomson Reuters Special Services) and LNSSI (LexisNexis Special Services Inc.). *Sign in Sheet ICE Data Analysis Services Industry Day* (July 18, 2017), https://www.documentcloud.org/documents/3914251-July-18-2017-Sign-in-Sheets-1.html#document/p1 [https://perma.cc/W26V-CSE7]; *see also* Sam Biddle & Spencer Woodman, *These are the Technology Firms Lining Up to Build ICE's 'Extreme Vetting' Program*, INTERCEPT (Aug. 7, 2017), https://theintercept.com/2017/08/07/these-are-the-technology-firms-lining-up-to-build-trumps-extreme-vetting-program/ [https://perma.cc/7VTX-5N5Y] (linking to attendee sign in sheets, which include TRSS and RELX employees).

"'scrape' social media profiles using vague and unproven criteria to monitor individual visa applicants and holders both in the United States and abroad."[152] After the investor day, ICE shelved the program because it found that data companies had not yet developed technology that could provide the level of monitoring the agency desired.[153] For now, the agency plans to hire people to manually surveil noncitizen social media accounts until the right technology is developed.[154]

While that aspect of the Extreme Vetting Program could not be implemented due to lagging technology, other technology-driven immigration surveillance efforts are in the works. The DHS's Office of Biometric Identity Management just reached a $95 million contract with Northrop Grumman to create a system that will match face, finger, and eye biometrics to identify people in photographs and videos.[155]

In addition to technological developments that deepen the amount and degree of information available to ICE, immigration surveillance is also undergoing a paradigm shift. Namely, immigration surveillance is moving from a reactive model that focuses on tracking individuals known or believed to be involved in criminal activities to a predictive model that uses artificial intelligence and computer models to attempt to forecast whether people who have no criminal record or ties to criminal activity may nonetheless commit a crime in the future.[156]

152. Press Release, Committee on Homeland Security, Thompson, Vela, Rice: Stop Ineffective and Discriminatory Extreme Vetting Program (Apr. 6, 2018), https://democrats-homeland.house.gov/news/correspondence/thompson-vela-rice-stop-ineffective-and-discriminatory-extreme-vetting-program [https://perma.cc/E3ZV-C5ZZ] (including statement by over 50 technology experts and 50 civil society groups expressing that "ICE's intention to build a program with unknown limits to search social media platforms demonstrates a disregard for privacy, due process, and the rights to free speech and free association").

153. Drew Harwell & Nick Miroff, *ICE Just Abandoned its Dream of "Extreme Vetting" Software that Could Predict Whether a Foreign Visitor Would Become a Terrorist*, WASH. POST (May 17, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/17/ice-just-abandoned-its-dream-of-extreme-vetting-software-that-could-predict-whether-a-foreign-visitor-would-become-a-terrorist/?noredirect=on&utm_term=.265d81cb37cc [https://perma.cc/Q2F9-C37H].

154. *Id*.

155. Press Release, Northrop Grumman, Northrop Grumman Wins $95 Million Award from Department of Homeland Security to Develop Next-Generation Biometric Identification Services System (Feb. 26, 2018), https://news.northropgrumman.com/news/releases/northrop-grumman-wins-95-million-award-from-department-of-homeland-security-to-develop-next-generation-biometric-identification-services-system [https://perma.cc/J5BQ-5UW5].

156. Predictive policing forecasts like those created by Palantir and used by ICE "identify likely criminal actors" and create "Chronic Offender Bulletins" listing "targeted individuals." Andrew G. Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1109, 1141 (2017). Ferguson also explains how "the law has lagged behind" policing technology, stressing that while Fourth Amendment stops can be predicated on predictive analysis, law enforcement must not use predictive policing technology as a "crystal ball" and they must verify connections drawn by computer models and AI. Andrew G. Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 408–10 (2015).

D. Big Data Policing and Legal Research Companies: Civil Rights Concerns

ICE's embrace of big data policing is anathema to civil rights advocates. The algorithm-based surveillance programs built by Thomson Reuters, RELX Group, and other companies increase the amount of data at ICE's fingertips, but data does not necessarily lead to accuracy. Instead, these predictive models are susceptible to creating and furthering racially discriminatory feedback loops.[157] While the models themselves may be subject to discriminatory methods of statistical analysis,[158] the bigger specter is often that racial bias is already present in the datasets that are collected from brokers and fed into the models. Historical data about crime, arrests, and gang affiliations, in particular, "directly correlate with racially discriminatory law enforcement practices."[159] Policing data aggregated from systems that have disparately targeted people of color for police stops, investigations, arrests, and convictions are racially-biased information collections.[160] When these discriminatory historical datasets are treated as neutral inputs they lead to inaccurate models of criminality which, in turn, perpetuate racial inequality and contribute to the targeting and over-policing of non-citizens.[161]

Data brokers like RELX Group profit from selling access to biased data, perpetuating and amplifying a racist policing system with products that connect "disparate law enforcement data" from across the nation into a single system in order to "anticipate events" and "predict offender behavior."[162] This predictive policing, fueled by Thomson Reuters and RELX Group's data products, raises significant Fourth Amendment concerns.[163] Older surveillance systems relied largely on "human intelligence," or information collected through human contact, labor-intensive work which was not easily scaled up.[164] Data

157. MIJENTE, *supra* note 15, at 53.

158. *Id*.

159. FERGUSON, *supra* note 4, at 47.

160. *Id*. at 48–52.

161. MIJENTE, *supra* note 15, at 54. Algorithmic bias affects everyone yet goes entirely unregulated, which is especially problematic when big data is used by law enforcement. Will Knight, *Biases are Everywhere, and No One Seems to Care*, MIT TECHNOLOGY REVIEW (July 1, 2017), https://www.technologyreview.com/s/608248/biased-algorithms-are-everywhere-and-no-one-seems-to-care/ [https://perma.cc/3CHU-EHRD]. *See infra* Section II.C.

162. Lexis Risk Solutions, Crime Analytics and Mapping, https://risk.lexisnexis.com/law-enforcement-and-public-safety/crime-analytics-and-mapping [https://perma.cc/XZ5W-N4XZ] (last visited Mar. 12, 2019).

163. Jonathan Hafetz, *How NSA Surveillance Endangers the Fourth Amendment*, CONST. DAILY (Aug. 13, 2013), https://constitutioncenter.org/blog/how-nsa-surveillance-endangers-the-fourth-amendment/ [https://perma.cc/6EVX-DUWB] (discussing the constitutional issues raised by "dragnet" suspicionless, widespread surveillance).

164. David Tuffley, *AI Can Help in Crime Prevention, But We Still Need a Human in Charge*, *The Conversation* (Apr. 27, 2018), https://theconversation.com/ai-can-help-in-crime-prevention-but-we-still-need-a-human-in-charge-95516 [https://perma.cc/7BM2-V7PH] (describing human intelligence-based policing in its simplest form as "eagle-eyed police patrols to

surveillance, on the other hand, is detached from human contact and can thus be scaled with ease, regardless of whether the data is outdated, biased, or completely inaccurate.[165] When police forces rely on databases rather than human intelligence, they are casting wide and imperfect nets over communities that will mistakenly catch people who are not threats.[166] Especially in the immigration context, where an arrest can lead to deportation, labelling and tracking people because of computer-perceived risk, as opposed to their tangible actions, could lead to heartbreaking and dangerous outcomes.

The three ICE contracts that Thomson Reuters has already signed raise red flags with civil rights and privacy advocates. Organizations from across the political spectrum have questioned the civil rights implications of law enforcement using artificial intelligence to sort people into criminal and non-criminal categories and making determinations about arrests based on computer generated lists.[167] Furthermore, license plate tracking is controversial: even the International Association of Chiefs of Police warn that LPRs raise privacy concerns.[168] In fact, similar concerns led DHS to cancel its license plate tracking plan in 2014.[169] However, in 2017, after the Trump executive order granting ICE broader power to maintain public order, the agency went ahead and purchased license plate recognition services from the Thomson Reuters subsidiary, West

ensure public safety").

165. Ferguson, *Policing Predictive Policing*, *supra* note 156, at 1124–25 (describing how predictive policing technology allowed NYPD and other police departments to implement high-tech, comprehensive policing technology even with dwindling budgets).

166. Ferguson, *Big Data and Predictive Reasonable Suspicion*, *supra* note 156, 398–403 (2015) (describing the data used for predictive policing and big data surveillance as rife with bad data and false positives).

167. Matthew Feeney, *Big Data Tool for Trump's Big Government Immigration Plans*, CATO INSTITUTE (Mar. 9, 2017), https://www.cato.org/blog/big-data-tools-trumps-big-government-immigration-plans [https://perma.cc/7D5F-QGBZ] (warning that systems like FALCON could be used to target any population that falls outside of a president or government's favor); Jay Stanley, *Beware of Data Miners Offering Protection*, ACLU (Dec. 1, 2011), https://www.aclu.org/blog/privacy-technology/beware-data-miners-offering-protection [https://perma.cc/2F75-YJKG] (arguing that Palantir's technology will mistakenly label innocent people as legitimate targets for terrorism suspects).

168. INT'L ASSOC. OF CHIEFS OF POLICE, PRIVACY IMPACT ASSESSMENT REPORT FOR THE UTILIZATION OF LICENSE PLATE READERS (Sept. 2009), https://www.aclu.org/sites/default/files/field_document/33225-33317_FOIA_No._12-00328_Privacy_impact_assessment_report_for_the_utilization_of_license_plate_readers_publication.pdf [https://perma.cc/ZYQ8-GKKS] (warning that implementing LPR surveillance without clear, uniform rules governing the appropriate use and sharing of LPR data could lead to First Amendment concerns as individuals would "become more cautious in the exercise of their protected rights of expression, protest, association, and political participation because they consider themselves under constant surveillance").

169. Ellen Nakashima & Josh Hicks, Department of Homeland Security Cancels National License Plate Tracking Plan, WASH. POST (Feb. 19, 2014), https://www.washingtonpost.com/world/national-security/dhs-cancels-national-license-plate-tracking-plan/2014/02/19/a4c3ef2e-99b4-11e3-b931-0204122c514b_story.html?utm_term=.56abca74523a [https://perma.cc/9K2Z-GQNG].

Publishing.[170]

Despite these critiques, Thomson Reuters and RELX Group are unapologetic about their lucrative work with law enforcement, including the work they do for ICE. Thomson Reuters issued a statement that it "supplies data to ICE in support of its work on active criminal investigations with the explicit purpose to focus resources on priority cases involving threats to public safety and/or national security."[171] Other companies, like IBM, faced significant public pressure after showing interest in supplying surveillance products to ICE and, in response, issued a statement that the company would not work on any projects that run counter to its values.[172] Thomson Reuters and RELX Group, however, have remained silent about their social responsibility standards.

III.
THE ETHICAL IMPLICATIONS OF LEGAL RESEARCH VENDORS DOING SURVEILLANCE

Thomson Reuters and RELX Group's ICE partnerships force lawyers to face difficult issues of social responsibility. The partnerships also raise professional responsibility issues, as the lawyers' code of ethics obligates practitioners to adhere to certain standards. The ABA Model Rules of Professional Responsibility often balance ethics against feasibility.[173] Lawyers must be ethical, but they must also adopt practices that are not so expensive or impractical that they disadvantage clients. Thus, lawyers must weigh the ethics of using legal research services that fuel ICE surveillance against the feasibility of adopting alternate legal research methods. Thomson Reuters and RELX Group's Westlaw and LexisNexis products are integral to the competent practice of law, and their legal research services are currently superior to their competitors', making it difficult to determine whether their use runs afoul of lawyers' professional code.

A. Westlaw and LexisNexis: A Duopoly Breeds Ethical Impunity

LexisNexis and Westlaw are not "mom n' pop law companies."[174] Their

170. *See supra* notes 143–46.

171. Ben Collins and Meghan Sullivan, *supra* note 128.

172. Dustin Volz, *IBM Urged to Avoid Working on "Extreme Vetting" of U.S. Immigrants*, REUTERS (Nov. 16, 2017), https://www.reuters.com/article/us-ibm-immigration/ibm-urged-to-avoid-working-on-extreme-vetting-of-u-s-immigrants-idUSKBN1DG1VT [https://perma.cc/EXG3-2A6X].

173. While the ABA Model Rules of Professional Responsibility are not themselves binding, "they are the primary basis for the ethics codes that regulate lawyers at the state level." Richard Acello, *New York Makes Itself a 'Model' State*, A.B.A. J. (Sept. 2009), http://www.abajournal.com/magazine/article/new_york_makes_itself_a_model_state [https://perma.cc/SVV4-ZNEL].

174. Sarah Lamdan, *Surveillance and Legal Research Providers: What You Need to Know*, MEDIUM (July 6, 2018), https://medium.com/@slamdan/surveillance-and-legal-research-providers-what-you-need-to-know-85a976134e8f [https://perma.cc/44KB-MM2Z].

legal research platforms are one of multiple sources of profit for large corporate conglomerates that also sell news content to journalists, science materials to doctors, financial data to traders, and surveillance data to law enforcement. On the virtual shelves of Thomson Reuters' and RELX Group's information warehouses, the Westlaw/Lexis legal product packages sit right next to the "risk solution" law enforcement surveillance products. Legal research products are part of the legal profession and as such they must meet lawyers' professional standards. When they wind up in the same information funnel as government surveillance products, legal research products no longer meet the ethical standards required by their lawyer consumers.

Lawyers need computer-assisted legal research to do their jobs, as proper legal research is necessary to avoid malpractice.[175] So long as the law is based upon a system of statutes, regulations, and case law precedent, the legal profession will rely on computerized database systems to sort, cite check, and update sources of law. Westlaw and Lexis have cornered the computer-assisted legal research market.[176]

Westlaw and Lexis's duopoly is easily explained by their corporate histories. The West company has been building its key number system since the 1800s,[177] and LexisNexis has been building its electronic case law resource since the 1960s.[178] Westlaw and LexisNexis had electronic legal research terminal services long before launching their online research systems.[179] Because they had already amassed electronically formatted legal records and organized case law, statutes, administrative law materials, and secondary sources, Westlaw and LexisNexis were able to create complex research systems that linked various legal materials together. These services also provide invaluable annotated information about primary sources of law by fusing content from their headnotes, citators, and secondary resources. By focusing narrowly on legal publishing, Westlaw and LexisNexis developed the top legal research tools, including their proprietary citator and headnote systems.[180] Despite numerous

175. Some equate not using the research systems to malpractice. *See, e.g.*, Carol M. Bast & Susan W. Harrell, *Ethical Obligations: Performing Adequate Legal Research and Legal Writing*, 29 NOVA L. REV. 49, 49 (2004) ("Failure to adequately research or write well, or both, is a violation of ethics rules and can result in a reprimand, suspension, or disbarment from the practice of law; a client may decide that it is the basis of a legal malpractice lawsuit.").

176. Olufunmilayo B. Arewa, *Open Access in a Closed Universe: Lexis, Westlaw, Law Schools, and the Legal Information Market*, 10 LEWIS & CLARK L. REV 797, 821 (Mar. 2006) ("…the online legal information industry can be characterized as a duopoly in which Lexis and Westlaw are the most important players").

177. WESTLAW, RESOURCES FOR CONDUCTING LEGAL RESEARCH 6 (2007), http://lscontent.westlaw.com/images/banner/documentation/ResearchResources.pdf [https://perma.cc/5U6B-EY43].

178. *The LexisNexis Timeline*, LEXISNEXIS, at 2, http://www.lexisnexis.com/anniversary/30th_timeline_fulltxt.pdf [https://perma.cc/6W6K-X6KE].

179. *Id*.

180. *Online Legal Research Databases: What Are Your Alternatives?*, SPECIAL COUNSEL BLOG (Jan. 4, 2018), http://blog.specialcounsel.com/legal-technology/alternative-legal-research-

attempts, no other legal research product has broken into the upper echelon of the legal research market.[181]

B. Professional Responsibility Considerations for Legal Research Vendors

At minimum, lawyers should ensure that the practices of their legal research companies comport with their professional ethics. Because the ABA Model Rules of Professional Responsibility have not kept pace with technological changes, the Model Rules are largely ineffective at providing guidance for the ethical conundrums that arise when legal research companies are involved in big data policing. It remains instructive to apply the existing rules, but until the rules are modified, lawyers must take action based on personal ethical imperatives. Some of the rules that provide useful guidelines include the Model Rule 1.7, prohibiting conflicts of interest, Model Rule 1.6, which requires lawyers to keep client work confidential, and Rule 5.3, which requires lawyers to vet third party vendors to ensure they are using ethically sound practices.[182]

1. Rule 1.7: Conflicts of Interest

Lawyers who represent immigrant clients in immigration court or the criminal justice system should consider whether using products related to the law enforcement surveillance of their own clients amounts to a conflict of interest. Rule 1.7, which governs conflicts of interests, suggests that legal research's connection to surveillance is a conflict which, although attenuated, is worth considering more closely.

The American Bar Association's ("ABA") Model Rule of Professional Conduct 1.7 prohibits lawyers from representing clients if there is a significant risk that their representation will be materially limited by the lawyer's responsibilities to a third person.[183] Conflicts of interest are not always easy to decipher. As one lawyer describes it, "Conflicts of interest appear in an infinite variety of situations and are frequently fact-specific, yet they often are difficult to identify."[184]

Using a legal research service connected to ICE surveillance presents one of those difficult-to-identify situations. If an attorney is obligated to pay a third

databases/ [https://perma.cc/M3MA-PXEG] (describing Westlaw and Lexis alternatives, but reminding legal researchers that Lexis and Westlaw are the "top tier" options because they have developed topical case law organization systems and citators).

181. LAC GROUP, *LexisNexis Versus Westlaw Revisited* (Feb. 22, 2018), https://lac-group.com/lexisnexis-versus-westlaw-revisited/ [https://perma.cc/32QS-S2V3] (finding that, "[w]hile Westlaw and Lexis continue to be at the top, their grip on market dominance has continued to loosen with the entrance of technology startups that are both well-funded and agile.").

182. *See* MODEL RULES OF PROF'L CONDUCT r. 1.6, 1.7, 5.3 (AM. BAR. ASS'N 2016).

183. *See* MODEL RULES OF PROF'L CONDUCT r. 1.7 (AM. BAR. ASS'N 2016).

184. Ellen Yankiver Suni, *Conflicts of Interest*, GPSOLO MAGAZINE (Oct. 2005), https://www.americanbar.org/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/conflictsofinterest.html [https://perma.cc/SDZ2-ERFQ].

party (Thomson Reuters or RELX Group), and that third party is helping ICE (opposing counsel) with a client's case, has the attorney fallen on an ethical tripwire wherein the attorney will materially limit the representation of her client? The possibility that you are helping ICE spy on your clients rises significantly when you use legal research products like Westlaw that reserve the right to share user data with other Thomson Reuters products and with law enforcement.[185]

Overall, lawyers' ethical standards and the ABA model rules focus on being honest and forthright with clients. Would clients feel that lawyers who pay Westlaw and LexisNexis, and possibly even type incriminating searches into those same programs, had their best interests at heart? In cases where ICE surveillance data harms a client, lawyers who pay for subscriptions to Westlaw or Lexis may have contributed to the client's adverse circumstances. While, in its current iteration, Rule 1.7 does not appear to implicate lawyers who use services that indirectly contribute to surveillance, it is worth considering whether lawyers' ethics should require a formal ethical boundary between client work and client surveillance.

2. Rule 1.6: Confidentiality of Information

Client confidentiality is a cornerstone of the legal profession: the attorney-client privilege allows clients to safely confide in their lawyers without inhibition. A critical piece of confidentiality is the assumption that clients' personal information is safe in their lawyers' hands. Under the microscope of confidentiality, Thomson Reuters and RELX Group's coziness with law enforcement yields an additional concern: are Westlaw and LexisNexis keeping records of lawyers' research and, through their parent companies, making it available to their law enforcement clients? And if so, does exposing your legal search terms constitute a breach of confidentiality?

Notably, neither Thomson Reuters nor RELX Group has promised that their legal research product is independent from the data services they provide to law enforcement. In fact, when asked about whether they use legal research user data in their surveillance search platforms, Bloomberg Law immediately responded that their product does not save user data, but Thomson Reuters representatives were "notably silent."[186] Thomson Reuters' lack of response corresponds to their privacy statement, updated in May, 2018, which explicitly says that the company shares its user information with a range of entities, including "within the Thomson Reuters group, with our business partners and third party service providers, the person providing for your access to our Services (if that is not

185. *See Privacy Statement*, THOMSON REUTERS (May 25, 2018), https://www.thomsonreuters.com/en/privacy-statement.html.

186. Joe Hodnicki, *Does Wexis Use Legal Research User Data in Their Surveillance Search Platforms*, LAW LIBRARY BLOG (July 16, 2018), https://llb2.com/2018/07/16/does-wexis-use-legal-search-user-data-in-their-surveillance-search-platforms/ [https://perma.cc/MQ2V-HDXG].

you) and in accordance with law."[187] This raises the additional concern that confidential information could be crossing between corporate subsidiaries, from Westlaw to the data services being sold to law enforcement.

The ABA has not directly opined on whether using products that participate in surveillance projects violates confidentiality obligations. When considering confidentiality and technology, ABA opinions have focused on communications between lawyers and clients[188] and been relatively silent on issues related to ethics and legal research. This is likely because legal research privacy is a contemporary issue. Until recently, research was done with books, and perusing court reporters is hardly a public communication. Further, law libraries comply with stringent patron privacy standards.[189] Online legal research services are a relatively new development,[190] and the purchase of these companies by larger data corporations that also sell surveillance products is an even newer phenomenon. Indeed, the ABA Standing Committee on Ethics and Professional Responsibility's notoriously slow response to technological changes in the profession[191] means there is no guidance on attorney use of legal research products that are linked to law enforcement surveillance.

Yet ABA opinions are unambiguous that using online services, email or otherwise, that do not protect client information can violate the lawyers' ethical code.[192] Model Rule 1.1 requires that lawyers be competent, an obligation that includes being aware of the risks of using various technologies.[193] Moreover, in 2012, the ABA's Standing Committee on Ethics and Professional Responsibility amended Rule 1.6(c) to require that lawyers "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to,

187. *Privacy Statement*, THOMSON REUTERS, *supra* note 185.

188. The ABA's primary guidance on confidentiality and technology focuses on email communications and cyber-threats and not the confidentiality issues that may arise as lawyers perform professional tasks on various electronic platforms. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 477R (2017).

189. *See Privacy*, AM. LIBRARY ASSOC. (last visited July 10, 2018), http://www.ala.org/advocacy/privacy [https://perma.cc/BL22-TZMX] ("Libraries, librarians, and library workers have an ethical obligation, expressed in the ALA Code of Ethics, to preserve users' right to privacy and prevent any unauthorized use or disclosure of users' personally identifiable information or the data associated with their use of the library's resources…. This includes the adoption of policies and practices that treat patron data as confidential.").

190. LexisNexis went online at the end of 1997, and Westlaw.com went online in early 1998. *See* Robert J. Ambrogi, *Westlaw, Lexis-Nexis Set Up Shop on the Web*, LEGALONLINE (Apr. 1998), http://www.legaline.com/col38.html [https://perma.cc/V7BR-9ZAX].

191. *See* Ambrogi, *supra* note 31.

192. *See* David L. Hudson, Jr., *Using Unencrypted Email in Client Communications Not Always Enough, Ethics Opinion Indicates*, ABA JOURNAL (May 11, 2017), http://www.abajournal.com/news/article/ethics_opinion_addresses_attorneys_obligations_secure_client_communications [https://perma.cc/5EB3-3LE3].

193. MODEL RULES OF PROF'L CONDUCT r. 1.1, cmt. 8 (AM. BAR ASS'N 1983) ("To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.").

information relating to the representation of the client."[194] This modification specifies that lawyers must try to prevent the disclosure of client data related to case work.

In 2017, the ABA Committee issued guidance for the 2012 amendments to Rule 1.6 to help lawyers determine whether they are doing enough to protect client information when they use technology in their practice.[195] The guidance asks lawyers to independently weigh the costs and burdens of implementing safeguards against the sensitivity of the disclosed information.[196]

Applying the 2017 guidance, an attorney's use of legal research providers indirectly involved in surveillance raises confidentiality concerns. Search data associated with lawyers' Westlaw and Lexis accounts can be sensitive material. In some states, search strategy and legal research fall squarely in the realm of confidential lawyer work product.[197] The balance of safeguarding sensitive legal research information use against the costs of selecting legal research products that guarantee confidentiality becomes easier as legal research market proliferate, offering ever-improving technology and competitive rates.[198] In a profession that prohibits even email tracing bugs as detriments to client confidentiality,[199] something as harmful to clients as police surveillance should be walled off from the legal profession, both personally and financially, and lawyers should opt to use legal research systems that protect sensitive client information.

3. Rule 5.3: Responsibilities Regarding Nonlawyer Assistance

Beyond a lawyer's own conflict of interest and confidentiality considerations, lawyers must make reasonable efforts to ensure that non-lawyers

194. ABA Comm. on Ethics & Prof'l Responsibility, Res. 105A (Aug. 6, 2012).

195. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 477R (2017) (discussing securing communication of protected client information).

196. *Id*. at 4 (offering a nonexclusive list of factors to guide lawyers, including "the sensitivity of the information," "the likelihood of disclosure if additional safeguards are not employed," "the cost of employing additional safeguards," "the difficulty of implementing the safeguards," and "the extent to which the safeguards adversely affect the lawyer's ability to represent clients").

197. For instance, the California Code of Civil Procedure, § 2018.030(a) says: "A writing that reflects an attorney's impressions, conclusions, opinions, or legal research or theories is not discoverable under any circumstances". But note that other states do not regard legal research as confidential. *See, e.g.*, New York Rules of Professional Conduct 1.6 ("'Confidential Information' does not ordinarily include (i) a lawyer's legal knowledge or legal research").

198. LAC Group, *LexisNexis Versus Westlaw Revisited* (Feb. 22, 2018), https://lac-group.com/lexisnexis-versus-westlaw-revisited/ [https://perma.cc/527B-4QQP] ("While Westlaw and Lexis continue to be at the top, their grip on market dominance has continued to loosen with the entrance of technology startups that are both well-funded and agile.")

199. Debra Cassens Weiss, *Lawyers May Not Use "Web Bugs" to Track Email Sent to Opposing Counsel, Ethics Opinion Says*, ABA JOURNAL (Nov. 6, 2016), http://www.abajournal.com/news/article/lawyers_may_not_use_web_bugs_to_track_email_sent_to_opposing_counsel_ethics/ [https://perma.cc/RMF3-GFXS].

under their authority engage in conduct that is compatible with the lawyer's own professional obligations.[200] To be sure, legal research companies are not "under the authority" of lawyers like companies providing discovery assistance or trial exhibits are. Nevertheless, many similarities exist between legal research companies and other non-lawyer assistance. Representatives from Lexis and Westlaw are in regular contact with their attorney clients, assisting with specific research questions[201] and designing special training packages to meet their clients' needs.[202] This personal contact, the digital customization of research results as well as the storing of research histories, and the suggestions of alternate research sources in response to search queries arguably create a similarly close and dependent assistant relationship to that of traditional non-lawyer assistance. In these types of vendor relationships, the ABA instructs lawyers to conduct due diligence on vendors that provide communication technology.[203]

According to the ABA, when lawyers use a third-party vendor in their practice, they must ensure 1) that the vendor maintains the same confidentiality and security standards that the lawyer must maintain, and 2) that the vendor does not use lawyer information in a way that creates a conflict of interest. The 2017 ABA opinion on technology and client communication builds on a 2008 opinion to clarify that lawyers have professional responsibility obligations when they outsource legal and non-legal services in their legal practices.[204] These obligations include considering vendors' security policies and protocols, using

200. MODEL RULES OF PROF'L CONDUCT r. 5.3(b) (AM. BAR. ASS'N 2016).

201. Reference Attorneys, Thomson Reuters, https://legal.thomsonreuters.com/en/support/reference-attorneys (last visited Mar. 22, 2019) ("Bar-admitted Reference Attorneys are ready to help you with time-saving guidance", "[c]ustomers should contact us at any point of their research. Whether it is to get a starting point or to ensure nothing has been overlooked; we can help you find what you are looking for quickly and efficiently. Reference Attorneys are available to help night and day"); LexisNexis Research Software, http://www.lexisnexis.com/custserv/researchsoftware.asp (last visited Mar. 22, 2019) ("The LexisNexis Customer Support team includes attorneys, computer engineers, information professionals, financial planners, and stockbrokers who are all available 24/7 to answer your questions and help you get the most out of LexisNexis Research Software").

202. Michael Feit, *A Librarian's Perspective: Concerns of Eliminating a Vendor*, FEIT CONSULTING (Apr. 17, 2017), https://www.feitconsulting.com/a-librarians-perspective-concerns-of-eliminating-a-vendor/ [https://perma.cc/JSR7-UVSG] (describing weekly visits from Westlaw and Lexis vendors and describing Westlaw and Lexis product representatives as "part of our extended library team"); Stosh Jonjak, *Law Firm Library Marketing: Taking Advantages of Existing Opportunities Part 2*, IBRARYGUY BLOG (June 24, 2015), https://ibraryguy2.wordpress.com/2015/06/24/law-firm-library-marketing-taking-advantage-of-existing-opportunities-part-2/ [https://perma.cc/SB27-8FMZ] ("Vendor presentations and workshops are pretty common in law firms. Remotely, vendors consistently offer webinars to showcase new software and updates. And in-person, vendors make weekly visits to our firm to provide hands-on training.").

203. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 477R (2017) (referring to ABA Formal Opinion 08-451 for this requirement).

204. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 08-451 (2008) ("Lawyer's Obligations When Outsourcing Legal and Nonlegal Support Services").

confidentiality agreements, and making sure the vendors do not have any conflicts of interest,[205] considerations lawyers should be applying with scrutiny to their legal technology vendors.

Obligations aside, the privacy agreements that Westlaw and LexisNexis provide to users do not make any assurance that they will maintain the necessary confidentiality and security standards that lawyers ascribe to.[206] Thomson Reuters do not separate products and work across "all platforms" as they develop their AI and machine-learning technology.[207] Based on Thomson Reuters' and LexisNexis's privacy statements,[208] the legal community should expect that the information they put into their Westlaw and Lexis accounts, including search histories and saved documents, are not confidential. The data you enter into Lexis and Westlaw could become part of ICE's surveillance data trove, linking your clients' personal data to your search histories and research and placing your clients' safety in jeopardy.

IV.
A CALL TO ACTION TO DIVEST FROM LEXIS AND WESTLAW

It is time for lawyers to be more vigilant about our "supply chain." If legal research products are engaged in unethical practices, or in practices that fail to comply with professional responsibility rules, lawyers should condemn those practices. No conscientious lawyer can stand by idly when Westlaw and LexisNexis's parent companies are building a "digital deportation machine"[209]

205. *Id*.

206. Both companies' privacy statements say they will share user data with company partners and with law enforcement to comply with requests from courts, law enforcement agencies, regulatory agencies, and other government authorities. *See Privacy Statement*, THOMSON REUTERS, *supra* note 185, at 25–26 (discussing Westlaw's privacy statement); *Privacy Policy*, LEXISNEXIS (May 7, 2018), https://www.lexisnexis.com/en-us/terms/privacy-policy.page [https://perma.cc/7U95-CU69]. At the AALL meeting and in subsequent conversations, Lexis representatives have suggested that they would write a statement promising to firewall user data from their surveillance products, but no such statement has been issued, despite repeated follow up by the author. *See* Hodnicki, *supra* note 188; *see generally Past Meetings: 2018 Baltimore*, AALL, https://www.aallnet.org/conference/about/past-meetings/2018-baltimore/ [https://perma.cc/6KMQ-BKW7].

207. THOMSON REUTERS 2017 ANNUAL REPORT, *supra* note 3.

208. *See supra* note 198. Like Thomson Reuters' privacy statement, LexisNexis's privacy statement explicitly says that the company will use your personal information to "enhance and improve the Service and our other products, events, and services and to develop new products, services and benefits" and to "comply with our legal obligations, resolve disputes, and enforce our agreements." LexisNexis shares subscribers' information with "…affiliates, trading names and divisions within the LexisNexis group of companies worldwide and certain RELX Group companies that provide technology, customer service and other shared services functions; and/or [LexisNexis] service providers, suppliers, agents and representatives…" as well as to "meet any applicable law, regulation, legal process or other legal obligation…" *Privacy Policy*, LEXISNEXIS, *supra* note 206.

209. Chantal Da Silva, *City Refuses to Let ICE Track License Plates With "Digital Deportation Machine"*, NEWSWEEK (Feb. 14, 2018), http://www.newsweek.com/city-refuses-let-ice-track-licenses-places-digital-deportation-machine-806845 [https://perma.cc/7GJ2-RZ64].

with profits from their lawyer customers. Instead, lawyers should switch to alternative products.

Westlaw and Lexis do not have to be lawyers' only choices for legal research. Even though these legal research services are universally blessed by the legal profession and considered the "top tier" research products,[210] a bevy of newer online legal research platforms are disrupting the legal technology field. Services like Bloomberg Law, Fastcase, and Casetext are building their own citators, headnote systems, and other legal research tools to sort and update primary and secondary sources of law. Many of these alternative legal research products do not participate in law enforcement surveillance. As we discuss the ethically fraught overlap of legal research and surveillance systems, we should consider opening our minds to these new legal research alternatives. Along with fancy bells and whistles like citators and annotations, big data ethics should be a guiding factor in selecting the legal research products we use in our practice.

Other professions have exerted pressure on companies whose contracts enable government cruelty.[211] Employees at companies like Microsoft and Amazon have denounced their employers' connections to ICE surveillance work.[212] And Google declined to renew a contract to provide artificial intelligence services to the Pentagon after thousands of employees signed a letter

210. Despite their market dominance, Westlaw and Lexis are far from perfect. A recent study found that Westlaw and Lexis's case classification systems reflect an outdated and biased "nineteenth-century worldview," less equipped to provide research results for twenty-first-century legal issues. Susan Nevelow Mart, *The Algorithm as a Human Artifact: Implications for Legal [Re]Search*, 109 LAW LIBR. J. 387, 419 (2017), http://scholar.law.colorado.edu/articles/755. Another study found that Westlaw and Lexis's citator systems incorrectly identify negative treatment of case law roughly one-third of the time. *See* Paul Hellyer, *Evaluating Shephard's, KeyCite, and BCite for Case Validation Accuracy*, 110 LAW LIBR. J. 449 (2018), https://www.aallnet.org/wp-content/uploads/2018/12/LLJ_110n4_02_hellyer.pdf.

211. *See, e.g.*, Michelle Chen, *How Tech Workers are Fighting Back Against Collusion with ICE and the Department of Defense*, THE NATION (June 27, 2018), https://www.thenation.com/article/tech-workers-fighting-back-collusion-ice-department-defense/ [https://perma.cc/N629-227H] (describing employee protests at major technology companies over their employers' contracts with ICE and the Department of Defense).

212. *See* Sheera Frenkel, *Microsoft Employees Protest Work with ICE, as Tech Industry Mobilizes Over Immigration*, N.Y. TIMES (June 19, 2018), https://www.nytimes.com/2018/06/19/technology/tech-companies-immigration-border.html [https://perma.cc/2Z2A-H7YZ] (more than 100 Microsoft employees wrote a letter asking the company to stop working with ICE to process data and develop artificial intelligence capabilities); Hamza Shaban, *Amazon Employees Demand Company Cut Ties with ICE*, WASH. POST (June 22, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/06/22/amazon-employees-demand-company-cut-ties-with-ice/?utm_term=.26c9f4a65aa9 [https://perma.cc/SL58-F2EK] (describing Amazon employees' letter to their employer, denouncing the company's efforts to sell its facial recognition platform to ICE); Michael Forsythe & Walt Bogdanich, *McKinsey Ends Work With ICE Amid Furor Over Immigration Policy*, N.Y. TIMES (July 9, 2018), https://www.nytimes.com/2018/07/09/business/mckinsey-ends-ice-contract.html [https://perma.cc/HE2Z-3E2F] (noting the management consultancy McKinsey & Company ended its contract with ICE after its employees complained about ethical issues, with the managing partner explaining that the firm "will not, under any circumstances, engage in any work, anywhere in the world, that advances or assists policies that are at odds with our values").

of protest and a handful of employees resigned.[213] The public has also stepped in to discourage companies from building technology to assist the administration's deportation machine.[214] To take a stand against the destructive practice of immigration surveillance, it is time for lawyers to choose to do the same.

CONCLUSION

The technological advancements of the last few decades have required lawyers to consider new ethics scenarios around email communications,[215] social media use in practice,[216] and blogging. Similarly, lawyers must now consider the ethical ramifications of using Westlaw and Lexis in the big data policing era, where legal research supports and overlaps with the very systems that turn data over to government enforcement entities, including ICE.

It's imperative that lawyers focus on these ethical quandaries now, because the government grows thirstier for more personal information as new surveillance and data technologies develop. RELX Group, Thomson Reuters, and other information companies will continue to build products to please this ever-growing surveillance customer base. At the Extreme Vetting Program investor day, ICE asked data companies for products the companies had not yet developed. It is likely that the investor day attendees will work to build those products and more for ICE in the near future. As long as legal research companies play a role in enabling government and ICE surveillance—and it is clear that they do—the legal community should condemn them and dump their products for more ethical alternatives.

213. Daisuke Wakabayashi & Scott Shane, *Google Will Not Renew Pentagon Contract that Upset Employees*, N.Y. TIMES (June 1, 2018), https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html [https://perma.cc/MWT4-94JM].

214. *See* THE ACTION NETWORK, *Sign the Petition to IBM's CEO: Don't Help Trump Deport Immigrants*, https://actionnetwork.org/petitions/dont-build-trumps-deportation-machine?source=IBMvetting_20171116_CMJ (last visited Oct. 15, 2018) [https://perma.cc/RE5X-8MKS] (public petition calling on IBM to decline to bid on the Extreme Vetting initiative).

215. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 477R (2017).

216. *See, e.g.*, ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 480 (2018); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 479, 5 (2017).