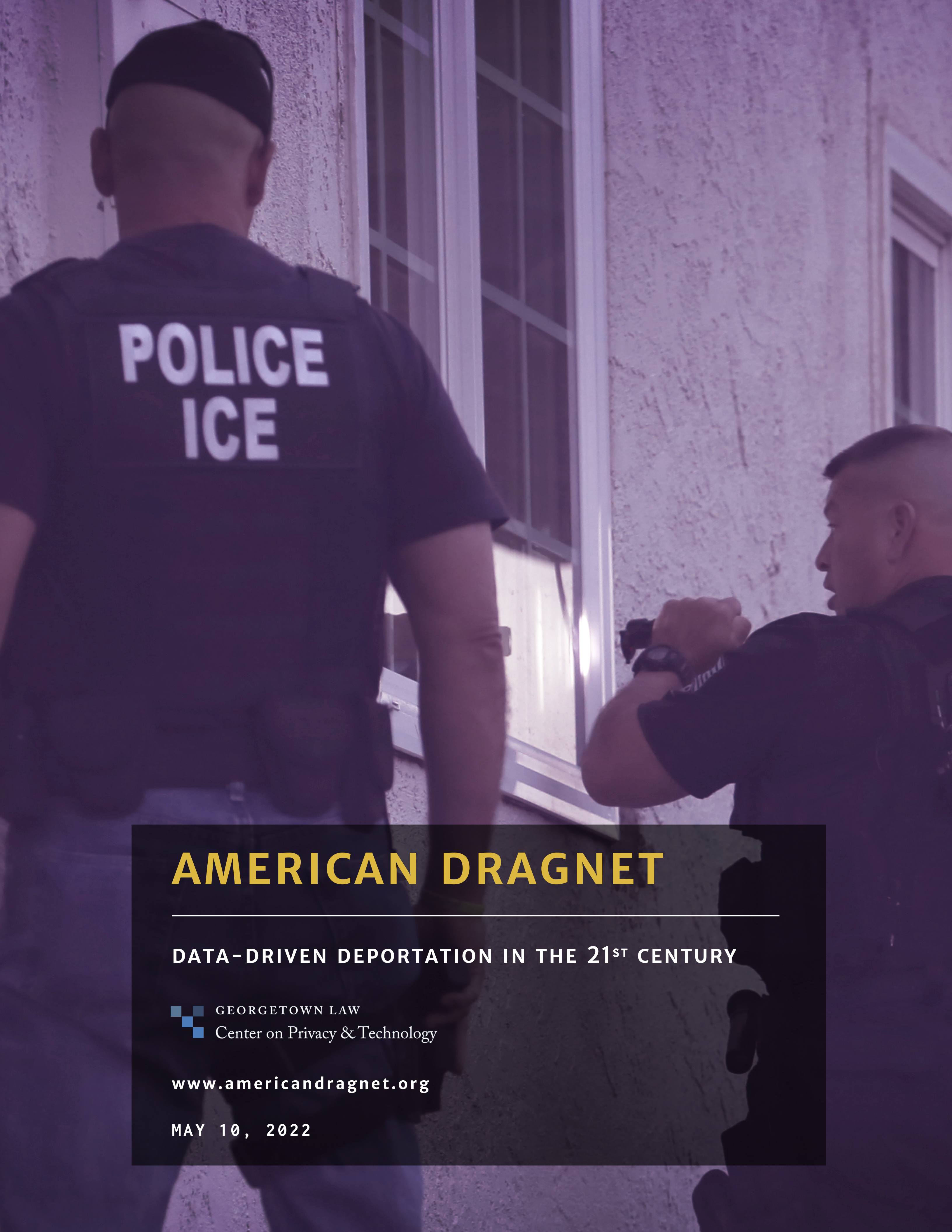


AMERICAN DRAGNET

DATA-DRIVEN DEPORTATION IN THE 21st CENTURY

GEORGETOWN LAW
Center on Privacy & Technology

www.americandragnet.org

MAY 10, 2022

Cover image: ICE conducts a raid to apprehend immigrants.
(Photo: Irfan Khan/LA Times via Getty Images)

AMERICAN DRAGNET

DATA-DRIVEN DEPORTATION IN THE 21ST CENTURY

GEORGETOWN LAW
Center on Privacy & Technology

ABOUT THIS PROJECT

Nina Wang, Allison McDonald, Daniel Bateyko and Emily Tucker are the authors of this report. Harrison Rudolph led the underlying research.

SUGGESTED CITATION

Nina Wang, Allison McDonald, Daniel Bateyko & Emily Tucker, *American Dragnet: Data-Driven Deportation in the 21st Century*, Center on Privacy & Technology at Georgetown Law (2022).

CONTACT

privacy@georgetown.edu / 202-662-9779

DESIGN

Rootid

www.americandragnet.org
www.law.georgetown.edu/privacy-technology-center

MAY 10, 2022

TABLE OF CONTENTS

EXECUTIVE SUMMARY

When you think about government surveillance in the United States, you likely think of the National Security Agency or the FBI. You might even think of a powerful police agency, such as the New York Police Department. But unless you or someone you love has been targeted for deportation, you probably don't immediately think of Immigration and Customs Enforcement (ICE).

This report argues that you should. Our two-year investigation, including hundreds of Freedom of Information Act requests and a comprehensive review of ICE's contracting and procurement records, reveals that ICE now operates as a domestic surveillance agency. Since its founding in 2003, ICE has not only been building its own capacity to use surveillance to carry out deportations but has also played a key role in the federal government's larger push to amass as much information as possible about all of our lives. By reaching into the digital records of state and local governments and buying databases with billions of data points from private companies, ICE has created a surveillance infrastructure that enables it to pull detailed dossiers on nearly anyone, seemingly at any time. In its efforts to arrest and deport, ICE has—without any judicial, legislative or public oversight—reached into datasets containing personal information about the vast majority of people living in the U.S., whose records can end up in the hands of immigration enforcement simply because they apply for driver's licenses; drive on the roads; or sign up with their local utilities to get access to heat, water and electricity.

ICE has built its dragnet surveillance system by crossing legal and ethical lines, leveraging the trust that people place in state agencies and essential service providers, and exploiting the vulnerability of people who volunteer their information to reunite with their families. Despite the incredible scope and evident civil rights implications of ICE's surveillance practices, the agency has managed to shroud those practices in near-total secrecy, evading enforcement of even the handful of laws and policies that could be invoked to impose limitations. Federal and state lawmakers, for the most part, have yet to confront this reality.

This report synthesizes what is already known about ICE surveillance with new information from thousands of previously unseen and unanalyzed records, illustrating the on-the-ground impact of ICE surveillance through three case studies—ICE access to driver data, utility customer data and data collected about the families of unaccompanied children. The report builds on, and would not have been possible without, the powerful research, organizing and advocacy of immigrant rights organizations like CASA, the Immigrant Defense Project, Just Futures Law, Mijente, the National Immigration Law Center (NILC), Project South and the American Civil Liberties Union (ACLU) of Northern California (among many others), which have been leading the effort to expose and dissever ICE's American dragnet.

A. FINDINGS

ICE surveillance is broader than people realize. It is a dragnet.

Most Americans probably do not imagine that their information is captured by ICE's surveillance networks. In fact, ICE has used face recognition technology to search through the driver's license photographs of around 1 in 3 (32%) of all adults in the U.S. The agency has access to the driver's license data of 3 in 4 (74%) adults and tracks the movements of cars in cities home to nearly 3 in 4 (70%) adults. When 3 of 4 (74%) adults in the U.S. connected the gas, electricity, phone or internet in a new home, ICE was able to automatically learn their new address. Almost all of that has been done warrantlessly and in secret.

ICE built its surveillance dragnet by tapping data from private companies and state and local bureaucracies.

For most of its history, immigration enforcement in the United States was a small data affair, relying primarily on ad hoc tips and information sharing agreements with state and local law enforcement agencies. After 9/11, ICE paired those programs with much broader initiatives, tapping vast databases held by private data brokers as well as state and local bureaucracies historically uninvolved with law enforcement. Through those initiatives, ICE now uses information streams that are far more expansive and updated far more frequently, including Department of Motor Vehicle (DMV) records and utility customer information, as well as call records, child welfare records, credit headers, employment records, geolocation information, health care records, housing records and social media posts. Access to those new data sets, combined with the power of algorithmic tools for sorting, matching, searching and analysis has dramatically expanded the scope and regularity of ICE surveillance.

ICE has scanned the driver's license photos of 1 in 3 adults.

ICE has access to the driver's license data of 3 in 4 adults.

ICE tracks the movements of drivers in cities home to 3 in 4 adults.

ICE could locate 3 in 4 adults through their utility records.

ICE has invested heavily in surveillance and has acquired advanced surveillance technology far earlier than people realize.

A review of over 100,000 spending transactions by ICE reveals that the agency spent approximately $2.8 billion between 2008 and 2021 on new surveillance, data collection and data-sharing initiatives. Those transactions also reveal that ICE was building up advanced surveillance capacities roughly half a decade earlier than previously known. Until now, the earliest records obtained by the Center on Privacy & Technology suggested that ICE began requesting and using face recognition searches on state and local data sets in 2014. However, our research uncovered a contract from 2008 between ICE and the biometrics contractor L-1 Identity Solutions. The contract enabled ICE to access the **Rhode Island** motor vehicle department's face recognition database to "recognize criminal aliens." That places the first known ICE face recognition searches during the waning days of the George W. Bush administration.

ICE exploits people's vulnerability and trust in institutions to get its hands on more data.

To locate its targets, ICE takes data that people give to state and local agencies and institutions in exchange for essential services. ICE often accesses that data without the permission or even awareness of the entity that originally collected the information. ICE has also taken advantage of the vulnerability of unaccompanied children seeking to reunite with their families.

- **ICE leverages people's trust in state DMVs to target deportations.**

  Across the country, 16 states and Washington, D.C. have allowed undocumented people to apply for driver's licenses, provided that they volunteer a range of personal information including their legal names, dates of birth and addresses. Hundreds of thousands of undocumented people have trusted state DMVs with that information to apply for driver's privileges. However, in at least five of those 17 jurisdictions, ICE can warrantlessly search through state driver records for the purpose of civil immigration enforcement. In at least six of those 17 jurisdictions, ICE has used face recognition to scan drivers' license photographs to carry out deportations. When undocumented drivers apply for licenses, they place a significant amount of trust in the state that their information will not be used against them. Allowing ICE to use driver records for immigration enforcement purposes is a profound betrayal of that trust.

- **ICE leverages people's need for water, gas, electricity, phone and internet to target deportations.**

  In addition to pulling DMV data, ICE also buys and searches customer records from utility companies to locate people for deportation. The agency has been able to access information from utility records by contracting with Thomson Reuters, a private data broker. While undocumented people may avoid sharing their information with entities like DMVs, it creates extreme hardship when people cannot connect their homes with water, gas, electricity, phone and internet. "For people who are not easily traceable via traditional sources," a Thomson Reuters marketing letter reads, "locator information from utility hookup records may provide the only current and accurate address and phone number data available." By contracting with private data brokers, ICE has been able to access utility record information belonging to over 218 million utility customers across all 50 states and the district.

- **ICE used interviews with unaccompanied children to find and arrest their family members.**

  In the last two decades, the number of unaccompanied children fleeing violence and poverty by crossing the U.S. border has risen by an order of magnitude. When children arrive at the border, they are suffering physical and emotional trauma. Congress has tried to protect those children by enacting bipartisan legislation to transfer the responsibility for their care away from law enforcement and to the U.S. Department of Health and Human Services (HHS).

To find proper placements for the children, HHS interviews them about any potential family members in the U.S. who could care for them. But in perhaps the starkest example of ICE exploiting the trust of vulnerable people, the agency entered into an information-sharing agreement with HHS to use the information these children and their family members shared to find and arrest at least 400 of those family members. While Congress later used an appropriations rider to partly end the program and U.S. Department of Homeland Security (DHS) Secretary Alejandro Mayorkas has since formally rescinded it, this arrangement illustrates the lengths that ICE has been willing to go to find information on potential targets.

ICE exploits people's trust and vulnerability to get its hands on more data.

ICE surveillance has evaded congressional oversight.

Most congressional leaders did not learn about ICE face recognition scans of DMV photos until The Washington Post ran an exposé on the practice, reporting on records obtained by the Center on Privacy & Technology. This exposé ran in 2019, over a decade after ICE penned its first known face recognition contract in 2008 for access to the **Rhode Island** driver database. The fact that ICE was conducting face recognition scans on driver's license photos came as a shock to senior lawmakers—even those with the greatest insight into DHS activities. On learning of the face scans, Rep. Zoe Lofgren, the longtime chair of the House Judiciary Subcommittee on Immigration and Citizenship, denounced the practice as "a massive, unwarranted intrusion into the privacy rights of Americans by the federal government, done secretly and without authorization by law." ICE's surveillance initiatives have regularly flown under Congress' radar. While a few political leaders have pressed ICE in oversight letters and used appropriations riders to end the most aggressive of ICE's actions, to date there has not been one full congressional hearing or Government Accountability Office (GAO) report focused on ICE surveillance.

State authorities are largely unaware of ICE's surveillance of residents.

State lawmakers are almost always entirely unaware of ICE surveillance in their states and typically learn about the agency's actions from the news. When Rep. Angela Romero of Utah learned that ICE and the FBI had searched through driver's records in her state, she responded as many lawmakers do when information about ICE surveillance comes to light: "[T]his has never been shared with us before and the Legislature hasn't approved it." The lack of awareness from political leaders is compounded by state agencies' failure to control or track ICE access to residents' data. In **Maryland**, for example, when lawmakers asked two state agencies—the Maryland State Police and the Maryland Motor Vehicle Administration—for information about ICE searches of Maryland driver's license data, the agencies each disclaimed responsibility and referred to the other as the ultimate custodians of information about ICE's access.

ICE has evaded state laws and lawmakers' efforts to rein in its surveillance capabilities.

When state officials enact laws and policies to cut off their states' data sharing with ICE, ICE regularly evades those restrictions—often by using alternative points of access within the complex web of systems connecting state and federal databases. In **Washington**, Governor Jay Inslee enacted a statewide policy to limit state agency cooperation with ICE only to discover that state licensing officials were routinely violating that policy. When state officials cut off ICE's access to a state-run driver database, previously unseen records show that DHS searches of a separate network of driver data—one not operated by the state—nearly doubled. In **Oregon**, soon after lawmakers passed a law cutting off state data disclosures to ICE, the Oregon DMV signed agreements to sell its driver's license records to Thomson Reuters and LexisNexis Risk Solutions, the two primary data brokers that sell ICE access to driver information.

ICE surveillance deters people from accessing essential services.

Historically, the "chilling effects" of government surveillance refer to the way in which surveillance deters individuals from engaging in activities that the First Amendment protects, such as freedom of speech and assembly. But a growing body of research suggests that fear of ICE surveillance also deters immigrants and their families from participating in a broad range of activities necessary for health and well-being not only of individuals, but of the communities of which they are part. Concern about ICE surveillance often leads individuals to avoid placing their information in government systems, even if those systems are unrelated to law enforcement. That fear inhibits people from enrolling in services critical for their own health and the health of their children. It also deters people from engaging with the legal system, such as by reporting crimes or testifying in court.

B. RECOMMENDATIONS

Congress

- **Congress should reform U.S. immigration laws to radically reduce the number of people who can be subjected to deportation.** The best and ultimately perhaps the only way to take apart ICE's dragnet is to take apart the laws on the basis of which the executive branch targets hundreds of thousands of people for deportation every year. Congress could significantly reduce the number of people subject to deportation by—for example—creating a pathway to citizenship for undocumented people, dramatically reducing the grounds of removability that are based on criminal legal involvement, and by enacting a statute of limitations on deportations. While those reforms do not address surveillance itself, they are the most direct way to undercut ICE surveillance authority.

- **Congress should protect people who trust the federal government with their data.** The federal government runs a range of programs that effectively ask undocumented people to out themselves and entrust the federal government with their personal information. A few examples of those programs include the Deferred Action for Childhood Arrivals (DACA) program, the IRS's use of individual taxpayer identification numbers and the U and T visas available to victims of certain crimes. It is unethical and arguably a violation of due process to use those programs as honeytraps for the undocumented. Congress could easily create a wraparound statute protecting that kind of data. Congress could model the wraparound statute on the federal laws protecting the confidentiality of census data, which prohibit the use of census data for nonstatistical purposes and broadly mandate that "[i]n no case shall information furnished [to the Census Bureau] be used to the detriment of any respondent or other person to whom such information relates."

Congress could model a law to protect data volunteered by undocumented immigrants after Census confidentiality statutes.

Until the passage of such a wraparound statute, Congress could protect information held in specific programs via piecemeal amendments to relevant statutes or appropriations riders. For its part, DHS could enact those protections as a matter of policy.

- **Congress should stop ICE's use of DMV data as a deportation gold mine.**
  Congress passed the Driver's Privacy Protection Act (DPPA) years before the modern era of mass deportation. ICE has not hesitated to use the broad carve-outs for government access in the DPPA to warrantlessly scan the driver's license photographs belonging to millions of Americans and to search through the address information of most U.S. residents provided on their driver's records. Congress should update the DPPA to prohibit (or require a warrant or court order for) any use of DMV data for immigration enforcement purposes.

- **Congress should conduct aggressive oversight of ICE surveillance.**
  Committee and subcommittee chairs do not need a majority or supermajority vote to compel ICE to answer for the massive expansion of its surveillance initiatives and the vast secrecy that surrounds them. ICE surveillance raises a wide range of fundamental constitutional concerns about everything from commerce to federalism, and each chamber of Congress has multiple committees and subcommittees that could lead aggressive oversight of the agency. Potential subjects for hearings or a GAO report include: (1) how and why ICE evades state laws protecting the data of drivers and other residents; (2) how ICE's reliance on data brokers limits public scrutiny and helps the agency evade statutory and constitutional privacy protections; and (3) how ICE currently uses biometrics, including face recognition, fingerprints and DNA, and how it plans to use them in the future. A more complete list can be found in the **Recommendations** section.

DHS & ICE

- **ICE should end all dragnet surveillance programs, including the use of face recognition on DMV data for immigration enforcement.**
  All of ICE's surveillance programs should be subjected to piercing scrutiny. However, ICE should immediately terminate all dragnet surveillance programs—both ICE led and obtained from data brokers—which indiscriminately collect data on as many people in the U.S. as possible. Programs that ought to be characterized as this type of especially problematic dragnet surveillance

include at least (1) the practice of scanning driver's license photos for immigration enforcement purposes; (2) the bulk collection of address information and other records from DMVs and utility companies; (3) the bulk collection of license plate photos capturing the movement of drivers in major US metropolitan areas; (4) the purchase of large datasets from private data brokers.

- **ICE should stop using water, heat, light, phone and internet records to carry out deportations.**

  People need heat, water and electricity to survive. They require phone lines for emergencies and internet access to work and attend school. DHS should not wait until immigrants begin cutting off those services for fear of deportation before issuing a clear prohibition against the use of utility records for immigration enforcement.

States

- **States should protect people who trust state and local governments with their data.**

  Of the 17 jurisdictions that offer undocumented residents the ability to apply for driver's licenses, seven have passed laws seeking to protect against warrantless ICE searches and face scans of drivers' data and photos. Unfortunately, few states have enacted truly comprehensive restrictions on ICE access to driver data. These statutes should: (1) focus on the data, not the custodian of that data; (2) focus on the purpose of the sharing, not the recipient; (3) protect against all forms of information sharing; (4) not distinguish between "civil" and "criminal" immigration enforcement; (5) ensure that face recognition is clearly encompassed in these restrictions; and (6) eliminate blanket exceptions for "law enforcement" access to state or locally held data.

State lawmakers have a major role to play in protecting their constituents against warrantless ICE surveillance.

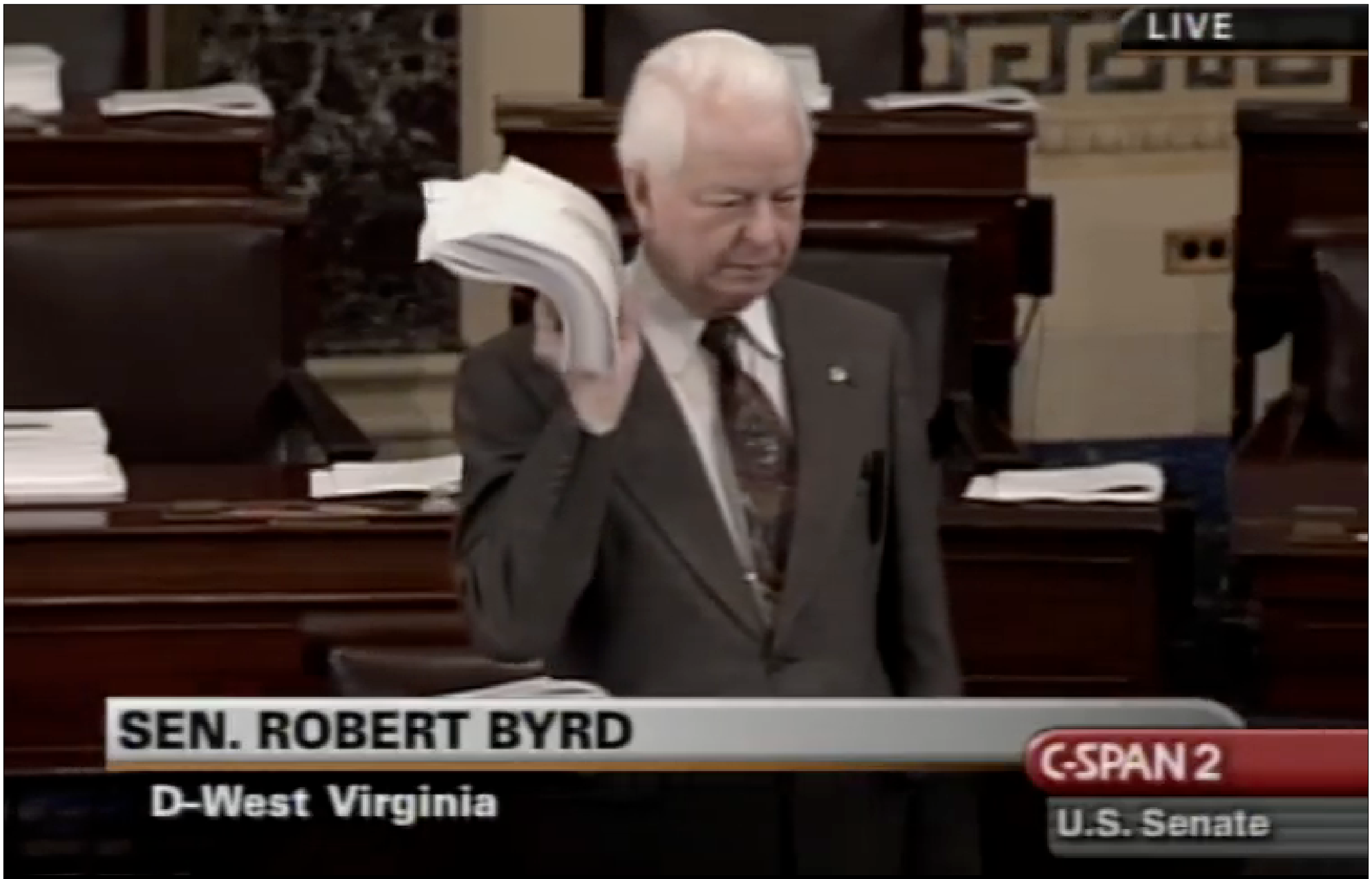
- **States should prohibit the use of water, gas, electricity, phone and internet records for immigration enforcement.**

  State and local authorities should prohibit the disclosure, sale or resale of this data for immigration purposes. Again, while a few states have good standards that apply to a specific utility (e.g., gas or electricity), not one has enacted meaningful wraparound privacy protections for customers of all utility services. In enacting these protections, state and local authorities should: (1) restrict disclosure to data brokers, not just the government; (2) avoid blanket carve-outs for credit reporting and evaluation; (3) protect against all forms of disclosure; and (4) be sure to protect customer addresses. Of all laws available, Connecticut laws governing the privacy of information held by gas companies likely represent the most protective standard to date.

- **States should structure their systems to track ICE access and closely audit that access.**

  Any state database administrator must be able to answer two questions: Does ICE have access to this database? If so, how and why has ICE accessed it? In the third decade of the 21st century, there is no excuse for a state or local government to build a database containing sensitive data without ensuring that the system carefully logs the times and frequency of user logins, as well as their searches and search results. State and local authorities should regularly audit these databases to determine whether, how and how often ICE is accessing them. If authorities do not run those audits on their own, legislators should send oversight letters to state agencies and hold oversight hearings to compel agency officials to do so.

INTRODUCTION: ROBERT BYRD AND JOSÉ HERNANDEZ



Sen. Robert Byrd holds a copy of the Homeland Security Act of 2002 while arguing against the legislation. (Photo: C-SPAN 2)

On Nov. 19, 2002, the bill to create the DHS came up for a final vote in the U.S. Senate. It had so far received little opposition. In the words of its leading opponent, the Homeland Security Act was "barrelling through Congress like a Mack truck, threatening to run over anyone who dares stand in its way."[1]

That critic was not the liberal lion Ted Kennedy, nor was it Russ Feingold of Wisconsin, the senator who cast the sole vote against the USA PATRIOT Act upon its passage, 98-1, a year earlier.[2] Rather, the voice of opposition belonged to Senator Robert Byrd of West Virginia, a man who had devoted decades of his career in Congress to building precisely the kind of federal bureaucracy that the bill would create.[3]

Perhaps the senator was worried that the sudden reorganization of dozens of federal agencies and over 150,000 employees under one new department would loosen his grip on those bureaucracies and the jobs they brought to his state. Across a half-century in Congress, Byrd had systematically steered federal facilities to his home state, including military training centers and the FBI fingerprint lab. In the coming years, he would eventually move the Coast Guard's National Maritime Center to landlocked Martinsburg, West Virginia.[4]

Senator Byrd warned of a program that would "peer into the daily transactions and private lives of every American."

Yet, that's not what Byrd talked about when he savaged the bill on the floor of the Senate.[5] Instead, he dismissed out of hand the primary rhetorical justification for the bill—that is, the idea that the bill was responding to an urgent national security need. The law enforcement officials charged with defending the country were already "out there … right now, right today," he explained.[6] He also rejected the suggestion that the bill was necessary to pay for domestic security, pointing out that Congress had approved $5.1 billion in emergency spending earlier that year, which President George W. Bush had declined to sign into law.[7] Instead, Byrd issued a warning: The Homeland Security Act was an "enormous grant of power to the executive branch."[8] The DHS would function as "a massive chamber of secrets" immune to transparency, internal auditing and external oversight.[9] The bill would empower the president "without any real mechanism to ensure those powers are not abused."[10]

In his darkest admonition, Byrd said that the result of this secrecy and impunity would be dragnet surveillance.[11] He had previously cautioned that the bill gave the Secretary of DHS "almost unlimited access to intelligence . . . without adequate protections against misuse" of that data.[12] On Nov. 19, he put it bluntly: "The [White House] told us it is not planning to create a new domestic spy agency in the United States," and yet the bill would authorize a Pentagon program that would "peer into the daily transactions and private lives of every American."[13]

That afternoon, Byrd's colleagues voted 90 to 9 in favor of the Homeland Security Act.[14] When asked why he had so fervently opposed a bill he knew would pass, Byrd answered: "[T]he matter is there for a thousand years in the record. I stood for the Constitution. I stood for the institution. If it isn't heard today, there'll be some future member who will come through and . . . comb these tomes."[15]

José Santos Quintero Hernandez of Rockville, Maryland in front of CASA headquarters in Adelphi, Maryland. (Photo: Alex Vazquez, CASA)

José Santos Quintero Hernandez and Maribel Cortez have been married for 22 years. They met in the U.S. after emigrating separately from El Salvador, fleeing violence and what Hernandez described as certain death.[16] The couple had led a quiet life, raising five children in Rockville, Maryland, a suburb less than one-hour's drive from the U.S. Capitol.[17]

One morning in early February 2020, a little over 17 years after Byrd's remarks, the Hernandez family got a knock at their door. One of the children opened it. The kids watched as ICE agents entered the house, arrested their father and took him away.

There are millions of undocumented people in the U.S. How did ICE come to arrest Hernandez? Had he just arrived and missed a court date? No, he had been living here for decades. Had he come to ICE's attention through local law enforcement? No, neither Hernandez nor Cortez had ever had any encounters with the police or immigration enforcement.

No, the agents explained to Hernandez as they walked him to their car. They found him because he had recently obtained a Maryland driver's license. They used the information he gave to the Maryland Motor Vehicle Administration to find him, arrest him, lock him up in an immigration detention center and start deportation proceedings against him.[18]

Later that month, The Washington Post and The Baltimore Sun revealed that, in addition to

Del. Joseline Pena-Melnyk. (Photo by Danielle E. Gaines and MarylandMatters.org)

searching through Maryland drivers' personal information—their names, addresses and dates of birth—ICE had also been scanning Maryland drivers' *faces* and conducting face recognition searches on their license photos. Those warrantless searches were not restricted to undocumented immigrants or other applicants for what are called "standard" licenses; ICE had been logging into a state face recognition database and scanning the faces of the state's drivers, which totaled more than 4 million people.[19]

Maryland lawmakers were shocked—particularly those who had led the effort in 2013 to allow undocumented residents to apply for licenses. Delegate Joseline Peña-Melnyk of Prince George's County was distraught to learn ICE was tracking down Maryland immigrants using a program she had supported. "It breaks your heart," she told The Washington Post. "We didn't know. We could have gotten it right in the beginning if we knew."[20] To this day, state officials seem to have no idea how many times ICE has scanned the faces of Maryland drivers.[21]

> **"We didn't know. We could have gotten it right in the beginning if we knew."**

What happened to Hernandez—and what happened in Maryland—is not unique. These discoveries are part of a common pattern. ICE quietly runs face recognition scans not just on Marylanders and not just on immigrants but on millions of drivers across the country.[22] ICE has also paid a data broker to gain access to a trove of license plate photos logging the daily movements of drivers in the 50 largest metropolitan areas in the U.S.[23] ICE also paid a separate data broker for the ability to search address records held by water, gas, electric, phone and cable companies, such that the moment a family, immigrant or native-born, moves into a new home and connects the water or turns on the lights, ICE can track them down.[24] When children arrived alone at the border, ICE even used information from interviews with these children to find, arrest and deport their family members.[25]

ICE consistently paints itself as an agency whose efforts are "focused" and "targeted" against specific individuals or limited groups of people, but those discoveries uncover a much different story.[26] When ICE uses bulk data from sources like driver's license records and utility customer information or engages in regular monitoring of a vast majority of people in the U.S., the relationship between ICE's supposed law enforcement purpose and its actual law enforcement practices begins to seem quite attenuated. Rather than being tailored or limited in any meaningful way, present day ICE surveillance is a sweeping dragnet.

The full reach of ICE's surveillance dragnet still remains secret. Press coverage offers snapshots of specific initiatives, often with little distinction between programs run by Customs and Border Protection (CBP) and those ICE operates. Few privacy advocates think of immigration enforcement as a site of large-scale surveillance, while immigrant rights advocates and organizers, overwhelmed with the work of resisting mass deportation themselves, often lack the resources to investigate the surveillance programs that are fueling the system. For its part, Congress has yet to devote a full oversight hearing to ICE surveillance. As a result, basic questions about ICE's surveillance arsenal have gone unanswered:

- How often does ICE search through driver information held by state DMVs?
- How many people have had their faces scanned by ICE?
- How many people have had their addresses sold to ICE as a result of connecting their water, electricity, gas, telephone or cable, and how exactly did ICE obtain that data?
- Why did ICE suddenly amass this arsenal, when its predecessor, the Immigration and Naturalization Service (INS), made few major technology investments?
- Does the law allow this surveillance, and if so, why?

This report, the product of a two-year investigation involving over 200 Freedom of Information requests, a review of over 100,000 ICE procurement transactions and a series of comprehensive legal surveys, fills many of those gaps. It explains the historical and legal context that has allowed ICE to create its dragnet and offers policymakers and advocates a frame through which to understand it. The report also illustrates the reach of ICE surveillance through case studies on ICE's use of:
(1) DMV data and photos, (2) utilities data and (3) interview data from unaccompanied children detained at the border.

The results of our investigation paint a stark picture of dragnet surveillance, indicating that ICE has used face recognition technology to scan the driver's license photographs of **1 in 3** adults, has access to the driver's license data of **3 in 4** adults, is able to track the movements of drivers in cities home to **3 in 4** adults and could locate **3 in 4** adults through their utility records. Secrecy, impunity, dragnet surveillance—19 years after Byrd stood in the well of the U.S. Senate and declaimed against the Homeland Security Act, his warning has come to pass.[27]

ICE has scanned the driver's license photos of 1 in 3 adults.

ICE has access to the driver's license data of 3 in 4 adults.

ICE tracks the movements of drivers in cities home to 3 in 4 adults.

ICE could locate 3 in 4 adults through their utility records.

This report is not the first to describe ICE's surveillance dragnet. For years, organizations like CASA, the Immigrant Defense Project, Just Futures Law, the Legal Aid Justice Center, Make the Road, Mijente, the NILC, the National Immigrant Justice Center (NIJC), the ACLU, Project South and dozens of others have warned of, and advocated against, ICE surveillance. This report is the first, however, that attempts to *quantify* the reach of ICE surveillance into "the daily transactions and private lives of every American," as Byrd predicted. Based on this new research and analysis, the report calls upon Congress to investigate and conduct oversight into ICE surveillance, and it offers policymakers and communities a set of concrete suggestions for taking apart this American dragnet.

A. SCOPE AND METHODOLOGY

1. Scope

Almost all of DHS's immigration control and enforcement operations have gone high tech, not just those run by ICE. Those systems are complex and interconnected, making it difficult to get a clear picture of any one agency's surveillance capacity.[28] This report focuses specifically on ICE, the agency charged with enforcing immigration law within the interior of the U.S. It does not touch upon, for example, the surveillance capacities of CBP, whose responsibilities include vetting travelers arriving from abroad and interdicting people entering the country without inspection at the border. The report is concerned with ICE's technical and legal ability to identify and target people *inside* the country for deportation, explaining how interior immigration enforcement has undergone profound yet often little-noticed transformations in the 21st century.

The report begins by offering a framework to understand the transformation of ICE surveillance. It then presents three case studies on different ICE surveillance initiatives. Two of those case studies—ICE's accessing state DMV databases and private utility customer records—illustrate ICE's reach beyond state and local law enforcement systems into records created by a much wider range of state and local government agencies. Those records encompass the majority of a state's adult population and do not distinguish (in some cases because law or policy prohibits distinguishing) between people on the basis of immigration status. The third case study, which describes ICE's use of information collected from unaccompanied immigrant children arriving at the border, underscores ICE's brazen refusal to observe basic legal and ethical norms and how contemporary understandings of chilling effects fail to capture to full scope of the harms of surveillance.

2. Methodology

To place ICE surveillance within a legal and historical context, the authors and approximately a dozen supporting researchers, including Center staff and fellows, Georgetown Law students and Georgetown University undergraduates, employed a range of research methods.

First, we filed over 200 Freedom of Information requests with state and local entities. Those requests fell into three categories:

- 51 requests to the DMVs for all 50 states plus Washington, D.C., focusing on the DMVs' use of face recognition systems and their disclosure of driver information to data brokers;
- 60 requests to the nation's largest municipal gas, water and electric utilities, focusing on their disclosure of customer information to ICE and to data brokers; and
- 102 requests to the DMVs and lead state law enforcement agencies in all 50 states plus the district focusing on ICE's queries to their employees and via direct access to those entities' databases.

Those requests resulted in more than 9,000 pages of responsive documents. Our **Appendix** includes the model language for each of those requests. We informed our review of those responses with a separate survey of agency, congressional, and other reports and regulatory filings regarding INS' and ICE's approaches to interior enforcement.

Second, we conducted three separate legal surveys to understand the existing landscape of state and federal laws reining in ICE access to different kinds of data. These included:

- a survey of privacy laws applicable to gas, water, electric, cable and phone companies in all 50 states plus the district;
- a survey of state privacy laws for driver data held in the 17 jurisdictions (16 states plus the district) that offer driver's licenses or privilege cards to undocumented residents; and
- a survey of federal privacy laws, including the DPPA and federal privacy laws applying to cable and phone providers.

Third, to estimate ICE's surveillance capacities and investments, we reviewed every publicly available ICE procurement transaction listed on USAspending from 2008 to 2021, which totaled over 100,000 transactions. That involved an initial review to manually identify surveillance, data collection and data-sharing investments, followed by a second review aided by an algorithm trained on those known surveillance-related transactions. For more information on our use of process to identify ICE surveillance transactions and a detailed overview of our procurement review methodology, see the **Appendix**.

Fourth, we conducted a public source survey of all information regarding the Thomson Reuters CLEAR database, the LexisNexis

Accurint database and the data broker Equifax to better understand how those entities secured access to customer address information held by utilities companies. Our research revealed that those companies were likely tapping into data held by a little-known trade group, the National Consumer Telecom & Utilities Exchange (NCTUE)—likely unbeknownst to millions of people whose data that organization held. We felt ethically bound to disclose that information as soon as possible and so released the information to The Washington Post in February 2021.[29] The publication of our findings, combined with the advocacy of Just Futures Law and Mijente, led Senator Ron Wyden of Oregon to push NCTUE to cease the sale of over 170 million utility customers' names, addresses and other personal information.[30] As a result of these efforts, NCTUE instructed Equifax in October 2021 to end the sale of this data.[31]

Fifth, to understand the harms this surveillance caused, we reviewed sociological and other scholarly literature on the impact of modern, data-driven immigration enforcement on the everyday lives of immigrants: their willingness to go to the doctor, to take their kids to school or to allow them to play on a public playground. That evidence-based and peer-reviewed research offers critical insight into the impact of surveillance and is not often taken into account in modern policy making around surveillance.

Finally, before and throughout this two-year period, we engaged in two advocacy initiatives that have given us a much clearer picture of the federal and state authorities that can limit ICE's surveillance activities and conduct oversight to rein the agency in. We worked with the Brennan Center for Justice, NIJC and several other civil society organizations to mobilize a coalition of national immigrant rights and privacy organizations to press Congress to block ICE's use of data from detained, unaccompanied children to target their sponsors for arrest and deportation.[32] That effort succeeded in the passage of a 2018 appropriations rider that cut off ICE's use of the data in many, but not all, instances.[33] DHS Secretary Alejandro Mayorkas finally ended the program in 2021.[34]

We also partnered with CASA, the mid-Atlantic region's leading immigrant rights organization, in conjunction with Georgetown Law's Federal Legislation Clinic to pass privacy laws in Maryland protecting utility customer records, driver records and other state-held data against warrantless disclosure to ICE or other immigration authorities. Those efforts succeeded in the passage of the Maryland Driver Privacy Act (HB 23, SB 234).[35]

This report was peer-reviewed by 10 experts, a group of scholars, advocates and former government officials, including individuals previously employed by DHS. While some of our peer reviewers chose to remain anonymous, others are named in our **Acknowledgments**.

I. ICE BUILT ITS SURVEILLANCE DRAGNET BY AMASSING DATA GENERATED BY STATE AND LOCAL BUREAUCRACIES.

Since its creation in 2003, ICE has consistently marketed itself as a law enforcement agency that targets "criminal aliens," a term the agency has used to describe noncitizens who have had contact with law enforcement, regardless of whether they were actually convicted of an offense.[36] ICE uses the language of the criminal legal system to defend deportation rhetorically, but it also relies heavily on criminal legal system infrastructure to carry out enforcement operations. Over the last two decades, the immigrant rights movement has done powerful work to reveal the ways that ICE uses police and jails to investigate people for deportation, including through the notorious mandatory fingerprint sharing scheme known as Secure Communities (S-Comm), which established a system by which fingerprint scans taken by state and local law enforcement are automatically compared against a database operated by DHS, alerting ICE to possible immigration violations.[37]

What has received less attention, however, is ICE's deployment of a much broader array of data-sharing and data collection programs that amass information from sources *outside* of law enforcement.[38] As cities and states have enacted sanctuary policies limiting law enforcement cooperation with immigration officials, ICE has progressively expanded its surveillance toolkit to include troves of data beyond what can be provided by state and local police. ICE has turned toward government agencies like DMVs, asking for driver information and requesting face recognition searches on entire license photo databases. It has ramped up investments in contracts with private data brokers, buying access to billions of pieces of data sourced from places like credit agencies and utility companies.

This section traces the evolution of surveillance by ICE and its predecessor, INS. It illustrates the shift from programs that rely on information collected by law enforcement to programs that draw data from a far wider-ranging array of sources, including private companies and government entities with no law enforcement authority. It then tracks this expansion in terms of dollar expenditures, showing a dramatic increase in investments in the latter type of surveillance programs. As **Section II** and **Section III** further explain, it is the data collected outside the law enforcement context that ICE has used to weave its surveillance dragnet.

A. THE FEDERAL GOVERNMENT BUILT ITS IMMIGRATION ENFORCEMENT SYSTEM ON TOP OF ALREADY UNJUST SYSTEMS OF POLICING AND PUNISHMENT.

For most of the 20th century, large scale deportations were ad hoc and episodic, usually driven by xenophobic reactions to particular political events. Examples include the first deportations under the Chinese Exclusion Act and the militarized border sweeps to return Mexican workers under the mid-20th century initiative that the government named "Operation Wetback," after the racial slur.[39]

In 1986, however, the government began to build up a bureaucracy for systematized immigration enforcement, increasingly exploiting the same "law and order" politics that brought about the era of mass incarceration to justify the criminalization of immigrants. That year, driven by pressures created by Reagan-era mandatory minimum sentencing guidelines that overcrowded jails and prisons, Congress passed the Immigration Reform and Control Act (IRCA), which required that noncitizens convicted of certain criminal offenses be deported "as expeditiously as possible."[40] Ten years later, in 1996, the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) radically expanded the number and types of offenses that could subject a person to (often mandatory) detention and deportation.[41] After the passage of IIRIRA, the number of people detained and deported expanded dramatically and in tandem with the skyrocketing number of people incarcerated through the criminal legal system.[42] In subsequent years, Congress continued to use the construct of criminality to expand grounds for deportation and to roll back legal protections for people in immigration custody and in immigration court.[43]

As the legislature was using the framework of the criminal legal system to expand the statutory basis for deportation, the agencies tasked with immigration enforcement were relying on the resources of state and local police to investigate people for deportation. In 1988, the INS launched a pair of programs, eventually consolidated into the Criminal Alien Program (CAP), which placed federal immigration enforcement officers in jails and prisons to identify and arrest people for removal. Eight years later, Congress authorized 287(g) agreements, named for their authorizing provision in the Immigration and Nationality Act to allow state and local police to enforce immigration law. While many 287(g) programs deputized police officers operating in the field, most of them trained officers to operate in jails and prisons, identifying individuals in police custody whom INS could deport.[44] After its creation in 2003, ICE has continued to rely on CAP and 287(g) agreements to investigate potential targets for deportation among those who have been brought into the criminal legal system.

One consequence of building immigration enforcement systems on top of criminal enforcement systems is that Black and Brown immigrant communities, already suffering brutal and discriminatory targeting by local law enforcement, are doubly policed and, when that policing results in judicial intervention, doubly punished.

In 2008, ICE expanded its cooptation of policing infrastructure to include digital infrastructure with the launch of the Secure Communities program. The keystone of S-Comm is a fingerprint-sharing initiative that automatically sends the fingerprints of any person who is booked by federal, state or local law enforcement to the FBI and ICE.[45] While several states initially resisted enrolling in S-Comm, the Obama administration stated that participation was mandatory.[46] As a result, all 3,181 law enforcement jurisdictions in the country—in all 50 states, the district and five U.S. territories—were enrolled in the program.[47] In 2014, after years of intense pressure from the immigrant rights movement, President Obama and DHS Secretary Jeh Johnson suspended S-Comm but replaced it with the substantially similar Priority Enforcement Program (PEP), leaving the biometric information sharing processes across the country unchanged.[48] That enabled President Trump to issue an executive order immediately restarting S-Comm five days after his inauguration.[49] Although President Joe Biden revoked that order in early 2021,[50] the fingerprint-sharing program still remains in place today.

These data-sharing programs and cooperative agreements with law enforcement agencies became cornerstones of U.S. immigration enforcement. Just three years after the launch of S-Comm, the number of people deported under the program made up 20% of total deportations that year.[51] As of 2020, about 70% of ICE arrests resulted from ICE officers being notified of a person's impending release from jail or prison.[52] The increasing levels of cooperation between immigration officials and law enforcement also coincided with an explosion in the number of deportations from the U.S. Between 1955 and 1988, the year that the INS launched CAP's predecessor programs, the U.S. never deported more than 30,000 people in a year. After 1988, immigration enforcement never deported *fewer* than that number of people in a year. Following ICE's creation in 2003, the number of people deported annually never dropped below 200,000, hitting a high of 432,448 in 2013[53]—the year that Obama sought to pass immigration reform legislation.[54]

Despite how entrenched ICE's reliance on state and local law enforcement has become, the legal authority for many of these initiatives remains unclear. No statute explicitly authorizes the fingerprint sharing program or requires state and local law enforcement to participate.[55] The same is true for many other forms of information sharing, such as the inclusion of civil immigration records in the form of "Immigration Violator Files" in the FBI's crime database.[56] The surveillance strategies described in this report, which are made possible by digital technology and infrastructure developed over the last 20 years, simply were not contemplated by the legal and policy frameworks relating to immigration, much less to privacy and civil rights generally. Limiting ICE's enforcement practices through litigation has been an uphill battle since the first legal challenges to the Chinese Exclusion Act, which established a precedent of extreme deference to the executive on matters related to immigration.[57]

B. AFTER 9/11, ICE AGGRESSIVELY EXPANDED ITS DATA SOURCES BEYOND POLICE AND CORRECTIONS AGENCIES.

While ICE's initiatives to draw information from state and local police were rolled out with great publicity, its efforts to reach data streams from sources *outside* of law enforcement have been extremely secretive. ICE began broadening the scope of its data collection in response to the events of Sept. 11, 2001, as part of an overarching federal initiative to radically increase domestic surveillance under the auspices of the "war on terror." Before 9/11, immigration authorities rarely investigated cases outside of the criminal context. The INS did not have personnel dedicated to finding and deporting people who had overstayed their visas or individuals with outstanding final removal orders (referred to as "abscondees").[58] The INS was explicit that enforcing those types of cases was not a priority.[59] The agency seldom pursued people with removal orders, and its investigators did not work abscondee cases as a matter of policy.[60]

One of the main reasons the INS generally did not pursue visa overstays or people with outstanding removal orders was that it struggled to find them. As the agency noted, abscondees were mostly living within the community, not incarcerated in jail or prison.[61] When the Department of Justice (DOJ) Inspector General audited the INS's Detention & Deportation program, it found that the lack of address information was one of the most frequently cited reasons for the failure to issue a surrender notice informing people of their deportation date.[62] Although since the 1940s federal law had required permanent residents and visa holders to register their addresses with the government and notify federal officials of address changes,[63] those requirements were rarely enforced and few people complied with them, which meant that federal address registries were largely unhelpful for INS investigations.[64]

The INS considered new ways to accumulate more information to target these cases but did not ultimately follow through on implementing them. For instance, some INS officials suggested that the agency go to DMVs and data brokers for address data:

> If there is no known last home or work address for the alien, searches are frequently not practical . . . The District Director in Miami, along with D&D managers elsewhere, noted that access to nationwide motor vehicle and credit bureau data bases [sic], as well as access to Social Security data, would help locate aliens.[65]

Those recommendations were not adopted.

Everything changed after 9/11. When it was discovered that two of the 15 9/11 hijackers had overstayed a visa, government officials used that fact to reshape the discourse on American immigration enforcement. "For terrorists, travel documents are as important as weapons," the 9/11 Commission wrote, concluding that "more effective use of information available in U.S. government databases could have identified up to 3 hijackers."[66]

Suddenly, tracking visa overstays and people with outstanding removal orders became a top priority, with a clear focus on targeting Muslim and Arab people.[67] In January 2002, Deputy Attorney General Larry Thompson launched the Absconder Apprehension Initiative, establishing 40 immigration agent positions across seven cities to "locate, apprehend, interview, and deport" people in the broader community.[68] According to the program's guidelines, immigration agents were to prioritize targeting people who came from "countries in which there has been Al Qaeda terrorist presence or activity."[69]

Within one year, however, it was clear that the program faced the same constraints that hampered similar initiatives in the past: a lack of reliable data. At the start, the INS had set out to depart all 314,000 noncitizens with final orders of removal in the U.S.,[70] but after six months, the Absconder Apprehension Initiative teams were only able to apprehend 712 people.[71] The GAO conducted an analysis showing that AAI's immigration enforcement efforts had been frustrated by unreliable address records in government databases and again recommended that the government adopt other methods of obtaining that information, such as purchasing it from data brokers.[72]

Ultimately, the INS would pass on the task of investigating visa overstays and people with outstanding final removal orders to its successor. ICE inherited the teams that the INS created in February 2002 to locate immigrants with outstanding final removal orders, organized under the National Fugitive Operations Program.[73] ICE also promptly created two new offices, the Fugitive Case Management Unit and the Fugitive Operations Support Center, to send the teams information and leads on people who could be deported.[74] In June 2003, ICE also established the first unit to identify and remove visa overstays: the Compliance Enforcement Unit, which was rebranded as the Counterterrorism and Criminal Exploitation Unit in 2010.[75]

ICE began systematically securing new troves of data that it could use to pull people into detention and deportation. Unlike the data fueling prior initiatives, this new data came overwhelmingly from sources outside of law enforcement, including agencies and offices within federal, state and local governments, as well as from the private sector. As ICE sought to remedy the data shortages that hindered previous efforts to pursue cases, it amassed records far beyond what was provided by state and local police, allowing the agency to track a significantly larger number of people. With these efforts, the reach of ICE surveillance far exceeded that of the already massive databases maintained on arrestees and visa holders, usurping data sets that easily included the majority of people in the U.S.

C. ICE CONTRACTS REVEAL A HUGE EXPANSION IN SURVEILLANCE CAPACITY.

Over the past decade, ICE has invested heavily in programs to track large swaths of the general population. Our review of over 100,000 ICE spending transactions from 2008 to 2021 reveals that the agency's annual spending on surveillance programs grew more than fivefold during this period, skyrocketing from about $71 million to about $388 million per year.[76] To analyze ICE's surveillance spending throughout this period in more detail, we categorized each of the agency's contract transactions by the primary surveillance service that it provided. Those categories are defined in **Sidebar 1**. The full list of surveillance contracts we identified and our calculations of ICE spending are included in the **Appendix**.

Our categorization of ICE transactions offers insight into the magnitude of the agency's spending on surveillance programs as well as the scope of the information that those programs provide. For example:

- In total, ICE spent a little over $1.3 billion on **geolocation** providers from 2008 to 2021. The broadest and most controversial of those contracts is one that allows ICE to access a license plate scanning database provided by Vigilant Solutions. The database contains high-speed photos of license plates from passing vehicles, along with the date, time and GPS coordinates of where the image was captured.[77] Vigilant's database consists of two types of license plate scans: those collected by private businesses—known as commercial license plate data—and those collected by law enforcement agencies.[78] According to documents obtained by the ACLU of Northern California, Vigilant's collection of commercial license plate scans are collected in places like toll roads, parking lots and garages, as well as by private vehicle repossession agents across 47 states,[79] covering metropolitan areas encompassing approximately 54% of the U.S. population.[80] Using that database, ICE can automatically compare new plate scans against a hot list of vehicles it is looking for.[81] In 2014, Obama DHS Secretary Jeh Johnson had cited privacy concerns to drop plans for ICE agency-wide access to the database, but Trump DHS officials penned an agency-wide contract for access to the Vigilant data at the end of 2017.[82]

SIDEBAR 1.
CATEGORIZING ICE SURVEILLANCE SPENDING

ICE often used a single contract to obtain multiple surveillance systems. One contract with the vendor Babel Street, for example, may offer ICE access to both geolocation information and an accompanying set of data analysis tools.[83] We assigned every contract transaction a primary functionality, each of which are described below.

Biometrics. This category includes contracts for technologies that allow ICE to collect and analyze biometric data, including tools for face recognition and fingerprint or DNA testing.

Data Analysis. This category includes contracts for technologies that allow ICE to connect disparate data sources, analyze large volumes of data and conduct case management.

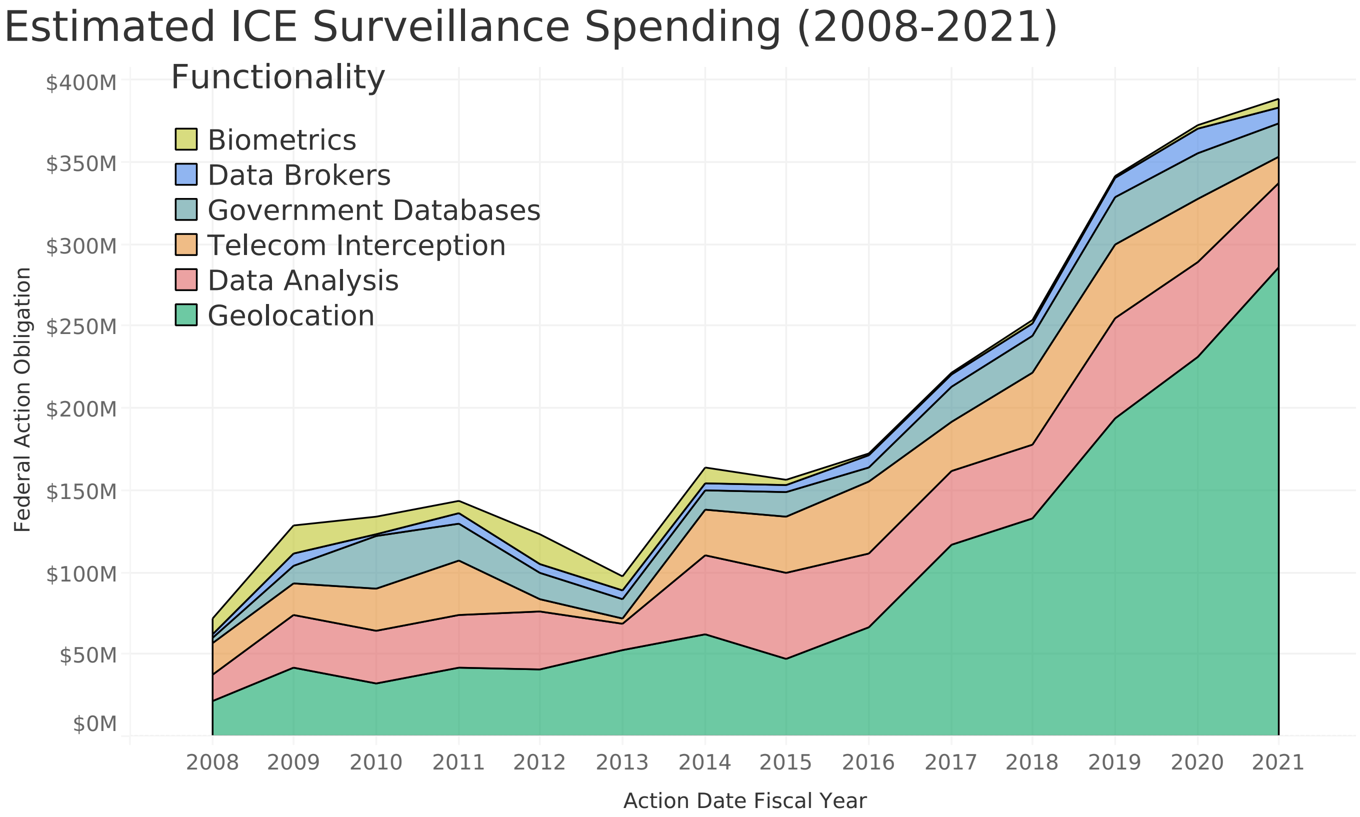
Geolocation. This category includes ICE contracts related to automated license plate readers, closed-circuit TV information, GPS tracking units, cell-site simulators and ankle monitors used in Alternatives to Detention programs.

Data Brokers. This category includes contracts for ICE to access private databases operated by companies that aggregate and sell individuals' information, including from credit headers and utility records.

Government Databases. This category includes contracts for state and local government databases, systems for indirect access to these databases and tools that facilitate sharing within these databases.

Telecom Interception. This category includes contracts for technologies that allow ICE to analyze and intercept telecommunications, including Title III wiretapping devices and Title III translation services, as well as Wi-Fi interception technologies. That does not include aggregators of information that may include telecommunications or video surveillance.

Figure 1.



- ICE spent roughly $96 million on **biometrics** in this period. One of the first ICE biometrics contracts, dated July 18, 2008, awarded $3,000 for a five-year contract for "services with the State of Rhode Island RMV services to access the face recognition database to recognize criminal aliens"[84]—placing the first known ICE DMV searches in the waning days of the Bush administration, roughly six years earlier than previously known. One of the most recent biometrics contracts, from September 2020, secured $224,000 for ICE's Dallas mission support office to use face recognition software from Clearview AI, a company known to have trained their algorithms on images scraped from public websites and social media pages without their subjects' knowledge.[85]

- ICE spent roughly $97 million on **data brokers** in this period. The primary contractor that has provided this service is Thomson Reuters, which offers a person-search database called CLEAR. The version of CLEAR built for law enforcement includes data from a massive range of different sources, including driver's licenses and vehicle registrations; credit headers, which contain the names, addresses, phone numbers and other personal information at the top of credit reports, collected in real-time from all three major credit reporting agencies; and, as discussed in **Section III**, address records from over 80 national and regional telephone, cable, gas, electricity and water companies across the country.[86] ICE's contract for the CLEAR database began in 2017 and was allowed to lapse in February 2021.[87] The agency appeared to replace this service with a new contract with LexisNexis Special Services, which offers a similar database.[88]

ICE began using face scans on DMV license photos in the closing days of the George W. Bush administration.

- ICE spent roughly $252 million on access to **government databases** in this period. The key database in this category is Nlets, the International Public Safety and Justice Network (formerly known as the National Law Enforcement Telecommunications System). As discussed in **Section II**, Nlets is a network operated by a nonprofit organization that allows ICE agents across the country to warrantlessly search 34 states' DMV databases for immigration enforcement purposes, including the databases of five of the 16 states that offer undocumented people the ability to apply for drivers' licenses.[89] Under Trump, ICE expanded many of its surveillance investments; in few other areas was this expansion more pronounced than in ICE's access to government databases.
- ICE spent roughly $389 million on **telecom interception** in this period.[90] The key vendors expanding ICE's wiretapping capabilities are JSI Telecom and Penlink, which sell interception equipment.[91] ICE uses Penlink equipment to track a person's phone calls or internet use in real time and collect a person's email and social media activity for later searches.[92] Although authorized on a case-by-case basis, each wiretap benefits from ICE's information stockpiles. ICE shares records obtained from wiretaps in its case management system using Penlink's custom-built software, allowing the agency to map connections between people.[93] ICE intercepts communications on such a scale that the agency needs half a dozen contractors to make sense of it all—wiretap translation services and storage contracts make up over half of ICE's telecom intercept spending.
- ICE spent roughly $569 million on **data analysis** in this period. That amount includes spending on ICE's third biggest contractor by dollar amount—Palantir Technologies. From 2008 to 2021, ICE awarded a total of $186.6 million to Palantir alone. Palantir's custom-built programs link together databases from a vast array of government and private sources, allowing ICE agents to access and visualize an interconnected web of data pulled from nearly every part of an individual's life. ICE has access to so much data, from so many sources, that its third-largest contractor is not a data provider but rather a company that helps ICE make sense of that data.

In addition to co-opting information from the state government and private sector, ICE also reached into federal sources. Soon after its founding, ICE's Fugitive Operations Support Center began accessing information on Americans held in federal databases at the Department of State, the Department of Labor, and the Department of Housing and Urban Development, using that information to find people to detain and deport.[94]

As **Section IV** discusses, the agency even used interview data from unaccompanied children at the border to investigate people for deportation. Beginning in a trial in 2017 and then under a formal 2018 policy, ICE used the information given by unaccompanied minors as well as any guardians who stepped forward to take them under their care to find and arrest those guardians. ICE engaged in that practice under a Memorandum of Understanding with the Department of Health & Human Services Office of Refugee Resettlement, an agency charged by federal law with protecting the welfare of children who arrive unaccompanied at the border.[95]

D. BY PULLING IN DATA FROM EVERY SOURCE AVAILABLE TO IT, ICE'S SURVEILLANCE PROGRAMS HAVE CAST A DRAGNET OVER THE WHOLE U.S. POPULATION.

The massive scale of ICE's surveillance programs have turned the agency into a key component in what Anil Kalhan, professor at Drexel Kline School of Law, has called "the immigration surveillance state."[96] According to Kalhan, ICE surveillance has "transformed a regime of immigration control, operating primarily on noncitizens at the border, into part of a more expansive regime of migration and mobility surveillance, operating without geographic bounds upon citizens and noncitizens alike."[97] University of California Irvine professor Ana Muñiz recognized a similar shift within a specific immigration enforcement system, the Enforcement Integrated Database. She argues that increased data collection and data-sharing arrangements transformed the database from "a case management system to a mass surveillance system."[98]

While Congress has authorized ICE to exercise certain limited investigative powers,[99] Congress has never explicitly authorized the massive scale of its surveillance programs. Consider Secure Communities. As Kalhan noted in 2013, the Visa Reform Act directed federal agencies to ensure that databases are "readily and easily accessible" to federal immigration officials "responsible for determining an alien's admissibility . . . or deportability."[100] But Congress never explicitly authorized the "routine bulk transmission to DHS of all state and local identification records" involved in Secure Communities.[101] That's true of other ICE surveillance programs as well. Congress has never explicitly authorized ICE to routinely seek bulk records about the public from state agencies or private companies.

II. ICE LEVERAGES TRUST IN STATE DMVS TO CARRY OUT DEPORTATIONS AND EVADES THE FEW PROTECTIONS AGAINST THAT PRACTICE.

Gov. Jay Inslee signs Executive Order No. 17-01 in Olympia on February 23, 2017. (Photo: WA Governor's Office)

In January 2018, Jay Inslee had a crisis on his hands. He was a two-term Democratic governor of Washington with presidential ambitions, and the last thing he needed was an immigration scandal. But one had just arrived on his desk. According to a report published in The Seattle Times, the state's Department of Licensing had been regularly handing over Washington drivers' personal information—including their names, addresses and driver's license photos—to ICE agents investigating Washingtonians for deportation.[102]

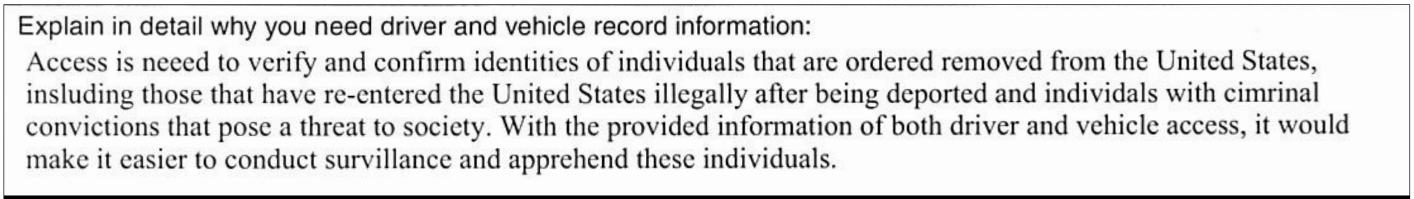
Inslee's office was caught off guard. The governor had tried to protect the privacy of immigrants in the state, asserting almost immediately after Trump took office that Washington would not be a "willing participant" in Trump's "mean-spirited policies that break up families."[103] In 2017, Inslee acted on this promise by signing an executive order prohibiting state agencies from cooperating with federal immigration authorities.[104] That included the Washington Department of Licensing, which promised its driver's license applicants that the state would be a safe place for immigrants to "live, work, drive, and thrive."[105]

But for 35-year-old Baltazar "Rosas" Aburto Gutierrez, and other immigrants like him, the agency didn't keep that promise.[106] According to the records uncovered by The Seattle Times, ICE agents had gone to the Department of Licensing for information on Gutierrez as they prepared to arrest the 15-year-long resident of Pacific County during his trip to the grocery store for coffee and eggs. They suspected that Gutierrez was undocumented in part because he had used a Mexican birth certificate to apply for his driver's license, which Washington State law has authorized since 1993.[107]

The revelation that ICE could access Washington's driver database sent shockwaves statewide. Inslee issued a personal apology, admitting that the state "fell short" in fulfilling

Aburto Gutierrez harvesting clams near Wallapa Bay off of the coast of Washington State. (Photo: Gladys Diaz) its commitment to protecting immigrants.[108] He also moved quickly to prevent something like that from happening again. Inslee immediately ordered Department of Licensing employees to stop sharing driver information with ICE absent a court order and ordered the department to conduct a full-scale internal review of its data-sharing practices.[109]

From the Department of Licensing's review came a first glimpse into the full extent of ICE's surveillance of Washington drivers. Results showed that the Department of Licensing had given ICE direct access to its electronic Driver and Plate Search (DAPS) database, which contained detailed records of drivers and vehicles registered in the state.[110] According to documents that the Center on Privacy & Technology uncovered, at least 28 ICE agents[111] had used DAPS to "to conduct surveillance and apprehend" immigrants living across Washington.[112] DAPS logs reveal that the ICE Enforcement and Removal Operations (ERO) division conducted more than 100,000 searches in the two-year period between Jan. 1, 2016, and Jan. 1, 2018.[113] Additional records the Center on Privacy & Technology uncovered and that The Washington Post reported on showed that, for purposes of immigration enforcement, ICE agents also requested face recognition searches of the state's driver's license photograph database.[114]



Explain in detail why you need driver and vehicle record information:

Access is neeed to verify and confirm identities of individuals that are ordered removed from the United States, insluding those that have re-entered the United States illegally after being deported and individuals with cimrinal convictions that pose a threat to society. With the provided information of both driver and vehicle access, it would make it easier to conduct survillance and apprehend these individuals.

Excerpt from a November 14, 2013 request sent by an ICE agent for direct access to Washington State's driver and license plate database. (Photo: Center on Privacy & Technology from FOIA documents)

By the time the results of the investigation went public, the Department of Licensing had decided to cut off ICE's access to the DAPS database.[115] The department no longer permitted face recognition searches on driver's license photographs for immigration enforcement purposes. Washington was assuring drivers that it had locked the door to the state's driver's license information. "We really want to make clear," Inslee's office told the press, "that we're not going to allow the federal government to commandeer the use of our state resources to use as part of their immigration effort."[116] Washington's message to all drivers was clear: We have your back.

Yet Inslee's attempts to sever ICE's access to driver's license records appear to have only encouraged the agency to turn toward a secretive side door.

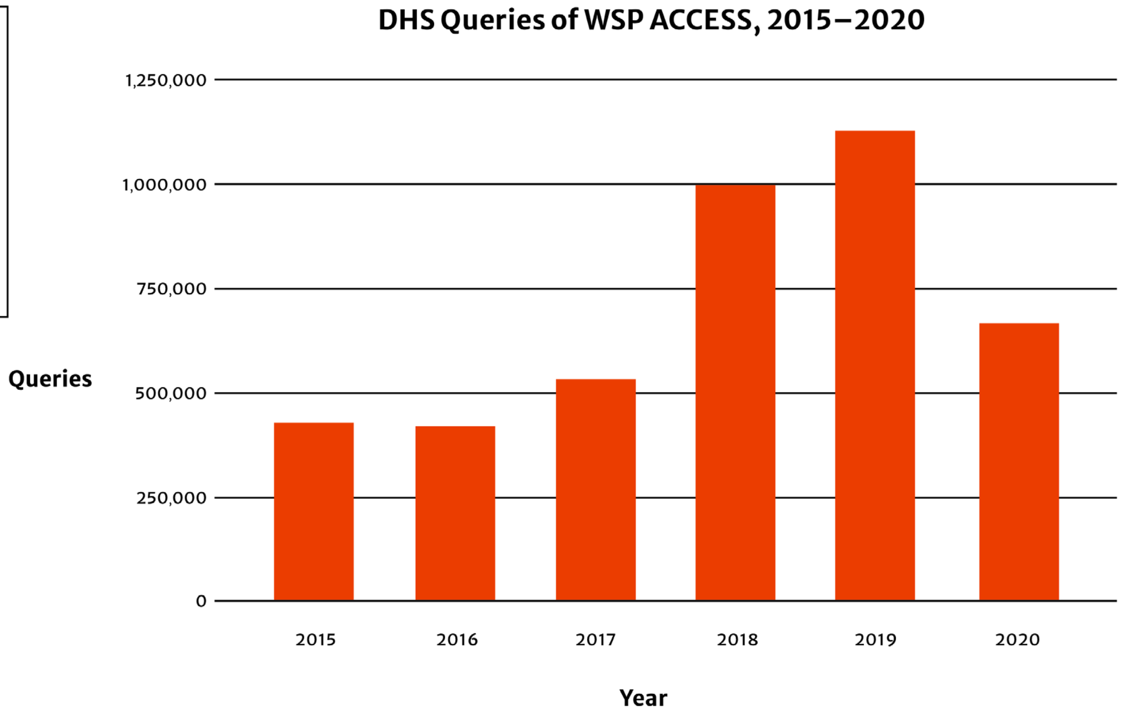
The governor's 2017 executive order had ended the Department of Licensing's "very liberal" policy for sharing driver's license photos, but as one employee explained to a CBP agent, there was another way. The Department of Licensing wasn't the only agency in the state that could grant access to drivers' records and license photos; the Washington State Police operated an electronic data-sharing system known as WSP ACCESS, and according to the employee, agents could use it to electronically query and receive the license photos of Washington drivers.[117]

Never-before-seen records from Washington suggest that DHS, ICE's parent agency, did not hesitate to take advantage of that alternative mode of accessing driver data. The number of queries for driver's license information that DHS sent through WSP ACCESS exploded in the years following the executive order. As **Figure 2** shows, from 2016 to 2019, the number of yearly searches from DHS rose from approximately 400,000 to a staggering 1.1 million.[118]

ICE has also prolifically used WSP ACCESS to access Washingtonians' driver data, sometimes with state employees' encouragement. As recently as October 2019, ICE agents requesting driver's license photographs for immigration enforcement purposes were advised by Department of Licensing employees that a driver's "image may be available to you in real time in WSP's ACCESS system through the driver query."[119] According to a Department of Licensing internal audit, never published publicly before, ICE submitted approximately 68,000 WSP ACCESS queries for driver's license information in 2019,[120] seeking driver's license photographs about one-third of the time.[121]

Figure 2.

Year	Queries
2015	398,710
2016	393,666
2017	539,638
2018	997,069
2019	1,129,711
2020	680,847



Despite Governor Inslee's best efforts, all signs suggest that ICE still has unrestricted, warrantless access to Washington drivers' data.

Alarmingly, despite the governor's best efforts, there is every indication that ICE still has unrestricted, warrantless access to Washington drivers' data. How is that possible? The answer lies in the multiplicity of intersecting access points through which states like Washington allow driver information to flow to outside agencies and the difficulty of severing those points of access. Despite the efforts states have taken to restrict ICE's access to driver's license data, ICE routinely finds ways to circumvent most state-imposed limits. When one spigot turns off, ICE simply moves to another pipeline.

This section identifies the different pipelines ICE uses to tap driver data, describes the scope and frequency of the agency's searches, and illustrates how a patchwork of federal and state laws (as well as ICE's willingness to secretly evade the few meaningful standards that do exist) have allowed ICE to weave driver data into its surveillance dragnet.

When one spigot turns off, ICE simply moves to another pipeline.

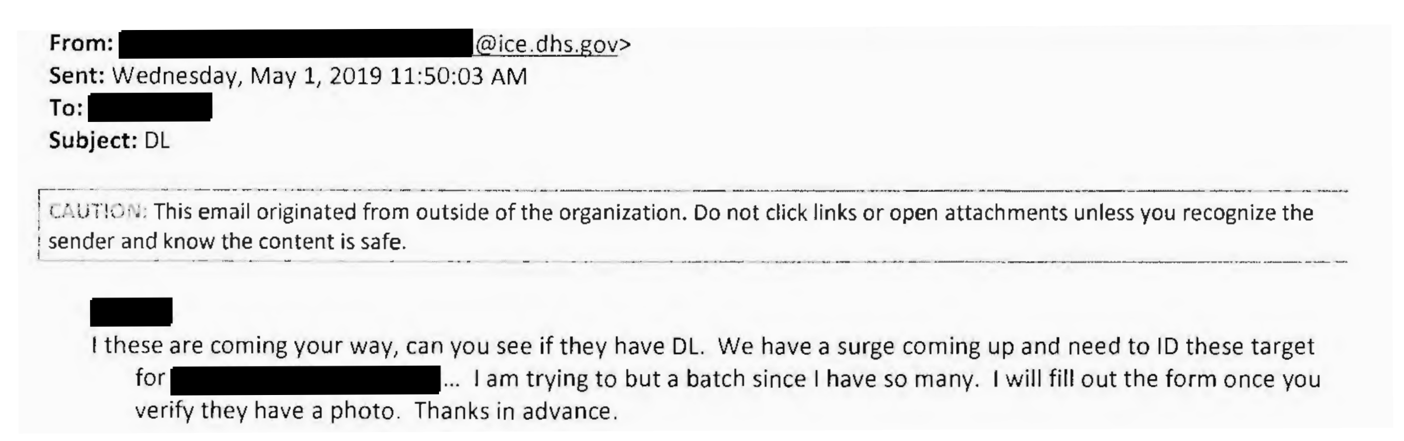
A. ICE USES AT LEAST THREE DIFFERENT PIPELINES TO ACCESS DRIVER DATA.

ICE investigators use a sprawling web of databases, networks and information-sharing initiatives to access states' driver records. On June 8, 2018, an ICE agent pursuing a case in Georgia wrote to an employee at the state's Department of Driver Services. "Can you assist me," the agent wrote, "with finding a specific person in GA?" The agent stated that they had the person's "cell [phone] number and the CLEAR results," referring to records pulled from a commercial database, and wanted to know if the person had a Georgia driver's license.[122] In a similar email sent to the department two weeks earlier, an ICE agent inquired whether a person had a driver's license, but only after the agent was "unable to verify [this information] in NLETS," a separate government system that ICE uses to access driver data.[123]

This set of communications reference the three major pipelines that ICE uses to obtain state driver's license information. First, ICE accesses driver's information by making **direct requests** to DMVs. ICE agents may contact DMV employees to ask for records and may also request employees to conduct face recognition searches. Second, ICE accesses drivers' information via **government databases**. ICE agents may directly search electronic databases of registered drivers and vehicles. Finally, ICE accesses drivers' information through **data brokers**. DMVs frequently sell driver's license data to private companies that resell access to ICE agents and others.

1. ICE agents directly ask state employees to search drivers' data and scan their faces, often in secret.

ICE agents often turn directly to DMV employees to request assistance with obtaining a person's driver's license information. Those requests frequently take place through long-standing relationships of active collaboration with state DMV employees, who are often eager to hand drivers' information over to immigration officials.[124] In Vermont, for example, one DMV employee was so cooperative in sharing information about possible targets that an ICE agent responded, "We're going to have to make you an honorary ICE officer!"[125]



From: [redacted]@ice.dhs.gov>
Sent: Wednesday, May 1, 2019 11:50:03 AM
To: [redacted]
Subject: DL

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

[redacted]

I these are coming your way, can you see if they have DL. We have a surge coming up and need to ID these target for [redacted]... I am trying to but a batch since I have so many. I will fill out the form once you verify they have a photo. Thanks in advance.

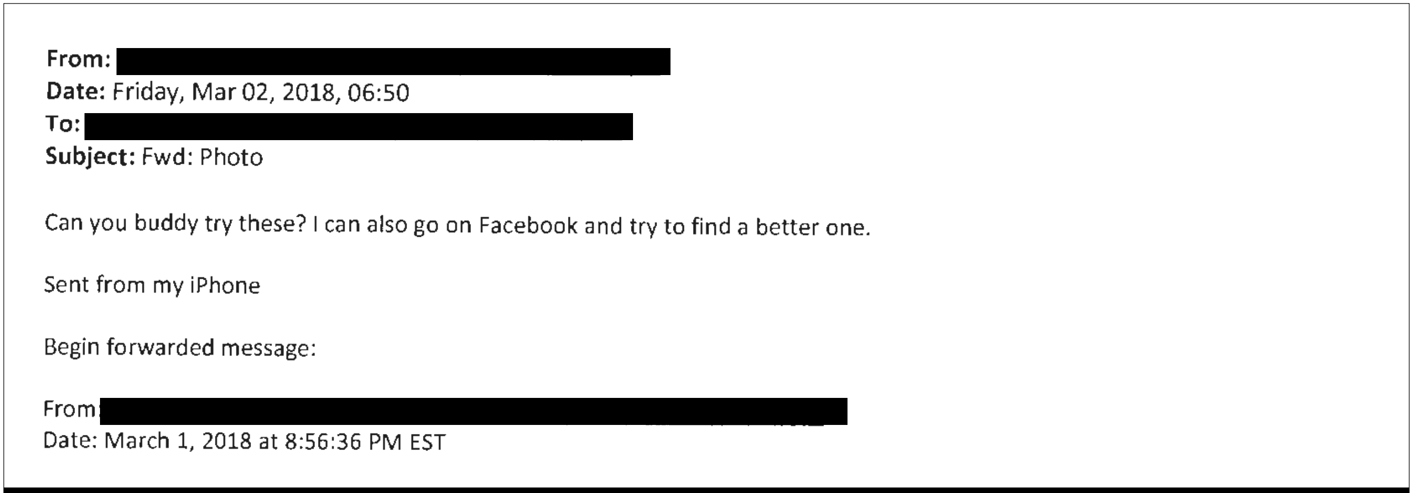
A May 1, 2019 email from an ICE agent to a Georgia licensing official. (Source: Center on Privacy & Technology FOIA documents)

Close working relationships between ICE agents and DMV employees enable ICE investigators to directly reach out to state employees asking for driver's license information. ICE's direct requests for driver's license information come in two main forms: requests for information associated with (1) a person's name, date of birth or other biographical information; and (2) a person's driver's license photograph, queried using face recognition technology.

a. Direct requests using biographical information

In cases where ICE agents have some basic information about a person of interest, like a name or a phone number, they may email DMV employees to assist with obtaining additional information from the person's driver records. A single state DMV may receive dozens of direct requests each year from ICE officials presenting a subject's name or other biographical information.[126]

While the total number of ICE's direct requests has largely been kept secret, evidence suggests that ICE makes hundreds or thousands of them each year to DMVs across the U.S. In advance of immigration raids planned for Atlanta, for instance, an ICE agent sent an email to Georgia's Department of Driver Services requesting a whole "batch" of driver's license information, including driver's license photographs, because there was "a surge coming up" and he had "so many" targets.[127] Similar records show an ICE agent sending a request to the Virginia DMV, seeking information about Virginians' driver's license application documents.[128] Those requests also reveal that ICE's searches have not been limited to people who are undocumented. In Arizona, an ICE agent emailed the Department of Transportation requesting driver's license information for a person with status under the DACA program.[129]



From: [redacted]
Date: Friday, Mar 02, 2018, 06:50
To: [redacted]
Subject: Fwd: Photo

Can you buddy try these? I can also go on Facebook and try to find a better one.

Sent from my iPhone

Begin forwarded message:

From [redacted]
Date: March 1, 2018 at 8:56:36 PM EST

A face recognition search request from an ICE agent to a Georgia licensing department employee.
(Source: Center on Privacy & Technology FOIA documents)

b. Direct requests for face recognition searches

When the only reliable information in ICE's possession about a person is a photograph, investigators may enlist state DMV officials' help in using face recognition technology to search for that individual among the state's database of driver's license photos.[130]

Records show that since 2015, ICE has requested face recognition scans of DMV databases in at least **14 states**. That includes the DMV databases of Alaska,[131] Arizona,[132] Colorado,[133] Florida,[134] Georgia,[135] Illinois,[136] Maryland,[137] Michigan,[138] Ohio,[139] Pennsylvania,[140] Utah,[141] Vermont,[142] Washington[143] and Wisconsin.[144] (As of the publication of this report, Colorado,[145] Illinois,[146] Maryland,[147] Utah,[148] Vermont[149] and Washington[150] have since prohibited DMV compliance with ICE face recognition requests for civil immigration enforcement purposes.) Furthermore, as described in **Section III**, ICE also held a contract with the Rhode Island DMV for access to its face recognition database.[151] Combined, this suggests that ICE agents and DMV officials acting on ICE's behalf have used face recognition technology to scan the faces of at least **83 million** drivers.[152] This includes about **1 in 3** adults in the U.S.[153]

Those searches easily constitute a dragnet. When ICE, and DMV officials on its behalf, use face recognition to search a state's license photograph database, everyone's image is being scanned by ICE, not just those of the person under investigation. In Wisconsin, one ICE agent conducting an identity fraud investigation requested a face recognition comparison against Wisconsin's database of **4.3 million** driver's license photographs.[154] In Georgia, another ICE agent repeatedly requested face recognition comparisons of an individual's photographs against Georgia's collection of **7.3 million** driver's license photographs.[155]

ICE's use of face recognition may result in misidentifications and false arrests. According to peer-reviewed research by scholars Joy Buolamwini, Timnit Gebru and others, face analysis algorithms often underperform when analyzing the faces of women, young people and people with darker skin tones.[156] Those bias problems extend to facial comparison systems and may worsen when state DMVs use antiquated face recognition systems—as is sometimes the case.[157]

There are few regulations limiting law enforcement's use of face recognition generally and almost no regulations addressing ICE's use of the technology. While courts have yet to rule on the constitutionality of face recognition in the law enforcement context, several scholars have raised concerns about its legality under various constitutional provisions, especially the First and Fourth Amendments, and it is unclear whether the practice is even legally authorized in the first place. Since at least May 2020, ICE policy has claimed to prohibit the use of face recognition technology by its ERO division for civil immigration enforcement purposes.[158] However, as a practical matter, there is no sharp line separating ICE ERO's enforcement of civil immigration law from the operations of ICE's Homeland Security Investigations (HSI) department, which is charged with investigating criminal activity. When ICE HSI conducts criminal investigations, its efforts routinely lead to "collateral arrests" of people who were not the original targets of the investigation.[159] As a result, even if those arrests constitute civil immigration enforcement, the investigations who led to them may be exempt from ICE's stated bar on face recognition.

ICE has shrouded its use of face recognition technology on state driver's photos in a level of secrecy more similar to what one would expect from a federal agency whose primary purpose is large-scale surveillance than from an agency that claims to be engaged in law enforcement. The FBI, one of the nation's most powerful law enforcement agencies, has disclosed the list of each state DMV it has relied on for face recognition searches.[160] It has also disclosed the memorandums of agreement underlying those efforts[161] and has for years publicized statistics about its use of its own face recognition system, the Next Generation Identification (NGI) Interstate Photo System (IPS), on a monthly basis.[162] Similarly, CBP has disclosed where each of its border face recognition systems has been deployed along with each of the photo databases it has relied on for face recognition searches, regularly publishing the number of face recognition searches it has conducted.[163]

ICE has shrouded its use of face recognition on state driver's photos in an abnormal level of secrecy.

By contrast, while ICE acknowledges that it routinely uses face recognition technology, it has never officially disclosed how often it does so or in which states, insisting that public comment about its use of the technology would threaten unspecified "law enforcement sensitivities."[164] As of this report's publication, ICE has still not disclosed any of those basic details. That is not to suggest that the FBI or CBP are sufficiently transparent but simply to point out that ICE's practices do not even rise to the level of the low bar its peer agencies have set.

2. ICE directly searches state DMV databases. In addition to contacting DMV officials directly for information, ICE also frequently queries state DMV databases for driver's license records. To do that, the agency relies on a service called the International Public Safety and Justice Network, more commonly known as Nlets.[165] Nlets, described as an "superhighway of information sharing" used by law enforcement agencies, has enabled ICE to electronically query and automatically retrieve driver's license information collected by participating state DMVs for over 20 years.[166] As of November 2020, ICE divisions representing all 50 states and the District of Columbia have obtained FBI-designated nine-digit Originating Agency Identification (ORI) Codes authorizing access to the Nlets system.[167]

According to a recently disclosed internal ICE memorandum, Nlets enables ICE agents to electronically query state driver's license databases for immigration enforcement purposes in 34 states.[168] Across those 34 jurisdictions, ICE may use Nlets to query the personal information of as many as **146 million** drivers.[169] This number is even higher when including the jurisdictions that enable ICE to query for non-immigration enforcement purposes. Using Nlets, ICE agents can electronically query state driver's license databases for non-immigration enforcement purposes in 39 states and the district.[170] Across those 40 jurisdictions, ICE may use Nlets to query the personal information of as many as **194 million** drivers, including approximately **3 in 4** adults.[171]

Public records obtained by the Center on Privacy & Technology through Freedom of Information requests reveal that ICE issues tens of thousands of driver's license and vehicle registration queries each month through Nlets. Records show that ICE issued **3,185** Nlets driver's license or Nlets vehicle registration queries over a **41-day** period in **Wisconsin** alone.[172] Other records show that ICE issued **223,814** Nlets driver's license queries between 2015 and 2020 in **Texas**.[173] Over the same five-year period, ICE issued **83,400** Nlets driver's license queries in **Iowa**.[174] Evidence suggests that those queries may concern a significant number of people. In **Washington** in 2019, ICE submitted **67,822** Nlets driver's license queries and retrieved records for **33,731** Washington drivers.[175] That's a rate of about one person for each pair of queries.

This partial picture of how ICE has used Nlets to reach into state driver records has only emerged by piecing together public court records with emails obtained by the Center on Privacy & Technology through Freedom of Information requests, as well as by consulting resources published by immigrant rights organizations like the NILC and Just Futures Law.[176] State and federal agencies have publicized very few details about how ICE uses Nlets to access DMV driver's license information, due to a combination of ICE's secrecy as well as state agencies' poor recordkeeping.

No agency can disclose details about ICE's searches for Maryland drivers' data. No agency claims responsibility for tracking that data.

At the state level, government officials have helped to preserve the secrecy of Nlets access records by essentially putting their heads in the sand. In Maryland, for example, no agency has been able to disclose details about ICE's Nlets queries of Marylander's drivers' data because no agency claims responsibility for tracking that data.

When the Maryland state legislature asked for information about ICE's use of Nlets to access drivers' records, the Maryland Department of Transportation (MDOT) said in a written testimony in January 2021 that it "does not control or monitor the access" of Nlets users.[177] Instead, MDOT suggested that separate branches of government held that information. It claimed that law enforcement access to Nlets is "certified by the Maryland State Police for state and local agencies and by the Federal Bureau of Investigations for federal agencies" and that Nlets queries "occur[] via the Department of Public Safety and Correctional Services."

> **"We simply make this information available . . . how the fields are used is a question for [the state police]."**

However, the Department of Public Safety and Correctional Services (DPSCS) denied that, claiming that it was "not the custodian of record for" records related to ICE's Nlets queries of Maryland driver's information. When the Center on Privacy & Technology sent the department a request for Nlets records, it instead forwarded the request to the Maryland State Police.[178] In response, the Maryland State Police just pointed back to DPSCS. A week after the DPSCS demurral, the Maryland State Police insisted that it "does not maintain anything related to" Nlets queries.[179] It claimed that Nlets queries are "logged at the state message switch housed by DPSCS," which "should be able to pull the logs."

This finger-pointing is common. In Iowa, employees at the Department of Transportation said that "we simply make this information available" to state police and "how the fields are used is a question for" them.[180] In Idaho, DMV officials said that the state police has oversight over the driver's license and registration information made available through Nlets and that the DMV was "not involved."[181] Yet, few state police departments have kept detailed records of ICE's Nlets requests for driver's personal information. Like the state police in Maryland, the Colorado Bureau of Investigation said that it does not record the number of queries received from ICE or other agencies for driver's license information.[182]

ICE, for its part, acknowledges that it "generally" retrieves state DMV driver's license information using the Nlets service,[183] but the full details surrounding DHS' use of Nlets to access DMV information have historically been a tightly kept secret. In 2020, the U.S. House of Representatives Homeland Security Committee launched a rare investigation into senior DHS officials for allegedly lying to Congress about the matter.[184]

3. ICE taps DMV records held by private data brokers.

ICE agents also use driver's license records sold by DMVs to private data brokers. ICE acknowledges that records obtained from those sources are often "incomplete, incorrect, or outdated" but claims that, with "the expenditure of additional time and effort," agents may be able to use them to uncover information such as a driver's home address.[185]

State DMVs frequently sell driver's license information to data brokers and other private entities, often generating millions of dollars in revenue in the process.[186] In Washington, for example, the Department of Licensing earned over $26 million in 2017 by selling driver's license and vehicle records to multiple data brokers, including LexisNexis.[187] While LexisNexis is a well-known legal research provider, it is also part of a vast information services enterprise that aggregates huge quantities of data and sells government agencies access to that data.[188] One of its subsidiaries, LexisNexis Risk Solutions, draws more than 10% of its $400 million annual revenue from sales of "data and advanced analytics" services to government and health care entities.[189]

Since March 2021, ICE has paid LexisNexis Risk Solutions $3.9 million to access driver's license information and other records to aid in the "in-depth exploration of persons of interest and vehicles."[190] The terms of ICE's contract with LexisNexis remain confidential, although LexisNexis has acknowledged in purchase agreements with DMVs that it sells its driver's license and vehicle registration records to homeland security and law enforcement customers.[191] As of this report's publication, more than 11,000 ICE agents may be able to conduct investigations by querying the LexisNexis Risk Solutions service.[192]

Evidence indicates that ICE has purchased access to DMV driver's license information through LexisNexis Risk Solutions. Records show that LexisNexis has purchased driver's license information directly from DMVs in **12 states** and the district: Arizona,[193] California,[194] the District of Columbia,[195] Florida,[196] Illinois,[197] Minnesota,[198] Nebraska,[199] Nevada,[200] North Carolina,[201] Oregon,[202] South Carolina,[203] Tennessee[204] and Wisconsin.[205] In total, this indicates that ICE may access driver's license information purchased by LexisNexis for **88 million** drivers, including **1 in 3** adults.[206]

ICE and LexisNexis have sought to keep the public in the dark about the terms of their relationship. For example, ICE withheld an overview of its March 2021 contract with LexisNexis Risk Solutions, claiming that it was "law enforcement sensitive and not for public release."[207] LexisNexis Risk Solutions has been more forthcoming about its agreements with the FBI, issuing a press release announcing the contract that gave the FBI access to its Accurint Virtual Crime Center service.[208] The FBI itself publicly disclosed that it uses LexisNexis Risk Services to access residence information, among other data as well.[209] As of this report's publication, however, ICE and LexisNexis have never disclosed those basic details about services rendered under their contract.

B. FEDERAL AND STATE LAWS HAVE PROVED INSUFFICIENT AGAINST ICE SEARCHES—AND EVASION.

State DMVs frequently promise strong state and federal protections for drivers' personal privacy,[210] but this report illustrates that ICE has been able to obtain wide-ranging access to driver's record information despite legal protections. That is because ICE takes advantage of weaknesses in federal and state driver privacy laws, which often still enable the agency to obtain driver information through one or more of its three main pipelines of access.

1. The federal DPPA of 1994 did not anticipate use of driver data by federal immigration enforcement.

DPPA, a federal law regulating state DMVs' sharing of driver's record information, passed through Congress in 1994. In the words of then-Senator Joe Biden, one of the major proponents of the DPPA at the time, this legislation was intended to thwart stalkers and harassers by protecting the "privacy [of] addresses and telephone numbers" provided to the DMV.[211] But neither the senator nor other members of Congress considered whether the law should protect Americans from privacy invasions at the hands of federal immigration enforcement. At the time, immigration enforcement operations were comparatively rare, and Congress likely did not foresee the problems that might arise if that changed.[212] The DPPA expressly allows state DMVs to share driver's information with government agencies as well as private data brokers who make it available to government agencies.[213]

ICE has operated within that blindspot in federal law to gain access to Americans' driver's license information. Without meaningful federal privacy protections that regulate how DMVs share driver data with government agencies and private companies, ICE has been able to persistently search driver's license information, even in states that have allowed and encouraged immigrants to apply for driver's licenses.

2. Most state laws protecting driver data have proved insufficient. ICE has evaded several of the few laws offering meaningful protection.

In the absence of strong federal regulations around ICE's access to driver data, many state and local lawmakers have enacted executive orders, agency policies, statutes and ordinances to resist ICE's expansion of surveillance capacities. But ICE has circumvented even the strongest policies that states have enacted to safeguard their drivers' information.

Oregon has one of the strongest driver privacy laws to protect driver information from ICE access. In 2017, at the urging of Governor Kate Brown, the legislature passed a law prohibiting the dissemination of address information and other data by government agencies for civil immigration enforcement purposes.[214] At first, the legislation seemed to work; after the law was passed, ICE requests for Oregon drivers' information fell off a cliff. Oregon DMV records that the Center on Privacy & Technology obtained show that the number of direct requests from ICE for driver's address information declined from 35 requests in 2015 and 40 requests in 2016 to three requests in 2018 and zero requests in 2019.[215] The spigot on direct requests for DMV information had been turned off. Only in August 2019, after that steep decline in ICE's direct requests, did Oregon pass H.B. 2015, the Equal Access to Roads Act, to expand driver's license eligibility to people without documentation.[216]

Just six months later, the Oregon DMV signed agreements to sell its driver's license records to the data brokers Thomson Reuters and LexisNexis Risk Solutions, granting the companies permission to disseminate it to "government agenc[ies] for use in carrying out [their] governmental functions."[217] Whether the Oregon DMV realized it or not and regardless of whether earlier contracts predated the law, the DMV appeared to be allowing immigrant drivers' information to end up in ICE's hands, despite the state's strong laws intended to prevent just that.

Across the country, immigrant communities have pressed policymakers to pass laws to

Governor Kate Brown announces a February 2, 2017 executive order to protect immigrants in the state. (Photo: Gordon Friedman/Oregon Live)

prevent this kind of abuse, and thanks to their organizing and advocacy, multiple states have tried to enact legislation to prevent ICE from warrantlessly accessing driver information. After Marylanders discovered multiple pathways of ICE access to its driver's license information, the immigrant rights group CASA led a campaign to pass the Maryland Driver Privacy Act, prohibiting any access to Maryland's driver's license information for immigration enforcement purposes.[218] The law passed in April 2021, and although the governor vetoed it a month later, the Maryland General Assembly overrode the veto in December and the law will go into effect in 2022.[219] Similar laws have passed in other states. When Californians discovered that the agency was using a state system to view driver's license information, the state passed AB 1747, prohibiting ICE access to the system for civil immigration enforcement purposes.[220] After Utahns learned about ICE using face recognition technology to scan their license photos, Utah passed S.B. 34, prohibiting the use of face recognition technology on government databases for civil immigration enforcement purposes.[221]

But these laws often fail to block all three of the above described pipelines for ICE access for driver information or come up short in other ways. In the words of San Diego Assemblywoman Lorena Gonzalez, "Every time we create a law in California, ICE figures out a way to get around [it]."[222]

a. State Driver Privacy Protection Scorecard

The Center on Privacy & Technology has conducted an analysis of driver privacy laws and policies in each of the 16 states that offer undocumented immigrants the ability to apply for a driver's license or its equivalent, along with the district, which has the same policy. We evaluated the strength of each jurisdiction's regulations on ICE access to driver's information through its three main pipelines of access, assigning each jurisdiction a rating according to the following criteria. A jurisdiction received:

- a **green** score when it prohibits dissemination of driver data to ICE without a warrant, access to driver data by ICE without a warrant, or when no such data is available for access or dissemination in the state;
- a **yellow** score when it prohibits access by or dissemination of driver data to ICE for civil immigration enforcement purposes; and
- a **red** score when no such protections appeared to apply to the access by or dissemination of driver data to ICE for civil immigration enforcement purposes.

We also rated jurisdictions along the same criteria based on whether they adopted protections against warrantless ICE face recognition searches.

The scorecard seen at **Figure 3** shows a clear pattern emerging. Our review found that among the 17 jurisdictions, six have no meaningful restrictions on direct request pipelines,[223] seven have no meaningful restrictions on government database pipelines,[224] and seven have no meaningful limits on data broker pipelines.[225] Five states have no meaningful restrictions on face recognition searches.[226] When state restrictions on certain pipelines for drivers' data do exist, they may accomplish little if laws allow ICE agents to access that information through other pipelines.

State laws to protect driver privacy often fail to protect against all three pipelines for ICE access.

Several states have adopted weak protections that do not require ICE to have a warrant to request driver's personal information if the request is predicated on a criminal investigation. Our review found that among the seventeen jurisdictions that grant driver's license eligibility to people without documentation, six states have weak restrictions on direct request pipelines;[227] seven states have weak restrictions on government database pipelines;[228] and six states have weak limits on data broker pipelines.[229] Five states and the district have weak restrictions on face recognition searches.[230] Without a warrant requirement, a criminal investigation predicate is little more than a parchment barrier between ICE and a driver's personal information.

State driver privacy protection laws typically contain one or more significant weaknesses. Typically, weak laws only limit the disclosure of driver's license information:

Figure 3.

STATE DRIVER PRIVACY PROTECTION SCORECARD

JURISDICTION	DIRECT REQUESTS	GOVERNMENT DATABASES	FACE SCANS	DATA BROKERS
CALIFORNIA	🟨	🟨	🟩	🟨
COLORADO	🟨	🟨	🟨	🟥
CONNECTICUT	🟥	🟥	🟥	🟨
DELAWARE	🟥	🟥	🟥	🟨
HAWAII	🟩	🟥	🟥	🟥
ILLINOIS	🟥	🟥	🟨	🟥
MARYLAND	🟩	🟩	🟩	🟩
NEW JERSEY	🟨	🟨	🟨	🟥
NEW MEXICO	🟥	🟥	🟥	🟩
NEW YORK	🟩	🟩	🟩	🟩
NEVADA	🟥	🟥	🟥	🟥
OREGON	🟨	🟨	🟩	🟨
UTAH	🟥	🟥	🟨	🟥
VERMONT	🟨	🟨	🟩	🟩
VIRGINIA	🟨	🟨	🟨	🟨
WASHINGTON	🟩	🟨	🟩	🟨
DISTRICT OF COLUMBIA	🟩	🟩	🟨	🟥

	🟩 WARRANT REQUIRED	🟨 NON-IMMIGRATION OK	🟥 IMMIGRATION OK
DIRECT REQUESTS	Dissemination to ICE prohibited without a warrant.	Dissemination to ICE for civil immigration enforcement purposes is prohibited (no warrant requirement for non-immigration).	Dissemination to ICE for civil immigration enforcement purposes is permitted.
GOVERNMENT DATABASES	Access by ICE is prohibited without a warrant.	Access by ICE for civil immigration enforcement purposes is prohibited (no warrant requirement for non-non-immigration).	Access by ICE for civil immigration enforcement purposes is permitted.
FACE SCANS	Warrant is required or jurisdiction does not use face recognition technology.	Direct access, or searches on behalf of ICE, for civil immigration enforcement purposes is prohibited.	Direct access, or searches on behalf of ICE, for civil immigration enforcement purposes is permitted.

	🟩 NO ICE SALES	🟨 NON-IMMIGRATION OK	🟥 IMMIGRATION OK
DATA BROKERS	Resale to ICE prohibited or jurisdiction does not sell to data brokers.	Resale to ICE for civil immigration enforcement purposes is prohibited.	Resale to ICE for civil immigration enforcement purposes is permitted.

- by the licensing agency, without a general prohibition on disclosures of the underlying data. Privacy protections that only apply to the licensing agency allow federal immigration enforcement to leverage other state employees to access and disseminate driver data.

- to certain recipients, without a general prohibition on disseminations intended for immigration enforcement purposes. Dissemination restrictions that only apply to specific recipient agencies allow federal immigration enforcement to leverage other federal employees to access and disseminate driver data.

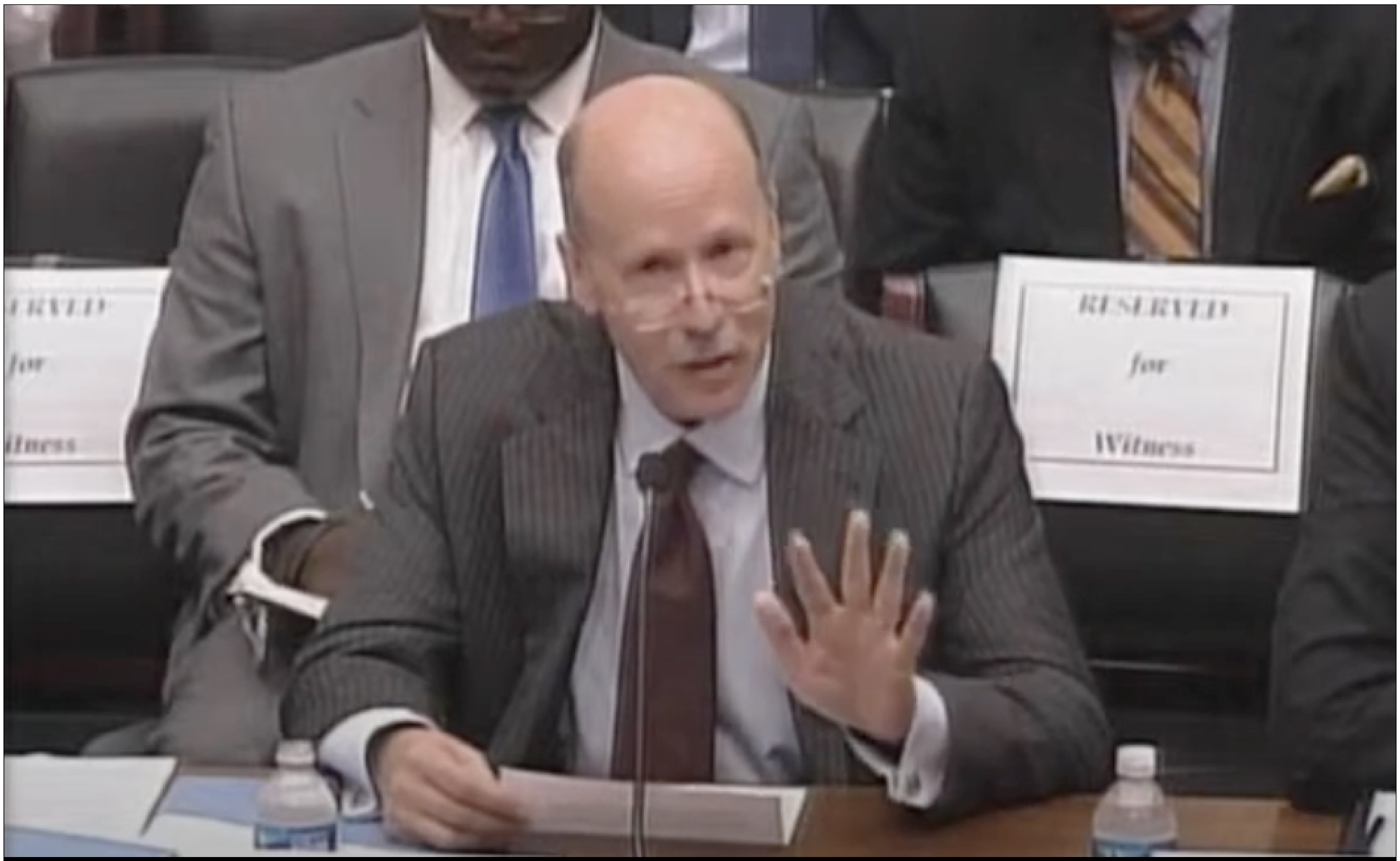
- when biographical information is directly requested by a federal immigration agent, without prohibitions on indirect access or biometrics. Privacy protections that only apply to direct requests for biographical data allow federal immigration enforcement to access driver's license information using electronic databases and face recognition searches.

- for civil immigration enforcement purposes, without prohibitions on dissemination for investigation of punishable immigration offenses. Privacy protections that only apply to requests for civil immigration enforcement purposes allow federal immigration enforcement to access driver information to engage in enforcement activities related to punishable immigration violations, such as the two federal border crossing offenses.

- unless it's requested by law enforcement. Privacy protections that contain overbroad law enforcement exceptions allow ICE to leverage local, state and federal law enforcement to access and disseminate driver data.

Based on our review, two states have enacted robust privacy protections for driver's license information. Maryland's Driver Privacy Act blocks warrantless sharing of data with "any federal agency" seeking access for the purpose of "enforcing federal immigration law."[231] New York's Driver's License Access and Privacy Act ("Green Light Law") paired its expansion of driver's license eligibility with a categorical prohibition on the DMV disclosing or making accessible "in any manner" driver's license records or information to federal immigration enforcement.[232] The passage of Green Light was the result of a multiyear campaign by a broad cross-sectoral coalition led by immigrant rights and workers rights groups from all across the state. One key consequence of New York's law was that state police started to cut off ICE access to driver's license information using Nlets. (The New York State Police prohibited ICE's FBI-designated ORI Codes from querying New York's driver's license information.[233]) Another key consequence was that the New York DMV began to prohibit buyers of the DMV's driver's license information from disseminating it to ICE.[234] With those protections, New York State has successfully protected its driver's license information from ICE surveillance and overreach.

III. ICE EXPLOITS PEOPLE'S BASIC NEEDS FOR HEAT, ELECTRICITY AND WATER BY COLLECTING UTILITY RECORDS THROUGH OPAQUE AND UNREGULATED DATA BROKERS.



Stuart Pratt, then-CEO of the Consumer Data Industry Association, testifies before the House Subcommittee on September 10, 2014. (Photo: House Financial Services Committee)

In 2014, the House Subcommittee on Financial Institutions and Consumer Credit held a hearing to discuss a bill aimed at expanding credit access for millions of Americans. According to Representative Keith Ellison of Minnesota, there were at least 50 million consumers in the country whose credit histories were too thin to generate high scores and another 50 million who were "credit invisible," meaning that they had no credit scores at all.[235]

"The solution is simple," Ellison told the committee.[236] Instead of needing credit to build credit, consumers could establish a record through something that many people already pay on a regular basis: their utility bill. The Credit Access and Inclusion Act would give the green light for gas, water, electric and other utility providers to notify credit bureaus each time a customer pays—or misses—a monthly bill, not just when an account is sent to collections.[237]

The idea behind using utility payments to show creditworthiness wasn't entirely new, and one major credit reporting agency, Equifax, was already collecting the "full-file" utility payment records of millions of customers for use in specialized credit reports delivered specifically to utility companies.[238] But the law was still unclear on whether full utility payment data could be factored into a consumer's credit score, and Ellison wanted to put an official rubber stamp on the practice. Approval from Congress, he hoped, would go a long way in helping low-credit and no-credit Americans break into the mainstream financial system.[239]

Among all the witnesses present at the hearing, none spoke as eagerly about the bill's potential to improve the lives of the underprivileged as Stuart Pratt. Pratt was the president and CEO of a trade group called the Consumer Data Industry Association (CDIA), whose members included the nation's big three credit reporting agencies: Equifax, Experian and TransUnion. "Ultimately," Pratt insisted before the committee, when credit bureaus can include full utility payment data in credit reports, "consumers who are new immigrants, unbanked and underbanked, are the beneficiaries."[240]

" . . . consumers who are new immigrants, unbanked and underbanked, are the beneficiaries."

Just one legislator voiced concerns about whether this trove of information might end up in the wrong hands. "I guess maybe I would ask the panel," said Vice Chairman Sean Duffy, "what steps are taken to protect the millions of bits of information that are collected in regard to people's credit history and personal information?"[241] As the industry representative, Pratt assured him that the companies in CDIA had security teams and could monitor whether credit reports were unexpectedly accessed, for example, by a Russian IP address.[242]

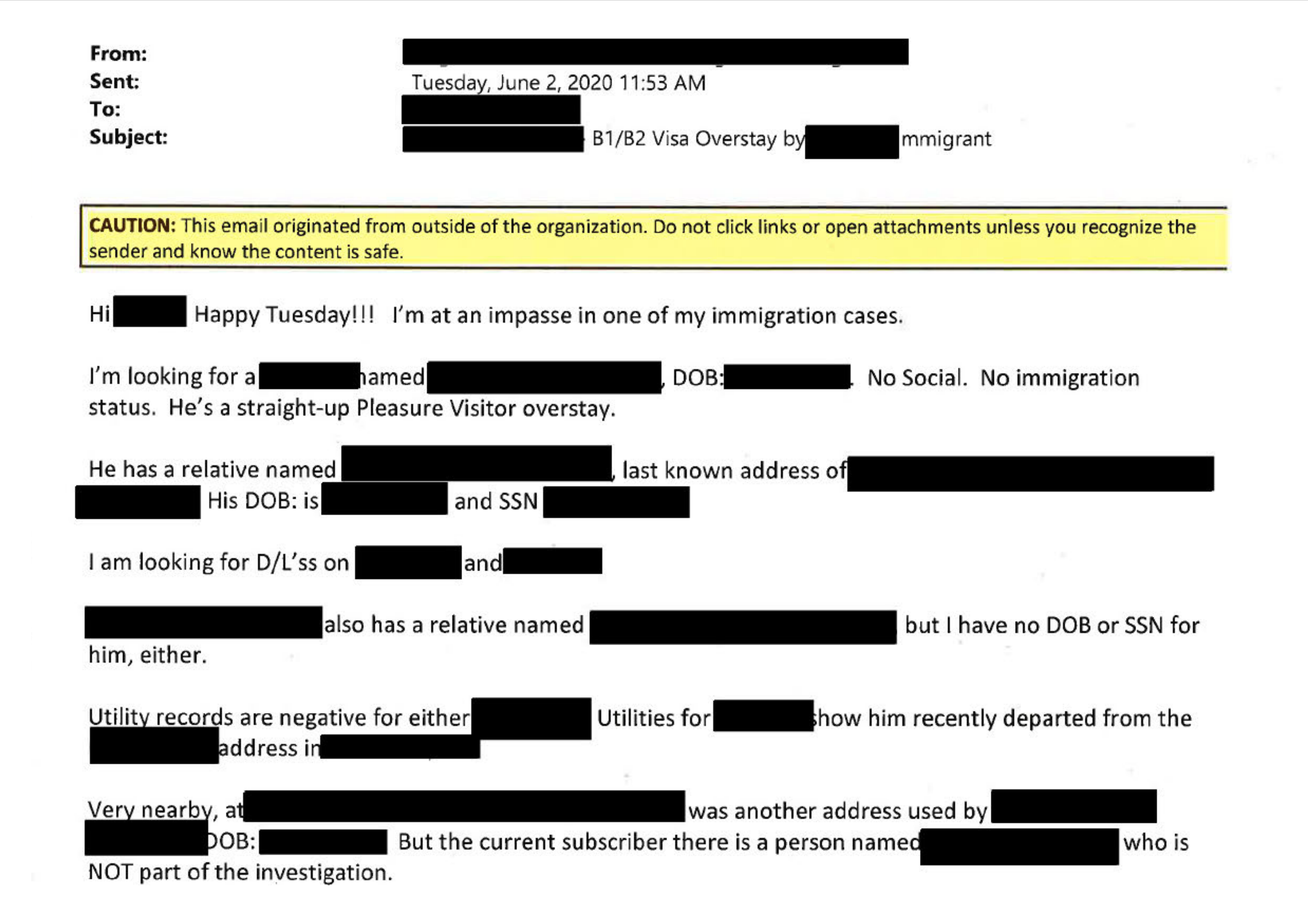
But Pratt failed to mention that Equifax, one of the largest members of his trade association, was packaging up the customer information that it received from utility companies and furnishing it to a private database used by ICE.

Seven years later, in February 2021, Reps. Raja Krishnamoorthi of Illinois and Jimmy Gomez of California demanded answers from Equifax and the data broker Thomson Reuters about the practice, expressing their concern that sharing utility customers' data with ICE represents "an abuse of privacy" and that ICE's use of this information constitutes "an abuse of power."[243]

A. ICE EXPLOITS THE NEED FOR WATER, LIGHT, HEAT, PHONE AND INTERNET TO TARGET PEOPLE FOR DEPORTATION.

On June 2, 2020, an ICE agent emailed a Georgia licensing official seeking assistance. "Happy Tuesday!!!" he wrote. "I'm at an impasse in one of my immigration cases."[244] The agent needed help tracking someone down. He had pulled the person's utility records, which revealed that the subject had "recently departed" from an address.[245] The agent took that information to the licensing department, hoping that driver records could tell him more.

Three months earlier, in the first days of COVID-19 lockdowns in the U.S., the acting head of ICE had announced that the agency would temporarily scale down arrests, with the exception of those deemed "mission critical" to "maintain public safety and national security."[246] But the agent who emailed the Georgia licensing department wasn't pulling utilities records to find someone who fit within ICE's newly defined priorities for enforcement. Rather, the agent had tapped a database containing millions of customers' water, electricity, gas, phone and other utility records in search of someone who had simply entered the country on a visa and remained longer than authorized—a "straight-up Pleasure Visitor overstay."[247]



From: [redacted]
Sent: Tuesday, June 2, 2020 11:53 AM
To: [redacted]
Subject: [redacted] B1/B2 Visa Overstay by [redacted]mmigrant

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hi [redacted] Happy Tuesday!!! I'm at an impasse in one of my immigration cases.

I'm looking for a [redacted]amed [redacted], DOB:[redacted]. No Social. No immigration status. He's a straight-up Pleasure Visitor overstay.

He has a relative named [redacted], last known address of [redacted] His DOB: is [redacted] and SSN [redacted]

I am looking for D/L'ss on [redacted] and [redacted]

[redacted] also has a relative named [redacted] but I have no DOB or SSN for him, either.

Utility records are negative for either [redacted] Utilities for [redacted]how him recently departed from the [redacted]address i[redacted]

Very nearby, at [redacted] was another address used by [redacted]OB: [redacted] But the current subscriber there is a person name[redacted] who is NOT part of the investigation.

A June 2, 2020 email from an ICE deportation officer to a Georgia licensing official.
(Source: Center on Privacy & Technology Freedom of Information documents)

For years, it has been known that ICE used a commercial database to gain access to millions of names, addresses and other personal information taken from their utility records.[248] What remained unknown, however, were the details: How exactly did utility customer data end up in a private database used by immigration agents? And precisely which utility companies allowed their customers' information to reach ICE?

By piecing together public marketing documents and DOJ filings, the Center on Privacy & Technology was able to identify the likely longtime source of ICE's utility information: a little-known credit reporting agency known as the National Consumer and Telecom Utilities Exchange (NCTUE). With access to customer data from NCTUE's several dozen member utility and telecommunication companies, ICE agents could likely view the utility record information of over **218 million** unique consumers, including about **3 in 4** adults in the U.S.[249]

ICE investigators gained the ability to dig through people's gas, water, electricity, phone, internet and other utility records when, in 2010, the agency penned a contract with Thomson Reuters for subscription access to a database called CLEAR.[250] CLEAR, designed to be a one-stop shop for investigators to gather information about their targets, vacuums up the data trails that individuals leave in the course of their daily lives.[251] The database pulls names and Social Security numbers from the top of consumer credit reports; matches license plate numbers from DMV records with snapshots taken at toll roads and parking lots; and—for the most up-to-date information on where people live—gathers the addresses listed on their gas, water, electricity and other utility bills.

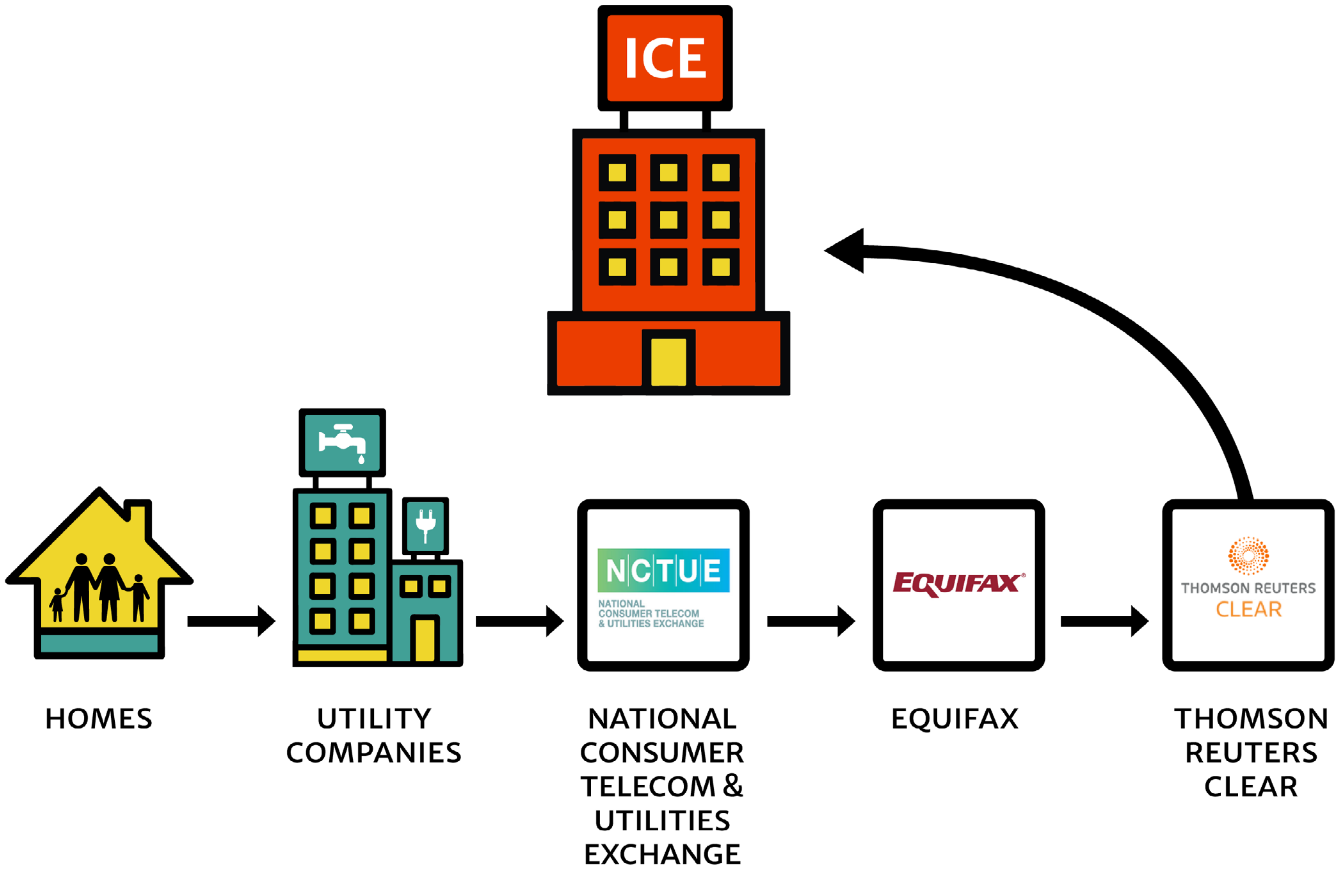
"For people who are not easily traceable via traditional sources . . . utility hookup records may provide the only current and accurate address and phone number data available."

In a marketing letter sent to potential subscribers, Thomson Reuters specifically emphasizes that utility records are uniquely valuable in shining a light on populations that are difficult to track through other means. "For people who are not easily traceable via traditional sources" such as credit reports, the letter reads that "locator information from utility hookup records may provide the only current and accurate address and phone number data available."[252] Thomson Reuters has taken care to ensure that its collection of utility records is extensive and up-to-date, boasting in the letter that "CLEAR offers the most comprehensive utility locator information on the market."[253]

In the letter, Thomson Reuters also reveals that Equifax is the supplier of CLEAR's utility dataset.[254] Equifax hosts a database containing millions of utility customers' payment records on behalf of NCTUE. This arrangement began in 1993, when a band of eight telecommunication carriers went to the DOJ to review its plan to build a "credit information clearinghouse,"[255] a central database where each company could share customers' account information and payment records with each other. (Absent such review, there would have been uncertainty about the outcome of possible antitrust scrutiny.)[256] The group selected Equifax to build and manage the database,[257] and in turn, Equifax negotiated the exclusive right to package the data and deliver it to downstream buyers.[258]

The purpose of the customer database was twofold. When the telecommunications companies first proposed their clearinghouse to the DOJ, they claimed that its "principal purpose" was "to provide carriers with advance warning about customers who pose a credit risk."[259] A potential customer with a history of leaving balances unpaid, for example, might be asked to pay a larger deposit. But the carriers also planned for this pool of records to serve as a "skip tracing" tool—a way to track down customers who left unpaid bills behind.[260] Customers may terminate services or move away, but anytime they signed

Figure 4. Likely Path of Utility Customer Data to ICE, 2010-2021


ICE
NCTUE
NATIONAL CONSUMER TELECOM & UTILITIES EXCHANGE
EQUIFAX
THOMSON REUTERS CLEAR
HOMES
UTILITY COMPANIES
NATIONAL CONSUMER TELECOM & UTILITIES EXCHANGE
EQUIFAX
THOMSON REUTERS CLEAR

up with another utility provider in the group, the clearinghouse would update with the new addresses and contact information listed on their applications.

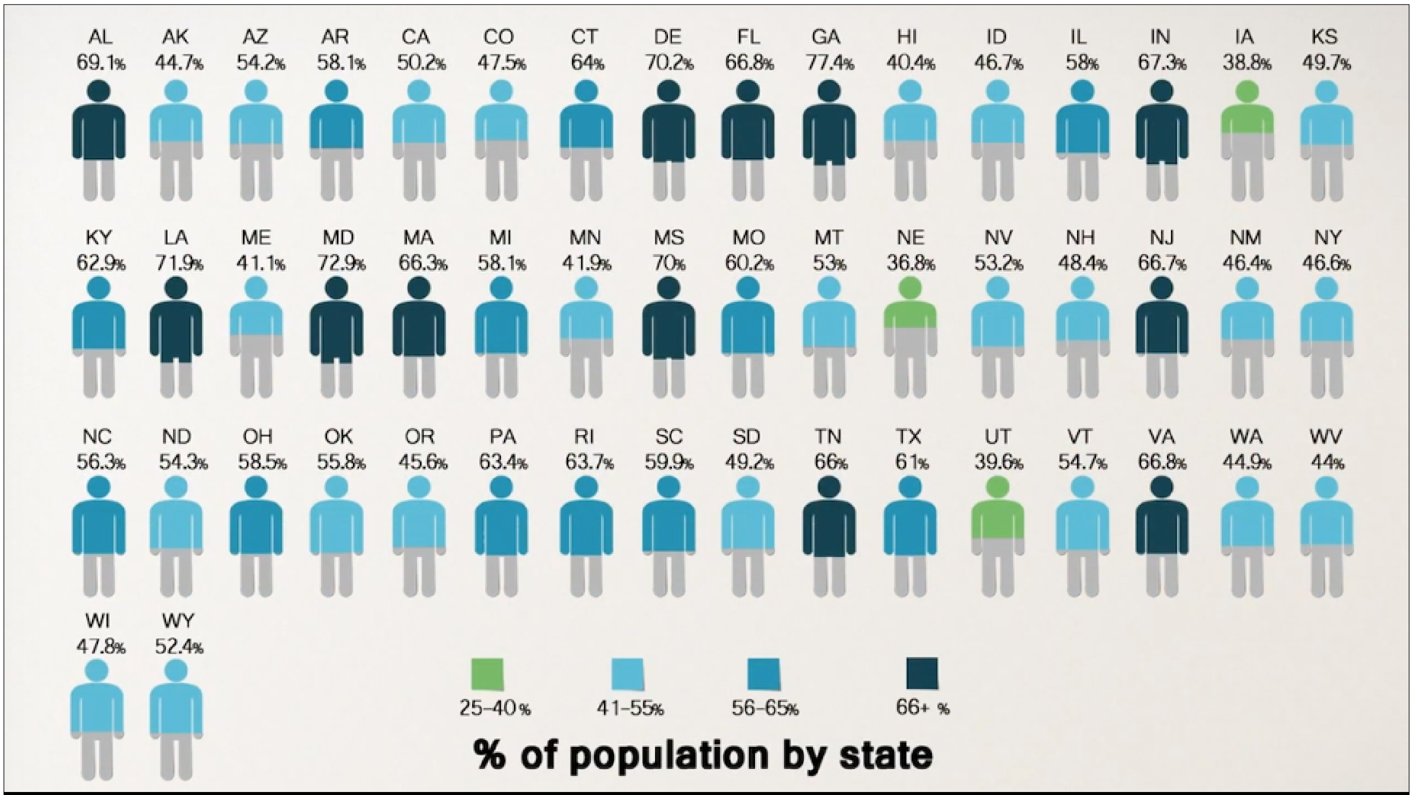
To make it even easier to trace old customers to new addresses, the initial group of telecommunications carriers decided to invite gas, water and electric providers to contribute their customers' records as well. According to another filing that the telecoms wrote to the DOJ in 2002, "the services provided by utilities companies are tied to physical location," which means that they "tend to have accurate address information."[261] With the addition of 37 utility companies contributing customer information, the group became known as NCTUE.[262] The NCTUE database became not only a useful tool for credit evaluation but also one of the most reliable sources of information on where people live.

When ICE agents used CLEAR to access millions of names and addresses from utility records, they were most likely viewing customer data that NCTUE's member companies handed over to Equifax. Such an extensive collection of utility record data was unlikely to come from any other source, as the NCTUE database is reportedly "by far the largest database of utility, pay TV, and telecom payment records" in the nation.[263] Equifax has also actively touted the NCTUE database's effectiveness in capturing "that elusive segment of the market—the no-hit or thin-files,"[264] who would likely be absent from the credit header data that Thomson Reuters gets from other credit agencies like Experian and TransUnion.

While no entity involved in supplying Thomson Reuters with utility records has confirmed their exact provenance, the dataset that Equifax manages for NCTUE and the dataset it handed over to CLEAR are near identical in number: CLEAR claims to hold over 400 million names and addresses obtained from more than 80 utility providers,[265] and Equifax reveals that the NCTUE database contains over 400 million records from more than 85 companies.[266]

Equifax and NCTUE have remained secretive about the full list of utility companies whose customers' records have ended up in the NCTUE database—and therefore likely in the hands of ICE—but evidence indicates that it has included national giants like Verizon[267] and AT&T[268] as well as regional utilities like Baltimore Gas & Electric[269] and Piedmont Natural Gas.[270] Evidence also suggests that even some publicly held service providers like Nevada Energy[271] and the Miami-Dade County Water and Sewer Department[272] have participated in the data exchange. Additional service providers that may have been part of NCTUE are listed in the **Appendix**.

ICE's broad access to utility data impacts millions of customers from dozens of utility providers across the U.S. The CLEAR utility dataset is drawn from national and regional telephone, cable, satellite, gas and electric and water providers across the country, including a special "focus on the top 50 companies."[273] The dataset encapsulates utility customers in all 50 states and the district, as well as Puerto Rico, Guam and the U.S. Virgin Islands, and it is updated daily.[274]



NCTUE coverage by state. (Source: Equifax)

Despite supplying the personal information of millions of utility customers to a database used by immigration enforcement, Equifax continues to uphold a public narrative of service to the most underprivileged consumers. In a promotional video posted by Equifax, a director for Verizon proclaims that the NCTUE data exchange is "very empowering"[275] for "underserved, underbanked, multicultural"[276] customers. An Equifax executive also claimed that the information exchange "present[s] a tremendous opportunity for the underbanked or credit invisible."[277]

> **A Verizon employee calls the NCTUE "very empowering" for "underserved, underbanked, multicultural" customers.**

SIDEBAR 2.
THE EARLY RELEASE OF OUR NCTUE FINDINGS

The Center on Privacy & Technology typically releases its research findings in conjunction with research reports. When we uncovered the likely data pipeline between the NCTUE and ICE, we decided that the information was too important to wait for our report's release. We provided the documents to Drew Harwell of The Washington Post, which published them in a front-page February 2021 exposé.[278] None of the companies involved denied that the data of NCTUE members' customers was being provided to ICE.

ICE's agreement with Thomson Reuters for access to the CLEAR database ended in February 2021. That same month, however, ICE appeared to replace its subscription to CLEAR by awarding a $16.8 million contract to LexisNexis Special Services, possibly for access to a similar database called Accurint.[279] Although it is unknown whether this contract offers ICE access to utility records from the NCTUE database, LexisNexis has advertised that its datasets include utility records of 210 million consumers—around the same amount as the NCTUE database claims to hold—derived from unspecified sources.[280]

In October 2021, NCTUE instructed Equifax to end the sale of names, addresses and other biographical data from customer records.[281] This was the result of action by Senator Ron Wyden of Oregon, who, after the release of our findings in The Washington Post in February and persistent advocacy by Just Futures Law and Mijente in subsequent months, pushed NCTUE to cease the sale of this information.[282] According to a statement issued by Thomson Reuters to customers of its databases, including CLEAR, utility header data is no longer being provided for law enforcement or non-law enforcement entities such as private investigators.[283]

However, although NCTUE agreed to end the sale of utility customer data, it is still just one out of many possible sources for this information. Without strong regulations to limit the dissemination of utility data, it may be only a matter of time before data brokers discover new avenues for amassing the same set of customer records. And although ICE has ended its contract with Thomson Reuters, its new agreement with LexisNexis reveals that multiple different companies can provide very similar services. When ICE terminates a relationship with one data broker, it can simply sign new contracts with another.

B. FEDERAL AND STATE LAWS OFFER LITTLE PROTECTION AGAINST WARRANTLESS ICE SEARCHES OF UTILITY DATA.

During a bill signing ceremony in late 2020, Governor Gavin Newsom proudly declared that immigrants and refugees make California a "greater and more vibrant place."[284] Among the new laws bearing the governor's signature that day was California Assemblymember Todd Gloria's bill, CA AB 2788, which promised to protect utility customer data—including utility usage information—from exposure to federal immigration enforcement.

Gloria's law responded to an urgent problem. Transparency reports from the state's utility companies showed that federal immigration enforcement had been routinely requesting Californians' utility customer information without first presenting a warrant.[285] Under the new law, if ICE wanted to directly request Californians' utility customer information, it would need to go to a judge and obtain a warrant or court order. If ICE wanted to access Californians' utility customer information through a data broker, the law stopped the data broker dead in its tracks.[286]

The passage of the law was "a tremendous victory," Gloria proclaimed, "for the privacy of all Californians and an important safeguard for our immigrant and refugee communities."[287]

But our findings regarding Equifax and NCTUE suggest that California's law contained a massive back door. While the legislation prohibited sales of customer data, it did not protect against simple dissemination. As a result,

California Gov. Gavin Newsom gives a thumbs up to Assemblyman Todd Gloria at a bill signing ceremony in 2019. (Photo: AP Photo/Rich Pedroncelli)

California's limit on the selling of customer data would be ineffective against a utility company that shares the information for free—to conduct a credit check, for example. When California utility companies disseminate customer information to NCTUE for credit evaluation and other purposes, they may not realize that NCTUE is entitled to resell their customers' information to third parties once the credit check is over. Indeed, despite the passage of this legislation, **1 in 2** Californians' utility customer data may have still been accessible by ICE through Equifax and NCTUE.[288]

California is not the only state whose laws have allowed utility customer information to reach ICE. Massive gaps in state utility privacy laws, combined with gaps in federal privacy laws, have left millions of Americans bereft of meaningful privacy protections when they sign up for gas or water. Within this regulatory vacuum, companies have built a lucrative marketplace to buy and sell utility customer information with ICE and other entities, even when legislators have tried to put strong regulations in place.

1. Federal privacy laws offer little to no protection.

When a marketplace for utility customers' name and address information first began to emerge in the late 1990s, federal regulators resisted putting rules on the buying and selling of that data. As the Federal Trade Commission (FTC) told Congress in 1997, "advances in computer technology" made it possible to look up Americans' personal information "from sources such as phone records, public utility records, and air travel records" more "easily and cheaply than ever before."[289] Despite how easy it was for that information to become available, however, many Americans had expressed strong privacy preferences,[290] and honoring those preferences seemed to be in the utility companies' own best interests.

The FTC simply recommended that Congress allow the Individual Reference Services Group (IRSG), a trade association representing major data brokers like Equifax and LexisNexis, to "be given the opportunity" to self-regulate. The ISRG accepted, promising the FTC that its companies would not sell customer information from telephone companies in cases where the customer chose to remain unlisted or any "similar information."[291]

It didn't take long for industry self-regulation to collapse. After the FTC adopted rules in 2000 to protect the privacy of consumers' personal information at banks and other financial institutions, the ISRG disbanded.[292] No federal regulators stepped up in its absence to safeguard customer data provided to utility companies. Over the next 20 years, Congress has failed to pass a single law protecting utility customer privacy.

Without meaningful lawmaking or industry self-regulation, utility customer privacy was hung out to dry. Federal regulators had already interpreted existing privacy laws like the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act to protect consumers' information only in the limited cases when financial institutions like banks used it or when it was material to consumer credit reporting.[293] Other privacy laws like the Cable Privacy Act or the Electronic Communications Privacy Act weren't interpreted to offer meaningful protections for the sale of consumers' name and address information either. And privacy protections for gas, electric and water customers were left to state regulators.

2. State privacy laws fail to adequately protect people's information.

Most states lack any meaningful privacy protections for the data generated by customers of gas, electric, water, telephone and cable companies. For the few laws and policies that do exist, closer examination reveals that the vast majority do little to protect customers' *addresses* against the two pipelines of disclosure through which that data travels: (1) disclosure to law enforcement by the company and (2) disclosure to commercial third parties, the path through which the bulk of that information travels to ICE, as evidenced by ICE's access of that data from Thomson Reuters and likely, today, LexisNexis.

a. State Utility Privacy Protection Scorecard

The Center on Privacy & Technology scored 51 jurisdictions' protections for utility customer addresses across the two pipelines of disclosure to ICE for all five utilities. For disclosure to law enforcement, a jurisdiction was given:

- a **green** score when it required a warrant for compulsory disclosure of a customer's address;
- a **yellow** score when a court-ordered subpoena or more is required for a customer's address or where agency regulation (but not law) prohibits disclosure of a customer's address; and
- a **red** score when an administrative subpoena or less is required to compel disclosure of a customer's address.

For disclosure to commercial third parties, a jurisdiction was given:

- a **green** score when it prohibited dissemination of a customer address to third parties or solely allowed its dissemination for specific business purposes and required prompt disposal;
- a **yellow** score when it prohibited dissemination of a customer address to third parties or solely allowed its dissemination for specific business purposes but did not require prompt disposal; and
- a **red** score when no such protections appeared to apply or when the jurisdiction predicated broad dissemination of a customer address to third parties on customer notice and consent, including for the purpose of credit evaluation.

Figure 5. State Utility Data Protection Scorecard for Law Enforcement Access

STATE UTILITY PRIVACY PROTECTION SCORECARD

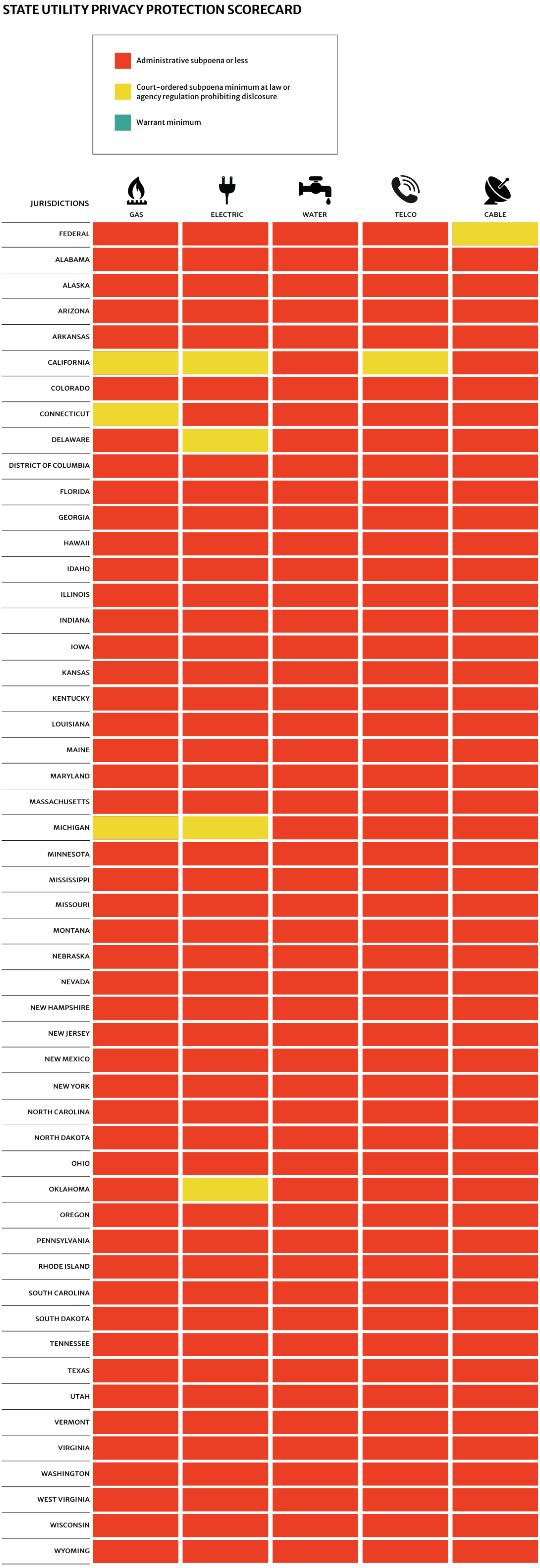
🟥 No protections at law or only notice and consent (including express or written consent), or use limitation without credit reporting exception

🟨 Dissemination to third parties limited to specific business purposes but no prompt disposal

🟩 Dissemination prohibited or dissemination limited to specific business purposes and prompt disposal required

JURISDICTIONS	GAS	ELECTRIC	WATER	TELCO	CABLE
FEDERAL	🟥	🟥	🟥	🟥	🟥
ALABAMA	🟥	🟥	🟥	🟥	🟥
ALASKA	🟥	🟥	🟥	🟥	🟥
ARIZONA	🟥	🟥	🟥	🟥	🟥
ARKANSAS	🟥	🟥	🟥	🟥	🟥
CALIFORNIA	🟥	🟥	🟥	🟥	🟥
COLORADO	🟥	🟥	🟥	🟥	🟥
CONNECTICUT	🟥	🟥	🟥	🟥	🟥
DELAWARE	🟥	🟥	🟥	🟥	🟥
DISTRICT OF COLUMBIA	🟥	🟥	🟥	🟥	🟥
FLORIDA	🟥	🟥	🟥	🟥	🟥
GEORGIA	🟥	🟥	🟥	🟥	🟥
HAWAII	🟥	🟥	🟥	🟥	🟥
IDAHO	🟥	🟥	🟥	🟥	🟥
ILLINOIS	🟥	🟥	🟥	🟥	🟥
INDIANA	🟥	🟥	🟥	🟥	🟥
IOWA	🟥	🟥	🟥	🟥	🟥
KANSAS	🟥	🟥	🟥	🟥	🟥
KENTUCKY	🟥	🟥	🟥	🟥	🟥
LOUISIANA	🟥	🟥	🟥	🟥	🟥
MAINE	🟥	🟥	🟥	🟥	🟥
MARYLAND	🟥	🟥	🟥	🟥	🟥
MASSACHUSETTS	🟥	🟥	🟥	🟥	🟥
MICHIGAN	🟥	🟥	🟥	🟥	🟥
MINNESOTA	🟥	🟥	🟥	🟥	🟥
MISSISSIPPI	🟥	🟥	🟥	🟥	🟥
MISSOURI	🟥	🟥	🟥	🟥	🟥
MONTANA	🟥	🟥	🟥	🟥	🟥
NEBRASKA	🟥	🟥	🟥	🟥	🟥
NEVADA	🟩	🟩	🟩	🟩	🟥
NEW HAMPSHIRE	🟥	🟥	🟥	🟥	🟥
NEW JERSEY	🟥	🟥	🟥	🟥	🟩
NEW MEXICO	🟥	🟥	🟥	🟥	🟥
NEW YORK	🟥	🟥	🟥	🟥	🟥
NORTH CAROLINA	🟥	🟥	🟥	🟥	🟥
NORTH DAKOTA	🟥	🟥	🟥	🟥	🟥
OHIO	🟥	🟥	🟥	🟥	🟥
OKLAHOMA	🟥	🟥	🟥	🟥	🟥
OREGON	🟥	🟥	🟥	🟥	🟥
PENNSYLVANIA	🟥	🟥	🟥	🟥	🟥
RHODE ISLAND	🟥	🟥	🟥	🟥	🟥
SOUTH CAROLINA	🟥	🟥	🟥	🟥	🟥
SOUTH DAKOTA	🟥	🟥	🟥	🟥	🟥
TENNESSEE	🟥	🟥	🟥	🟥	🟥
TEXAS	🟥	🟥	🟥	🟥	🟥
UTAH	🟥	🟥	🟥	🟥	🟥
VERMONT	🟥	🟥	🟥	🟥	🟥
VIRGINIA	🟥	🟥	🟥	🟥	🟥
WASHINGTON	🟥	🟥	🟥	🟥	🟥
WEST VIRGINIA	🟥	🟥	🟥	🟥	🟥
WISCONSIN	🟥	🟥	🟥	🟥	🟥
WYOMING	🟥	🟥	🟥	🟥	🟥

Figure 6. State Utility Data Protection Scorecard for Commercial Third-Party Access



STATE UTILITY PRIVACY PROTECTION SCORECARD

🟥 Administrative subpoena or less

🟨 Court-ordered subpoena minimum at law or agency regulation prohibiting dislcosure

🟩 Warrant minimum

JURISDICTIONS	GAS	ELECTRIC	WATER	TELCO	CABLE
FEDERAL	🟥	🟥	🟥	🟥	🟨
ALABAMA	🟥	🟥	🟥	🟥	🟥
ALASKA	🟥	🟥	🟥	🟥	🟥
ARIZONA	🟥	🟥	🟥	🟥	🟥
ARKANSAS	🟥	🟥	🟥	🟥	🟥
CALIFORNIA	🟨	🟨	🟥	🟨	🟥
COLORADO	🟥	🟥	🟥	🟥	🟥
CONNECTICUT	🟨	🟥	🟥	🟥	🟥
DELAWARE	🟥	🟨	🟥	🟥	🟥
DISTRICT OF COLUMBIA	🟥	🟥	🟥	🟥	🟥
FLORIDA	🟥	🟥	🟥	🟥	🟥
GEORGIA	🟥	🟥	🟥	🟥	🟥
HAWAII	🟥	🟥	🟥	🟥	🟥
IDAHO	🟥	🟥	🟥	🟥	🟥
ILLINOIS	🟥	🟥	🟥	🟥	🟥
INDIANA	🟥	🟥	🟥	🟥	🟥
IOWA	🟥	🟥	🟥	🟥	🟥
KANSAS	🟥	🟥	🟥	🟥	🟥
KENTUCKY	🟥	🟥	🟥	🟥	🟥
LOUISIANA	🟥	🟥	🟥	🟥	🟥
MAINE	🟥	🟥	🟥	🟥	🟥
MARYLAND	🟥	🟥	🟥	🟥	🟥
MASSACHUSETTS	🟥	🟥	🟥	🟥	🟥
MICHIGAN	🟨	🟨	🟥	🟥	🟥
MINNESOTA	🟥	🟥	🟥	🟥	🟥
MISSISSIPPI	🟥	🟥	🟥	🟥	🟥
MISSOURI	🟥	🟥	🟥	🟥	🟥
MONTANA	🟥	🟥	🟥	🟥	🟥
NEBRASKA	🟥	🟥	🟥	🟥	🟥
NEVADA	🟥	🟥	🟥	🟥	🟥
NEW HAMPSHIRE	🟥	🟥	🟥	🟥	🟥
NEW JERSEY	🟥	🟥	🟥	🟥	🟥
NEW MEXICO	🟥	🟥	🟥	🟥	🟥
NEW YORK	🟥	🟥	🟥	🟥	🟥
NORTH CAROLINA	🟥	🟥	🟥	🟥	🟥
NORTH DAKOTA	🟥	🟥	🟥	🟥	🟥
OHIO	🟥	🟥	🟥	🟥	🟥
OKLAHOMA	🟥	🟨	🟥	🟥	🟥
OREGON	🟥	🟥	🟥	🟥	🟥
PENNSYLVANIA	🟥	🟥	🟥	🟥	🟥
RHODE ISLAND	🟥	🟥	🟥	🟥	🟥
SOUTH CAROLINA	🟥	🟥	🟥	🟥	🟥
SOUTH DAKOTA	🟥	🟥	🟥	🟥	🟥
TENNESSEE	🟥	🟥	🟥	🟥	🟥
TEXAS	🟥	🟥	🟥	🟥	🟥
UTAH	🟥	🟥	🟥	🟥	🟥
VERMONT	🟥	🟥	🟥	🟥	🟥
VIRGINIA	🟥	🟥	🟥	🟥	🟥
WASHINGTON	🟥	🟥	🟥	🟥	🟥
WEST VIRGINIA	🟥	🟥	🟥	🟥	🟥
WISCONSIN	🟥	🟥	🟥	🟥	🟥
WYOMING	🟥	🟥	🟥	🟥	🟥

State laws designed to establish privacy protections for utility customers' personal information typically contain one or more significant weaknesses. Weak state laws typically only limit disclosures of utility customer information:

- when disclosure is compelled by law enforcement, without prohibitions on voluntary dissemination to other entities. Privacy protections that only apply to compulsory requests by law enforcement allow utility companies to voluntarily disclose utility customer information to data brokers and other third parties for any other purpose.
- when it's sold, without prohibitions on nonremunerative dissemination. Privacy protections that only apply to the sale of utility customer information allow utility companies to disclose utility customer information to federal immigration enforcement, data brokers and other third parties for any other purpose, including consumer credit reporting and immigration enforcement.
- concerning usage information, without prohibitions on disclosures of name and address information.
- unless it's disclosed to consumer credit reporting agencies. Privacy protections that contain overbroad credit reporting exceptions allow credit reporting agencies to disseminate customers' name and address information to third parties, including federal immigration enforcement.

As **Figure 5** shows, the overwhelming majority of states have failed to adopt meaningful privacy protections restricting the release of utility customer information to law enforcement. Only three states—California, Connecticut and Michigan—require law enforcement to obtain at least a court order to compel the disclosure of gas customers' information. For electricity customers, it's five states: California, Delaware, Michigan, Oklahoma and Wisconsin. For telecommunications customers, it's only California. Zero states have adopted any meaningful restrictions on the disclosure of water and cable customers' information to law enforcement.

Likewise, as **Figure 6** indicates, the overwhelming majority of states have also failed to adopt meaningful privacy protections restricting the dissemination of utility customer information to commercial third parties.

One state, however, stands out. Nevada has adopted strong rules that prohibit the dissemination of gas, water, electrical and telecommunications consumer information to third parties. Those rules protect consumers by strictly limiting the lawful purposes of dissemination and prohibiting disseminations for commercial purposes. Critically, unlike certain other states, Nevada's rules don't make an exception for the dissemination of a consumer's information with the consumer's permission. In a world where most regulators don't understand the marketplace for the resale and dissemination of consumer information, consumers cannot be expected to understand and be able to meaningfully consent to it either.

IV. ICE EXPLOITED THE TRUST OF UNACCOMPANIED CHILDREN AND THEIR FAMILY MEMBERS TO TARGET THOSE FAMILY MEMBERS FOR DEPORTATIONS.

Marisol holds her 7-year-old son as she speaks to immigration attorneys at the Santa Fe Dreamers Project.
(Photo: Gabriela Campos/The New Mexican)

In January 2017, a teenager fleeing his violent uncle in Guatemala crossed the Sonora Desert and showed up alone at the Arizona border. He hoped to reach his older brother, Gari, who was living in Santa Fe, New Mexico.[294]

The 17-year-old was taken in by border officials and later transferred to the custody of the Office of Refugee Resettlement (ORR), which is run by HHS. Upon arrival, ORR officials asked the teenager whether he had any close family members living in the U.S. who could take him in. Unaccompanied minors at the border are often afraid to answer that question, especially if their relatives are undocumented, because the children understand that sharing any information with government officials could put their family members in jeopardy. But the children have few alternatives. They are desperate to see their families. So, they take the risk.[295] The teenager told the officials that he had a brother in the U.S. and gave them Gari's name and phone number.

When Gari received the call about his brother, he was struck with concern, but he was also worried about what it would mean to step forward and take the boy under his care. Gari had a family of his own—a wife, a 7-year-old son and an infant daughter—and he was afraid that participating in the extensive application and background check process would put him at risk of deportation.

But HHS officials had assured him that that would not be the case. Gari was told that his participation in the process wouldn't affect his own safety. It was simply necessary to place his brother with a caretaker during the boy's immigration case. With that in mind, Gari decided to accept legal guardianship of his brother, whom he hadn't seen in more than a decade.

Just a few months later, however, Gari's fears were realized. After his brother told the government his name and after Gari agreed to step forward as a sponsor, ICE went after him. That August, ICE agents arrived at his home, arrested him, detained him in an ICE facility in Chaparral, New Mexico and placed him in deportation proceedings.[296] The immigration agents even looked for his wife, Marisol, before they finally took Gari away.

A. ICE MINED CHILD WELFARE RECORDS TO TARGET DEPORTATIONS.

In the last two decades, the number of unaccompanied children fleeing violence and poverty by crossing the U.S. border has risen by an order of magnitude, from just under 5,000 in 2003 to nearly 50,000 in 2018.[297] Those children are often covering vast distances and dangerous terrain to seek asylum or other protections in the U.S. and join family members on the other side of the border.[298] When they arrive, they are traumatized and exhausted.

Historically, when unaccompanied children arrived at the border, the now-defunct INS was the only agency responsible for their care and custody. The agency kept children in conditions so dire that they ultimately led to a class-action lawsuit, *Flores v. Reno*, which alleged deplorable conditions in INS facilities, including children being housed in the same facilities as adults, being subjected to strip searches, and lacking education and recreation—all while INS refused to release them to responsible adult guardians who wanted to care for them properly.[299]

The suit ultimately ended in a settlement agreement that set the standards for how children in INS custody should be treated, including requirements for clean water, food and the prioritization of the placement of a child with a relative or guardian so as to minimize their time in detainment.[300] With the Homeland Security Act of 2002, the job of caring for unaccompanied children arriving in the U.S. was separated from federal immigration enforcement and instead placed with ORR within HHS,[301] an agency better suited to care for children.

Today, under the framework established by that law, unaccompanied children are required to be moved from the custody of immigration enforcement agencies like CBP or ICE and into the care of ORR as quickly as possible. When an unaccompanied child reaches the U.S. border and is encountered by border patrol or another arm of DHS, they must be referred to ORR within 72 hours for care while they await legal review of their case.[302] ORR has binding obligations, via the *Flores* settlement and the Trafficking Victims Protection Reauthorization

Act of 2008 (TVPRA), to find the "least restrictive setting that is in the best interest of the child" and to release the child into that setting promptly.[303] Whenever possible, that means that ORR should find family members or guardians who can sponsor the child.[304]

To find potential sponsors, ORR relies on information that the minors themselves are able to provide. Upon intake, staff members ask the child if they have relatives or guardians with whom they intend to live within the U.S. If the child is able to provide this information, ORR will contact the potential sponsor to ask if they are willing to step up and take care of the child.[305]

But before releasing a child into a sponsor's custody, ORR is responsible for assessing the suitability of the sponsor and, when relevant, verifying that the adult is a relative or guardian of the child. Those who apply to sponsor a child must provide ORR extensive personal documentation: their contact information, proof of address, information about others living in the household, financial information, and information about their relationship to the child.[306] The sponsor is also subjected to a public records check and fingerprints are collected for a criminal background check.[307] Sharing such personal data is in many cases a difficult choice but one that thousands of people have made as they understand that they may offer the only way out of a detention facility for a child they care about. In sharing that information, they must trust that ORR has only the child's best interests in mind.

Under the Trump administration, ICE exploited that trust to target deportations of the family members who came forward to care for unaccompanied children. In May 2017, ICE began its Human Smuggling Disruption Initiative, supposedly intended to target human smuggling and trafficking organizations. That initiative was an "interagency 90- to 120-day operation" with a focus on the "identification, investigation, and arrest of human smuggling facilitators, including, but not limited to, parents and family members."[308]

ICE agents mined data provided by unaccompanied children and their sponsors to build "target packages" of sponsors.

Under this operation, ICE agents mined years of ORR records containing information provided by unaccompanied children and their potential sponsors. The agency used Nlets to receive information submitted by ORR and compiled the data in the form of "target packages" on potential sponsors.[309] ICE took those target packages and opened cases in Palantir's Investigative Case Management (ICM) software, a system that helps agents manage investigations and that integrates a multitude of other data streams from sources within law enforcement.[310]

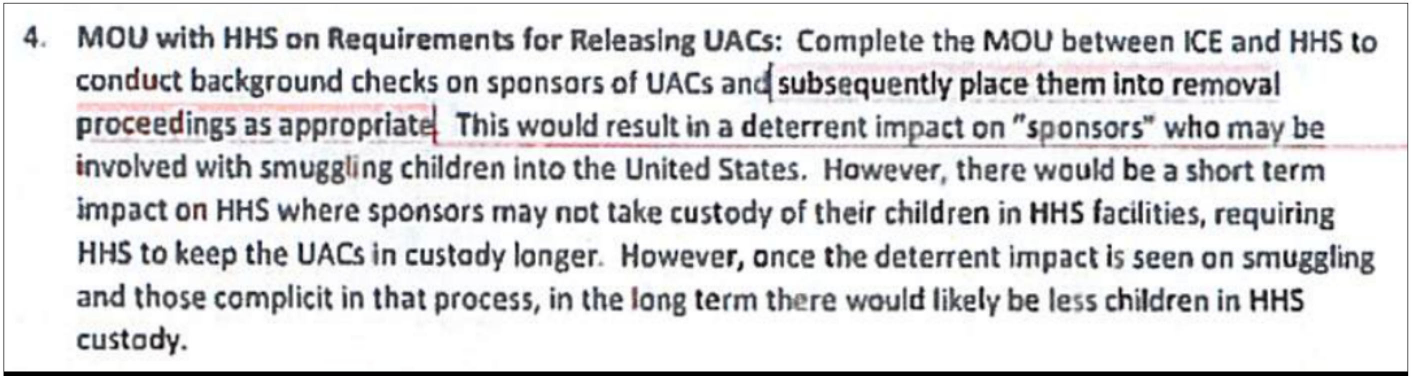
In the end, despite its stated purpose, ICE used the initiative almost exclusively to target potential sponsors of unaccompanied children rather than human smuggling operatives. Out of the more than 400 people who were arrested during this program, the vast majority were never charged with smuggling crimes but rather only with civil immigration infractions.[311] ICE not only targeted potential sponsors, but it also made "collateral arrests" of people found to be living in a potential sponsor's household.[312]

ICE's actions had immediate effects on the well-being of children and their potential sponsors. In a December 2017 letter to the DHS' Office of Civil Rights and Civil Liberties, eight civil rights organizations documented the harms already occurring to children and sponsors. The letter noted that potential sponsors grew fearful that stepping up to care for a child would lead to their own arrest or the arrest of their family members, and they were less likely to come forward, leaving children to languish for lengthening amounts of time in detention. Their prolonged stays also contributed to severe bed shortages in government shelters, creating a backlog of children in crowded cells at Border Patrol stations that lacked basic equipment for their care.[313]

The data-sharing policy also had devastating impacts on sponsors and the members of their households. Families who had already been reunited with a child through ORR began receiving unexpected visits from ICE, and sponsors who had committed to caring for a child were rewarded with interrogation and arrest, separating them not only from their sponsor child but also often from their own children as well. In the face of new and unexpected legal challenges, families faced financial and housing instability, and children reported experiencing significant mental health consequences.[314]

> **" . . . the increase in prosecutions would be reported by the media and it would have a substantial deterrent effect."**

The harm ICE was causing to these children and that their U.S. sponsors faced was not the byproduct of ill-conceived border security measures; it was an intentional part of the policy. A memo leaked to Senator Jeff Merkley (D-OR) in 2019 shows that the targeting of potential sponsors for deportation was *intentionally* designed to deter future asylum seekers, with the full knowledge that it would negatively impact children already in custody.[315] The memo, dated December 2017, details how a formal data-sharing agreement with ORR furthers that goal.



4. **MOU with HHS on Requirements for Releasing UACs:** Complete the MOU between ICE and HHS to conduct background checks on sponsors of UACs and subsequently place them into removal proceedings as appropriate This would result in a deterrent impact on "sponsors" who may be involved with smuggling children into the United States. However, there would be a short term impact on HHS where sponsors may not take custody of their children in HHS facilities, requiring HHS to keep the UACs in custody longer. However, once the deterrent impact is seen on smuggling and those complicit in that process, in the long term there would likely be less children in HHS custody.

Excerpt from "Policy Options to Respond to Border Surge of Illegal Immigration," a DHS internal memo obtained and released by Senator Jeff Merkley (D-OR) in January 2019. (Photo: Office of Sen. Merkley)

In the face of mounting evidence of the harms this policy caused, ORR and ICE decided to formalize the policy. In a Memorandum of Agreement dated April 2018, ORR agreed to provide ICE with “the name, date of birth, address, fingerprints […], and any available identification documents or biographic information regarding the potential sponsor and all adult members of the potential sponsor’s household.”[316] That gave ICE not only access to historical ORR data but ongoing information about potential sponsors and the members of their households.

With the information provided directly from the agency statutorily bound to serve the “best interests of the child,” ICE proceeded to target and arrest hundreds of potential sponsors who had stepped up to care for children who otherwise would have remained in detention. According to congressional testimony from Matthew Albence, the then-acting director of ICE, the agency had arrested approximately 330 potential sponsors based on information obtained via the data-sharing program before it ended.[317] That is in addition to the roughly 400 arrested during the pilot program.

With every passing month, the negative consequences of the ICE-ORR data-sharing policy continued to accumulate. Fewer and fewer potential sponsors were willing to step up for fear of risking arrest themselves or for others in their family. A survey conducted by the Women’s Refugee Commission and NIJC of people working with unaccompanied children (e.g., child advocates, lawyers, biometric technicians) found that 75% of respondents knew of potential sponsors who had not come forward for fear of the data-sharing agreement, and two-thirds of those knew of multiple cases.[318] The fear was not limited to sponsors who were themselves undocumented; because the sponsorship application asks for all members of the household the child would join, sponsors could be deterred from stepping up as a result of the need to protect other relatives living in their home.

Unaccompanied minors were left to spend prolonged time in ORR facilities. The average length of time a child spent in detention more than doubled between 2017 and 2019.[319] The number of children kept in detention also soared; between summer 2017 and summer 2018, the number of migrant children in detention increased fivefold, from 2,400 to 12,800.[320] Meanwhile, the backlog continued to grow at Border Patrol stations, where thousands of children sat in cramped holding cells waiting for space to open up in ORR shelters.[321]

As it became more and more glaringly evident that the ICE-ORR data-sharing policy violated the *Flores* settlement and TVPRA[322] and as the public outcry grew louder, lawmakers attempted to intervene. The FY19 Appropriations Bill barred DHS from using funds to “place in detention, remove, refer for a decision whether to initiate removal proceedings, or initiate removal proceedings against a sponsor, potential sponsor, or member of a household of a sponsor or potential sponsor of an unaccompanied alien child.”[323] (The Center on Privacy & Technology is proud to have partnered with the Brennan Center for Justice, NIJC and a coalition of dozens of other civil society organizations to press for this provision.)

Still, the appropriations rider did not legally bar the agencies from sharing data for this purpose, nor did it cut off funding in every instance. It wasn’t until March 2021 that the Memorandum of Agreement was officially ended and replaced by one that no longer commits ORR to sharing sponsor data like fingerprints and biographic information with ICE.[324]

Unfortunately, this story is not the only one of its kind. The fact that the ICE-ORR data-sharing agreement deterred potential sponsors from coming forward to care for unaccompanied children, causing them to languish in prolonged detention at the border, must not be viewed as an isolated atrocity. It must be understood as part of a much broader pattern by which ICE uses surveillance to target, coerce and exploit some of the most vulnerable people in our country.

B. ICE SURVEILLANCE CAUSES CLEAR AND MEASURABLE CHILLING EFFECTS ON PEOPLE'S ABILITY TO ACCESS BASIC NECESSITIES.

Originating in First Amendment doctrine, the phrase "chilling effects" captures the idea that some law or government action deters people from engaging in activity protected by the Constitution, largely for fear of prosecution or due to uncertainty about the legal process.[325] When it comes to surveillance, that sense of uncertainty—around what is known by the surveiller, where and how one might be watched, as well as what the consequences of that observation may be—is what makes it especially effective at chilling behaviors.[326]

However, as was made clear by the deterrent effects of the ICE-ORR data-sharing agreement, surveillance by immigration enforcement chills actions far beyond those protected by the First Amendment alone. In addition to inhibiting speech or assembly, ICE surveillance—or even just the possibility of surveillance—also deters people from participating in a broad range of basic activities necessary for health and well-being.

1.Surveillance drives immigrants to avoid institutional systems, regardless of the purpose of those systems.

The sociologist Sarah Brayne introduced the concept of "system avoidance" to capture how concerns about law enforcement surveillance can dampen individuals' willingness to participate in essential activities.[327] Through two longitudinal, nationally representative surveys with American youth, Brayne found that individuals who have had any contact with the criminal legal system—ranging from being stopped briefly on the street to being incarcerated—are less likely to interact with record-keeping institutions such as banks, hospitals, employers and schools compared to people who have not had contact with the criminal legal system. At the same time, contact with the criminal legal system did not decrease the rate at which people interacted with *non*-record-keeping institutions like volunteer organizations and religious groups, which suggests that individuals' avoidance is closely tied with the act of record-keeping and concerns about how that information may be used.

Similarly, sociologist Asad L. Asad observed that fears about deportation correlated with immigrants' concerns about being "in the system."[328] Drawing on 50 in-depth interviews with Latin American immigrants in Dallas, Asad found that undocumented participants described a feeling of safety in keeping their information private from record-keeping institutions. Some undocumented immigrants even avoided processes that could legalize their status, because participation would require them to become visible to an institution that could deport them. Among authorized immigrants, such as lawful permanent residents or individuals with DACA protections, Asad observed that being "documented" could actually increase fear. Immigrants with legal status expressed concerns that any misstep—misfiled paperwork, an unpaid traffic ticket—could be noted in their records and put their status at risk.

Those fears can last for generations. In a survey of adult children of immigrants, many of whom are themselves U.S. citizens, Desai et al. found that system avoidance is associated with having an undocumented parent.[329]

Those studies offer a lens through which we can begin to understand what has been reported both anecdotally and in the academic literature: Concerns about data sharing cause immigrants to avoid record-keeping institutions that are critical to the well-being of themselves and their families. That fear persists even when it comes to engaging with institutions that are unrelated to immigration. The rest of this section demonstrates how surveillance chills participation in three specific contexts: child welfare, health care and access to legal systems.

SIDEBAR 3.
HARMS OF CHILLING EFFECTS REACH FAR BEYOND UNDOCUMENTED PEOPLE

Avoidance of record-keeping institutions hurts individuals, but those harms also reverberate throughout entire families and communities. Many immigrant families are mixed-status families, which means that different members of the household have different legal statuses and therefore face different levels of risk of deportation. The impacts of system avoidance by undocumented parents therefore extend to their children, almost 90% of whom are themselves U.S. citizens.[330] Those impacts are likewise felt throughout the community. If some community members avoid seeking health care, for example, otherwise preventable health issues can become debilitating and costly for the rest of the community.[331] In schools, food insecurity that a particular child experiences can disrupt the learning environment for all students.[332]

2. Surveillance chills people's use of services that promote children's well-being.

Research suggests that fears about ICE surveillance deter undocumented families from seeking benefits to support their own and their children's well-being. The children of undocumented parents are often U.S. citizens, which means that they may be eligible for programs like food assistance. However, the willingness of households to sign up for those programs can be influenced by the fear of surveillance by immigration enforcement. A study that used data from a nationally representative, longitudinal survey of household food consumption for families with children found that food insecurity in Mexican noncitizen households with children increased nearly 10 percentage points in metro areas where local law enforcement had entered into 287(g) agreements to share data with and cooperate with immigration enforcement.[333]

3. Surveillance drives people to avoid health care.

Concerns about data sharing between hospitals or clinics and government agencies also deter immigrants and their families from seeking health care. A review of studies that examined barriers to health care for undocumented immigrants found that a majority of those studies report immigrants' concerns that providing documentation or using a health care or benefit service could result in them being reported to immigration authorities.[334]

Health care providers also offer anecdotal reports about how fears about immigration enforcement can impact individuals' willingness to seek care. The Mile High Health Alliance, a multi stakeholder collaboration in Denver aimed at addressing challenges to health care access, conducted a survey of member and partner clinics about immigrant and refugee utilization of health services beginning in 2017.[335] In the survey, many clinics reported that patients expressed concerns about information sharing, which led them to opt out of Medicaid and other benefits they were entitled to for fear of being in a "government system." Some patients even refused to answer some questions from their own doctors, such as questions about their country of birth. One patient whose child was undocumented spent their appointment asking about sanctuary policies that restrict information sharing and other forms of cooperation with immigration enforcement.

Denver clinics reported that some patients opted out of Medicaid for fear of being in a "government system."

The deterrent effect of surveillance has also been demonstrated at a larger scale and not just among people with precarious immigration statuses. A 2015 survey of Latinx U.S. citizens found that respondents would be less likely to make an appointment at a health care provider if immigration were mentioned during the scheduling process.[336] The effect is even more pronounced in those who have seen immigration enforcement activities up close. Latinx U.S. citizens who knew someone who was undocumented or who had been deported were found to be more skeptical of the security of the information they share with health care providers, expecting that it might be shared beyond the provider.

4. Surveillance deters people from interacting with the legal system and other government entities.

Data sharing among government agencies and immigration enforcement has been shown to discourage immigrants from interacting with government entities and participating in legal processes. A survey by the Urban Institute showed that families with immigrant members were less likely to participate in a number of routine activities like applying for a driver's license, talking to police, reporting crime, using public transportation and talking to school officials for fear of needing to disclose their immigration status—even though many of those institutions are not formally connected to federal enforcement.[337]

Other studies have demonstrated that the fear of data sharing plays a key role in deterring immigrants and their families from interacting with bureaucratic systems. A survey of Latinx immigrants found that respondents reported they would be less likely to interact with legal and bureaucratic systems if they knew that the entities were sharing data with ICE.[338] Specifically, their findings describe the way that ICE data sharing chills willingness to report a crime to police, testify in court and access resources for child care.

> **People with immigrant family members were less likely to drive, apply for a driver's license, talk to the police, visit a doctor, report a crime, use public transportation or talk to school officials for fear of needing to disclose their immigration status.**

CONCLUSION AND RECOMMENDATIONS

Maribel Cortez testifying at the Maryland General Assembly. (Photo: Erin Cox/The Washington Post via Getty Images)

On Feb. 27, 2020, not even a month after ICE agents arrested and detained her husband, Maribel Cortez walked into the halls of the Maryland General Assembly. She was accompanied by three of her children and representatives from CASA, the immigrant rights organization that spearheaded efforts to protect immigrants in Maryland from the reach of ICE surveillance.

Maribel testified before committees in both the House of Delegates and the state Senate, telling her story and working to pass a law to protect families like her own. She spoke in Spanish with the support of an interpreter from CASA. "This has destroyed my children," Maribel said, through tears.[339] "For their whole lives, they've had their father in their lives. And now it's very difficult for them," she told The Washington Post.[340]

Maribel's story encouraged lawmakers to act. A year and one month to that day, the Maryland General Assembly passed the Maryland Driver Privacy Act, a bill that will end ICE's warrantless access to Marylanders' data.

Remarkably, what Maribel did in Annapolis, Maryland, that day, other immigrants have done across the country in Albany, New York; Denver; the district; Honolulu; Montpelier, Vermont; Olympia, Washington; Richmond, Virginia; Sacramento, California; Salem, New Hampshire; Santa Fe, New Mexico; Springfield, Massachusetts; and Trenton, New Jersey—arm in arm with organizations like the Immigrant Defense Project, Just Futures Law, the Legal Aid Justice Center, Make the Road New York, Mijente and NILC.

The following recommendations are inspired by the bravery of the communities that continue to fight against mass deportation and have been crafted in consultation with leaders in the immigrant rights movement and other experts.

A. CONGRESS

1. Congress should reform U.S. immigration laws to radically reduce the number of people who can be subjected to deportation.

The best and ultimately perhaps the only way to take apart ICE's dragnet is to take apart the laws on the basis of which the executive branch targets hundreds of thousands of people (primarily poor people and people of color) for deportation every year. Congress could significantly reduce the number of people subject to deportations by creating a pathway to citizenship for undocumented people and by dramatically reducing the grounds of removability that are based on criminal legal involvement. To build an additional bulwark, Congress could enact a statute of limitations on deportations. Most crimes and civil offenses cannot be prosecuted after five years. Incongruously, however, a person can be deported from this country via a process in which they are not legally guaranteed an attorney, despite having lived here, built a family and paid taxes over the course of decades. Immigrant rights organizations have put forth a number of legislative frameworks over the last decade that would accomplish these reforms among many important others.[341] While these proposals do not address surveillance itself, they are the most direct way to undercut ICE's claims of broad surveillance authority.

2. Congress should protect the privacy of people who trust the federal government with their data.

The federal government runs a series of programs that actively solicit undocumented people, many of whom are in trauma or under duress, to provide federal agencies with a wide variety of highly sensitive personally identifying information.

Congress must broadly prohibit the government from using data solicited from people, for the purpose of providing benefits and services, to carry out deportations. Such a policy could be modeled on the federal laws protecting the confidentiality of census data, the gold standard for protections of sensitive data the federal government solicits from the people.[342] Critically, those laws prohibit the use of census data for nonstatistical purposes and broadly mandate that "[i]n no case shall information furnished [to the Census Bureau] be used to the detriment of any respondent or other person to whom such information relates," with a narrow exception for violations of the census rules themselves.[343] Congress should achieve those protections via a wraparound statute; until that passes, Congress should do so through restrictions on the usage of funds in appropriations bills, and the DHS should do so via policy.

At a minimum, Congress should amend the laws governing these programs to prohibit immigration enforcement's use of the specific data that the programs generate. Congress should amend the following laws in this way:

- TVPRA, 8 U.S.C. § 1232, which protects unaccompanied children;
- the federal statutes creating T and U visas for victims of trafficking and other crimes, 8 U.S.C. § 1101(a)(15)(T) & (U);
- the federal tax privacy laws, 26 U.S.C. § 6103; and
- the Higher Education Act's privacy provisions for data from federal financial aid forms, 20 U.S.C. § 1090(a)(3)(E).

President Biden or the DHS secretary could also enact additional privacy protections for DACA applicants and other forms of temporary status or deferred action through executive order or department policy.

3. Congress should stop ICE's use of DMV data.

Congress passed the DPPA before the modern era of mass surveillance and mass deportation. The act passed in 1994—three years before the U.S. began removing approximately 100,000 people annually, nine years before ICE was created and 15 years before ICE began deporting roughly 0.1% of the American population every year.[344]

ICE has not hesitated to use the broad carve-outs for government agency access in the DPPA to warrantlessly scan the faces of an astonishing number of Americans and to search through the address information of most U.S. residents. Congress should update the DPPA to prohibit or require a warrant or court order for any law enforcement use of DMV data for immigration purposes.

4. Congress should conduct aggressive oversight of ICE surveillance.

While specific members of Congress have begun to pressure ICE through oversight letters, no congressional committee or subcommittee of the many ostensibly charged with overseeing ICE has held a hearing devoted to this subject. There also has not been any GAO investigation into ICE's vast surveillance arsenal.

That must change—and it can change quickly. Committee and subcommittee chairs do not need a majority or supermajority vote to force ICE to answer for its surveillance abuses and the vast secrecy that surrounds them. Potential subjects for a hearing or GAO report include:

- whether there exists any legal basis, given the absence of any explicit authorization in statute or regulation, for ICE's surveillance practices;
- how ICE sidesteps state laws protecting the data of drivers and other residents;
- whether ICE's dragnet surveillance and data sharing violates the Fourth Amendment or any other constitutional provision;
- how ICE's reliance on data brokers evades public scrutiny and helps the agency circumvent statutory and constitutional privacy protections;

Reps. Raja Krishnamoorthy (D-IL) and Jimmy Gomez (D-CA) pressed Thomson Reuters and Equifax for more information on their sale of utilities customers' data to ICE. (Photos: Tom Williams / Pool via Getty Images (L, R))

- how ICE currently uses biometrics, including face recognition, fingerprints and DNA, and how it plans to use them in the future;
- the practical and ethical ramifications of ICE's use of gas, electric, water, phone and internet records to target deportations; and
- the taxpayer expense of ICE surveillance.

The wide range of concerns raised by ICE surveillance should make it possible for any number of congressional committees and subcommittees to engage on this topic through a hearing or a request for a GAO investigation.

Congress should also require detailed public reporting about ICE's surveillance programs as part of the annual appropriations process.

B. DHS & ICE

1. ICE should end all dragnet surveillance programs.

ICE agents have run or obtained face recognition searches on the faces of at least 1 in 3 adults. They have hired a company that tracks vehicle movements of the residents of America's 50 largest cities—a majority of the U.S. population. They have hired another company to give them the utilities records of a majority of the U.S. population.

Run in secret, even to the most senior members of Congress charged with conducting oversight of the agency, those actions undermine even basic notions of balance of powers, corrode public trust and fly in the face of the Fourth Amendment.

All of ICE's surveillance programs should be placed under piercing scrutiny. However, ICE should immediately terminate all dragnet surveillance programs—both ICE-led and obtained from data brokers—that indiscriminately collect data on as many people in the U.S. as possible. Programs that ought to be characterized as this type of especially problematic dragnet surveillance include at least (1) the practice of scanning driver's license photos for immigration enforcement purposes; (2) the bulk collection of address information and other records from DMVs and utility companies; and (3) the bulk collection of license plate photos capturing the movement of drivers in major U.S. metropolitan areas; the purchase of bulk data sets containing any of the above information from corporate data brokers.

2. ICE should stop using face recognition for immigration enforcement.

In May 2020, ICE issued a Privacy Impact Assessment asserting that "Enforcement and Removal Operations (ERO) will not use and HSI will not support ERO in using [face recognition systems] solely in furtherance of civil immigration enforcement."[345] This statement would appear to still allow ICE to use face recognition to freely target roughly 4 in 10 undocumented people who entered the country without inspection or any other immigrant who was alleged to be involved in any other crime, however minor.[346] Those offenses would justify scans of the faces of millions of Americans, native- and foreign-born, documented and undocumented alike.

In 2021, face recognition algorithms have been found to be rife with race and gender bias—by the federal government itself.[347] They have been used in ways that obviously violate basic principles of privacy and due process.[348] They have resulted in the wrongful arrests or accusations of several people without legal basis, many of whom were people of color.[349] ICE should not use that tool for any kind of immigration enforcement.

3. ICE should stop exploiting people's need for water, heat, electricity, phone or internet to target them for deportation.

There is now a broad body of evidence-based, peer-reviewed research showing that immigrants avoid basic services like health care, not just for fear that they will be arrested on-site but also because they fear their *data* will be shared with the federal government and that their information will be held in government systems.[350]

People need heat, water and electricity to survive. They need the internet and phone lines to maintain their livelihoods and connect with their communities. Yet we now know that nearly 200 million adults have had their addresses and other information shared with ICE as a result of their opening accounts for water, gas, electric, phone or internet service.[351] DHS should immediately issue a clear prohibition against the use of this data in immigration enforcement.

4. ICE should disclose surveillance investments and programs to members of Congress and key state officials.

The chairs of key congressional committees have learned of vast ICE surveillance programs from the newspaper. So have state legislators, who are responsible for authorizing and voting to finance many of the state databases that ICE uses. One in 3 adults have had their faces scanned by or at the request of ICE—all without their knowledge.[352]

This is not acceptable. It is also incompatible with basic principles of democratic governance.

At a bare minimum, ICE should regularly brief the members and staffs of key congressional oversight committees and subcommittees, including:

- the Senate Homeland Security & Government Affairs Committee;
- the Senate Judiciary Committee, including the Subcommittee on Immigration, Citizenship & Border Security and the Subcommittee on Privacy, Technology & the Law;
- the House Homeland Security Committee;
- the House Judiciary Committee, including the Subcommittee on Immigration & Citizenship; and
- the House Committee on Oversight & Reform.

ICE should also brief the governors and key legislators in states where ICE is conducting surveillance. ICE commonly notifies state and local officials before large on-site enforcement actions targeting several hundred people. When ICE engages in dragnet surveillance programs that ensnare millions of the state's licensed drivers, for example, they should tell state officials about it.

5. The DHS inspector general should issue regular public reports on ICE surveillance activities.

Briefing legislators alone is not enough; the executive branch often has a very different sense of what it has disclosed as compared to its audience. In 2013, after the press published court orders revealing that the National Security Agency was collecting substantially all Americans' domestic call records, Obama assured the public that "every member of Congress has been briefed on this program."[353] The House sponsor of the USA PATRIOT Act, Rep. Jim Sensenbrenner (R-Wisconsin) immediately retorted that, actually, "most" members of Congress—including himself—had been left in the dark.[354]

To avoid repeating these mistakes, the DHS inspector general should go beyond disclosure to members of Congress, governors and state legislators by offering annual public reporting. At a bare minimum, these reports should identify:

- the kinds of technologies ICE is using (e.g., face recognition, automated license plate reader, etc.);
- the states and counties in which ICE uses them;
- the government and commercial databases ICE is accessing, the kinds of data held within those databases and the number of searches within those databases;
- the approximate number of individuals whose data it has collected or whose data is held in the databases accessed;
- the number of individuals who were arrested, incarcerated and deported on the basis of the information collected or accessed; and
- whether ICE has briefed federal, state and local officials about these deployments.

The federal government already releases detailed annual reports on where, when and for how long it conducts wiretaps; the nature of the crimes investigated; and the ultimate results of those investigations. That is done regardless of the severity of the offense.[355]

C. STATE & LOCAL LAWMAKERS[356]

1. State and local lawmakers must protect people who trust them with their data.

When undocumented people apply for a driver's license, enroll themselves or their kids in school, register for a COVID-19 vaccination, or rely on state or local nutritional assistance programs, they do so under explicit or implied promises that state and local authorities will not allow for their data to be shared, in bulk, with immigration enforcement.

State and local governments must offer wraparound protections for any data solicited from undocumented residents and held by the state—not just driver information. What's more, jurisdictions that have already enacted those policies should take steps to make them as strong as possible. Specifically, policymakers should:

- **Adopt a policy of data minimization.** Immigration authorities, data brokers and other parties cannot exploit data that does not exist. State and local bureaucracies should adopt a policy of data minimization, collecting only data that is necessary to administer services, storing that data for the minimum time necessary and designing digital record keeping systems with data minimization in mind on the front end.

- **Focus on the data, not the custodian.** Many different agencies can have access to the same pools of data, including driver records. The D.C. Sanctuary Values Act avoids that problem by restricting release of personally identifying information and other data by the "District of Columbia," rather than naming any specific agencies or subagencies.[357]

- **Focus on the *purpose* of the sharing, not the recipient.** Naming ICE is both under- and overinclusive. Other federal agencies (e.g., CBP) regularly engage in immigration enforcement, and certain ICE components' work is typically separate from immigration enforcement.[358] Thus, jurisdictions should protect against sharing for the *purpose* of immigration enforcement, not merely against sharing to ICE, the entity. One example is Maryland's Driver Privacy Act, passed in 2021, which blocks warrantless sharing of data with "any federal agency" seeking access for the purpose of "enforcing federal immigration law."[359]

- **Protect against all forms of information sharing,** including (1) sharing in response to a direct request, (2) database access for immigration enforcement officials, and (3) the sale or sharing of information to data brokers, who in turn give that data to immigration enforcement. It is often straightforward to address the first two modes of sharing, but the third typically requires dedicated language. New York's Green Light law is a model in that respect, containing a provision that requires any entity receiving driver data to certify that it will not disclose the information to immigration enforcement agencies.[360]

- **Don't distinguish between "civil" and "criminal" immigration enforcement for the purposes of privacy protection and data-sharing restrictions,** because federal law criminalizes illegal entry and illegal re-entry.[361] For example, Hawaii's law allowing undocumented people to apply for driver's licenses institutes a simple prohibition against sharing of applicants' data without any carve-outs for any kind of immigration enforcement.[362]

- **Ensure that face recognition is clearly encompassed by these restrictions.** DMV photos are sometimes excluded from the categories of data protected by state privacy laws.[363]
- **Eliminate blanket exceptions for "law enforcement" access to state or locally held data.** Between 2017 and 2019, California legislators passed three separate laws to prevent state agencies from freely sharing driver data with immigration authorities.[364] Unfortunately, they did not amend a separate law mandating that "law enforcement agencies … shall have access to" the records of the California DMV, a provision cited by the DMV to defend its apparent sharing of driver data with ICE.[365]
- **State and local lawmakers should structure their government databases to track ICE access and audit those databases regularly to identify the routes, frequency and nature of that access.**

Any database administrator must be able to answer two questions: Does ICE have access to this database? If so, how and why has ICE used it? In the third decade of the 21st century, there is no excuse for a state or local government to build a database containing sensitive data that does not allow for detailed monitoring to ensure it is being accessed by authorized people for authorized use.

State and local authorities should regularly audit these databases to determine whether, how and how often ICE is accessing them. If authorities do not run those audits on their own, legislators should send oversight letters to state agencies demanding that they do so and hold oversight hearings to force agency officials to do the work.

Legislators who press for those audits should know that it is unacceptable and unusual for a modern database to omit those capacities; if they are told otherwise, they should press further. In Maryland, for example, legislators were initially told that the state's face recognition system, the Maryland Image Repository System, was not capable of tracking users by agency. During a subsequent site visit, however, the legislators learned that the Department of Public Safety and Correctional Services was, in fact, capable of tracking that data.[366]

It is unacceptable and unusual for a modern government database to lack audit trails. If legislators are told otherwise, they should press further.

SIDEBAR 4. FEDERAL PROHIBITIONS ON STATE AND LOCAL "SANCTUARY" LAWS

There is no federal law that limits or prohibits a state or locality from establishing restrictions on the collection, retention or disclosure of residents' name and address information. One federal law, 8 U.S.C. 1373, purports to prohibit a state or locality setting limits on information sharing related to a resident's "citizenship or immigration status."[367] But that law's constitutionality remains unsettled[368] and by its own terms does not extend to restrictions on collecting, retaining or sharing a resident's name and address information.

State and local lawmakers should block the disclosure, sale or resale of utilities data for use in immigration enforcement.

Gas, water and electric utilities are largely regulated at the state and local level through statutes, ordinances and oversight by public utilities commissions. State and local governments also often have protections for telephone and internet data that supplement federal law.[369] State and local authorities should prohibit the disclosure, sale or resale of that data for immigration purposes.

A few states have good standards that apply to a specific utility (e.g., gas or electricity). Not one state or territory has enacted meaningful wraparound privacy protections for all utilities. In enacting those protections, state and local authorities should:

- **Restrict disclosure to *data brokers*, not just the government.** ICE usually gets access to utilities data through data brokers, rather than direct requests to companies. Laws must protect against disclosure of the data to third-party companies, not just the government.
- **Avoid blanket carve-outs for credit reporting and evaluation.** Data disclosed to a credit agency for credit purposes can easily be redisclosed for immigration enforcement. Indeed, the entity that created the database

accessed by Equifax to disclose utilities data to Thomson Reuters, and subsequently to ICE, is a credit reporting agency.[370] Unfortunately, state privacy laws governing utilities are rife with these loopholes.[371]

- **Protect against *all* forms of disclosure.** The pathway of utilities data to ICE appears to have involved utilities voluntarily sharing (rather than selling) data to NCTUE, which in turn disclosed the data to Equifax, which then disclosed it to Thomson Reuters, which then disclosed it to ICE. Any law that prohibits only "sale" of that data rather than any form of disclosure or that does not address *re*sale or *re*disclosure of the data will fall short.
- **Be sure to protect customer addresses.** Many utility privacy laws focus on usage data. Unfortunately, some of those laws are unclear on whether addresses are protected.[372]

Connecticut privacy laws for gas companies offer a rare model for what an ideal statute might look like. The laws prohibit sharing with most third parties, closely limit the sharing that does occur, contain no blanket exceptions for credit reporting and protect against all forms of sharing—not just sale.[373]

Since Biden took office in early 2021, not much has changed about the scope of ICE surveillance. The agency's contracts for automated license plate readers, public records databases, face recognition technology, geolocation tracking and systems for data visualization and analysis have each been sustained, renewed and—in some cases—enlarged. Government policies and agreements that allow unchecked access to state databases still remain in place. Instead of dismantling what was inherited, Biden and Congress have maintained the immigrant surveillance state.

Before the election, the Biden campaign promised "sensible enforcement priorities," writing that "no one should be afraid to seek medical attention, go to school, their job, or their place of worship for fear of an immigration enforcement action."[374] Nearly one year later, Biden has taken some steps to reduce deportation, and the number of immigration arrests are at their lowest level in a decade.[375] But the administration has not yet used the considerable power of the executive to curtail the large-scale surveillance activities that ICE is engaging in every day, posing immediate risks to the safety and well-being of immigrant communities across the country.

Regardless of whether this particular administration uses surveillance to carry out four or 400,000 deportations this year, the existence of ICE's surveillance apparatus is itself a serious problem. Just as there is no statute or regulation explicitly authorizing the federal government to use mass surveillance to carry out deportations, there is no statute or regulation requiring the federal government to use the information gathered from such surveillance only for deportation. ICE surveillance should concern *you*, if not because you care about what may happen to immigrant communities or to public trust in government institutions or to privacy rights or to the balance of political power in our democracy, then because you care about what may happen to you and to the people you love if someone goes looking for you in the American dragnet.

APPENDIX

APPENDIX A: DETAILED PROCUREMENT ANALYSIS METHODOLOGY

A. DATA SOURCES

We surveyed all ICE contracts from January 2008 to September 2021—40,715 unique ICE contracts, totalling 108,873 transactions.[376] We downloaded ICE contract information from USAspending, the federal government's "official source for spending data."[377] In cases where ICE closed out a surveillance contract during our review period without spending more money on it, we excluded the contract.

There are some limitations with the reliability of this dataset.[378] For example, we do not have access to ICE's actual payouts.[379] We instead used USAspending data that tracks ICE's promises to spend funds, which are known as obligations.[380] For a closed contract, the total obligation should equal the real-world total ICE spent, but any open contract we reviewed might change in value. Furthermore, ICE provides its award spending data to the Federal Procurement Data System data, shared on USAspending, and agency mistakes can lead to misreported values.[381] Our data is current as of September 2021.[382]

B. METHODOLOGY

1. Overview

To identify and analyze ICE spending on surveillance technologies, we reviewed ICE award transactions listed on USAspending, the official source of federal spending information.[383] We identified ICE spending transactions that were likely for surveillance technologies and categorized them under six functionalities: geolocation, biometrics, data analysis, data brokers, government databases, and telecommunications.[384]

2. Identifying Surveillance Awards

We took two approaches to identifying surveillance awards. With the first approach, we started with a list of known surveillance tools and identified the ICE awards for those tools. With the second, we started with a set of ICE awards and looked into the ones that we suspected were for surveillance tools.

For our first approach, we assembled a list of known ICE surveillance vendors. We reviewed DHS/ICE's Privacy Impact Assessments (PIAs) and System of Record Notices (SORNs), which are some of the only public-facing documents that DHS makes available about its initiatives. We downloaded each PIA and SORN from the DHS/ICE website archive and read the documents for mentions of technologies covered in our functionality categories. Almost none of the PIAs or SORNs related to a particular contract but rather gave general information of existing ICE initiatives, projects or programs (e.g., LeadTrac, RAVEN, VISA, etc). We later connected initiatives and programs to certain contracts through alternative means. We also gathered the names of known ICE surveillance vendors from reports published by organizations like NILC, Mijente, TechInquiry and Top10VPN.[385] Lastly, we conducted keyword searches on search engines to identify names of other ICE surveillance programs and technologies.

For our second approach, we read through thousands of awards, flagging those that we suspected were related to surveillance functionalities.[386] We flagged awards for software that contained surveillance-related keywords (e.g., "biometric"), awards that were labeled under a possibly surveillance-related category (i.e., had a product code for "Information Retrieval") or had other fields that stood out. Then, we conducted online keyword searches of suspected surveillance contracts by their contract award number, the contracting companies, and the product or service provided. Those searches yielded company websites, media coverage and other information that helped us create a list of vendors and their surveillance products.

For any vendor that we identified as a surveillance vendor, we searched for its other ICE awards using its unique identifier, known as a DUNS number. We then reviewed each of the company's ICE awards, adding awards that matched our functionality categories. In cases where the vendor predominately sells technology falling under a functionality, we included all its ICE awards in our list. Moreover, since ICE may make more than one transaction for any award, whenever any spending transaction associated with an award that was likely surveillance related, we included the entire award in our final list.

3. Categorizing Awards

Many ICE awards were for technologies that provided multiple surveillance functionalities. For example, ICE uses some technologies that cut across categories, such as cell-site simulators that intercept communications (telecom interception) to track people (geolocation).[387] To decide on one functionality, we relied on a contract's labeled product or service category. Contract awards are assigned codes from the North American Industry Classification System (NAICS), a federal standard for classifying businesses,[388] and a Product Service Code (PSC), a Federal Procurement Data System (FPDS) standard for describing products and services.[389] When analyzing the contracts that fell under our functionality categories, we noticed patterns in how NAICS and PSC codes were assigned. For example, FPDS assigned the PSC "Web-based Subscription" for many of the ICE contracts we categorized as data brokers. As a result, we treated the PSC code "Web-based Subscription" as a signal that an award may best belong under the data broker functionality.

4. Automated Contract Analysis

Our manual review of ICE transactions yielded an initial dataset of ICE surveillance transactions, but the approach was time-intensive. To evaluate more contracts and to find contracts we missed on our first pass, we trained a model to identify contracts with a high probability of being surveillance related. We then manually reviewed each contract flagged by the model. The model complemented our manual review and flagged vendors, products and services that we did not identify in our first pass, for reasons such as irregular spelling in the award description. Using the model to aid our process also allowed us to analyze a significantly larger number of contracts and identify more instances of ICE surveillance spending.

5. Standardizing Contractor Names

- **Removing duplicates**

  ICE often fails to keep to a standard when recording the names of recipients. For example, ICE may record the City of Philadelphia, a contractor, as "philadelphia city of," "philadelphia, city of," or simply "Philadelphia." To standardize recipients' names, we used Open Refine's key collision algorithms to fuzzy-match and merge names.[390] We then supplemented that automatic merge with manual corrections.

- **Listing Contractors by Their Parent Company**

  Attributing a contract to a vendor is not always straightforward. Some companies obscure their ICE contracts by providing services through shell or child companies. Companies also change names or acquire or merge with smaller companies. To disentangle this web, we refer to award recipients by their present-day parent company names, current as of October 2021. To connect vendors to their parent companies, we used a vendor mapping developed by TechInquiry.[391]

6. Calculating Total Spending

Our report tracks the cumulative amount ICE spent over 12 years. Because awards frequently do not record cumulative spending on the contract, we recalculated the running total values of all surveillance awards. To compute the running sum of an award's value each year, we summed each award's yearly transactions—the "federal action obligations" in a running sum.

7. Limitations

a. Undercounting contracts

By erring on the side of caution, we may have undercounted ICE's surveillance contracts. Even after significant research, we were unable to make out whether some contracts had a categorizable surveillance purpose. For example, we excluded an ICE purchase of "scanners"[392] because the vendor sells both image scanners and fingerprint scanners.

b. Overcounting contracts

We also may have overcounted surveillance awards as a consequence of ICE's opaque reporting practices. ICE seldom discloses enough information to tell what the agency is purchasing or how its agents will use it. For example, ICE described one purchase as "required for electronic surveillance operations."[393] Not only is the award ambiguous, but the vendor sells many kinds of surveillance technologies, including those our report does not track.[394]

c. Third-party contractors

Our review does not disentangle providers from third-party vendors. For example, we listed a HART contract acquiring Amazon Web Services under the third-party vendor awarded the contract.[395]

APPENDIX B:
LIST OF ICE SURVEILLANCE CONTRACTS AND SPENDING CALCULATIONS

To view spreadsheet and calculations, please click here.

APPENDIX C:
SAMPLE RECORDS REQUESTS

A. SAMPLE REQUESTS TO STATE DMVS

1. Request to State DMVs for Records on Direct Searches and Nlets

[Date]
[Agency Address]

Re.: Records Request

Open Records Officer:

The Center on Privacy & Technology, a think tank based at the Georgetown University Law Center, is conducting a survey of departments of motor vehicles concerning agency information sharing practices.

Pursuant to [State Records Request Law and citation], we request the following records.

Records Requested

Please provide copies of the following records related to information sharing since 2015:

1. Requests received from U.S. Immigration and Customs Enforcement (ICE) seeking driver information, including requests for driver address information.

2. Agreements or memoranda of understanding signed with ICE or the U.S. Department of Homeland Security concerning access to driver information, including access to driver address information.

3. Policy documents, including guides, manuals, or other memoranda, containing procedures for using Nlets to share driver information, including driver address information.

This request is made on behalf of a not-for-profit organization whose mission is to advance the field of privacy and technology policy and to train law students from around the county in this field. Because of our not-for-profit status and the fact that this request is about a matter of public concern, we request a fee waiver. If such a waiver is denied, please inform us in advance if the cost will be greater than $50.

According to [State Records Request Law], a custodian of public records shall comply with a request [within X business days of receipt/timeframe specified in the law]. Please furnish responsive documents to [name and contact information] or:

[mailing address]

If you have any questions or if you cannot comply with this request in the statutory time period,or if this request is misdirected, please contact me at [contact information]. Thank you for your prompt attention to this matter.

Sincerely,
[name]

2. Request to State DMVs for Information about Database Access and Face Recognition Searches

[Date]
[Agency Address]

Re.: Records Request

Open Records Officer:

The Center on Privacy & Technology, a think tank based at the Georgetown University Law Center, is conducting a survey of state agency information sharing with data broker companies.

Pursuant to [State Records Request Law and citation], we request the following records.

Records Requested

Please provide copies of the following records related to facial recognition since 2015:

1. Requests received from the U.S. Department of Homeland Security, including its components U.S. Immigration and Customs Enforcement, and U.S. Customs and Border Protection, to run facial recognition searches or internal logs recording DHS facial recognition searches, and any materials sent to DHS in response to these requests and/or searches.
2. Agreements or memoranda of understanding signed with the U.S. Department of Homeland Security, including its components U.S. Immigration and Customs Enforcement and U.S. Customs and Border Protection, permitting the agency to run or request facial recognition searches.

Please provide copies of the following records related to information sharing with data broker companies since 2015:

3. Contract documents, including purchase orders, invoices, licensing agreements, non-disclosure agreements, or other procurement, service, or maintenance agreements with Giant Oak, IHS Markit (previously d/b/a RL Polk), Thomson Reuters (including its subsidiary, West Publishing Corporation) and RELX (including its subsidiary, LexisNexis).
4. Marketing materials advertising products or services offered by Giant Oak, IHS Markit (previously d/b/a RL Polk), Thomson Reuters (including its subsidiary, West Publishing Corporation) and RELX (including its subsidiary, LexisNexis).

This request is made on behalf of a not-for-profit organization whose mission is to advance thefield of privacy and technology policy and to train law students from around the county in this field. Because of our not-for-profit status and the fact that this request is about a matter of public concern, we request a fee waiver. If such a waiver is denied, please inform us in advance if the cost will be greater than $50.

According to [State Records Request Law], a custodian of public records shall comply with a request [within X business days of receipt/timeframe specified in the law]. Please furnish responsive documents to [name] at [contact information] or:

[mailing address]

If you have any questions or if you cannot comply with this request in the statutory time period, or if this request is misdirected, please contact me at [contact information]. Thank you for your prompt attention to this matter.

Sincerely,
[name]

B. SAMPLE REQUESTS TO UTILITY PROVIDERS

[Date]
[Agency Address]

Re.: Records Request

Open Records Officer:

The Center on Privacy & Technology, a think tank based at the Georgetown University Law Center, is conducting a survey of public utility companies about the sale or transfer of utility customer information to credit reporting agencies.

Pursuant to [State Records Request Law and citation], we request the following records.

Records Requested

Please provide copies of the following records since January 2015:

1. Contract documents, including purchase orders, invoices, licensing agreements, non-disclosure agreements, or other correspondence, procurement, service, or maintenance agreements with Equifax, Experian, and Transunion.

2. Policy documents, including guides, manuals or other memoranda, containing procedures for conducting a credit check or an identity verification on prospective or existing customers.

This request is made on behalf of a not-for-profit organization whose mission is to advance the field of privacy and technology policy and to train law students from around the county in this field. Because of our not-for-profit status and the fact that this request is about a matter of public concern, we request a fee waiver. If such a waiver is denied, please inform us in advance if the cost will be greater than $50.

According to [State Records Request Law], a custodian of public records shall comply with a request [within X business days of receipt/timeframe specified in the law]. Please furnish responsive documents to [name] at [contact information] or:

[mailing address]

If you have any questions or if you cannot comply with this request in the statutory time period, or if this request is misdirected, please contact me at [contact information]. Thank you for your prompt attention to this matter.

Sincerely,
[name]

APPENDIX D:
UTILITY PROVIDERS THAT HAVE LIKELY PARTICIPATED IN NCTUE

1. AT&T[396]
2. DIRECTV[397]
3. Verizon[398]
4. Sprint[399]
5. Citizens Communications Inc. (now Frontier)[400]
6. Broadwing Communications Inc.[401]
7. Dish Network[402]
8. American Electric Power[403]
9. Baltimore Gas & Electric[404]
10. Southern Company[405]
11. Georgia Power[406]
12. PSNC Energy (now North Carolina Gas)[407]
13. Scana Energy[408]
14. Piedmont Natural Gas[409]
15. Citizens Energy[410]
16. Nevada Energy[411]
17. Consumers Energy Company[412]
18. Miami-Dade County Water and Sewer Department[413]

Evidence also indicates that the following utility providers have not been or are no longer members of NCTUE:

1. Duke Energy[414]
2. Minnesota Energy Resource Corporation[415]

ACKNOWLEDGMENTS

This report would not be possible without the powerful research and advocacy of our friends and allies working to expose ICE's surveillance dragnet. We are deeply grateful for the work of organizations like CASA, the Immigrant Defense Project, Just Futures Law, the Legal Aid Justice Center, Make the Road, Mijente, the National Immigration Law Center, the National Immigrant Justice Center, the American Civil Liberties Union, Project South, Stop LAPD Spying Coalition and dozens of others.

Critical guidance and close reading of this report were provided by Professor David Vladeck, who serves as a faculty director for the Center. We also thank our outside reviewers, including Heidi Altman, Tanya Broder, Joan Friedland, McKenzie Funk, Anil Kalhan, Sarah Kim Pak, Julie Mao, Jack Poulson, Vasudha Talla and others who will remain anonymous, for lending valuable expertise throughout the drafting process. Reviewers do not necessarily agree with the subject matter of the report.

Furthermore, this report would not be possible without the entire team at the Center, who helped in countless ways: Katie Evans, Clare Garvie, Cynthia Khoo, Laura Moy, Korica Simon, Jameson Spivack and Serena Zets. We are also grateful to the Center's research assistants, practicum students and summer fellows, including Daniel Barabander and Romina Montellano Morales; Ashley Burke, Augusto Cividini, Dana Holmstrand, Jeremy Penn, Jesús Rodríguez and Natalie Tverdynin; our copy editor, Joy Metcalf; our design and web development firm, Rootid; and our report translator, María Ítaka of Sirena Peligro.

The Center on Privacy & Technology at Georgetown Law is supported by the Ford Foundation, the Kresge Foundation, the Open Society Foundations, the MacArthur Foundation, Luminate, the Media Democracy Fund, the Seldin/Haring-Smith Foundation and Georgetown University Law Center.

ENDNOTES

1. 148 Cong. Rec. S8046 (daily ed. Sept. 3, 2002) (remarks of Sen. Robert Byrd). Parts of this introduction draw from Alvaro Bedoya, *Watching Immigrants*, Harv. Nat'l Sec. J. (forthcoming 2022). Professor Bedoya has not reviewed or approved this report.

2. 147 Cong. Rec. S11059 (daily ed. Oct. 25, 2001) (Sen. Feingold as sole "nay" in 98-1 final vote).

3. *See* John Tierney, *THREATS AND RESPONSES: THE SENATE; Byrd, at 85, Fills the Forum With Romans and Wrath*, New York Times (Nov. 20, 2002) (describing Sen. Byrd as opposing the bill "virtually alone"); *Pork or Progress? Sen. Byrd Leaves Legacy*, CBS News & Associated Press, June 28, 2010 (on Sen. Byrd's legacy of appropriations for West Virginia).

4. *Id. See also* Temporary Relocation of the Coast Guard National Maritime Center (NMC), 72 Fed. Reg. 58,865 (Oct. 17, 2007) (move from Arlington, Va. to Kearneysville, W.Va.); Permanent Relocation of the Coast Guard National Maritime Center (NMC), 73 Fed. Reg. 12,747 (March 10, 2008) (move to Martinsburg, W.Va.).

5. *See generally* 148 Cong. Rec. S11358-113560 (daily ed. Nov. 19, 2002) (remarks of Sen. Byrd in opposition to the Homeland Security Act of 2002).

6. *Id* at S11359.

7. *Id.*

8. 148 Cong. Rec. S8045 (daily ed. Sept. 3, 2002).

9. *See* 148 Cong. Rec. S11359 (daily ed. Nov. 19, 2002) ("massive chamber of secrets"). *See also* 148 Cong. Rec. S8047-8048 (daily ed. Sept. 3, 2002) (discussing exemptions to the Federal Advisory Committee Act and the Freedom of Information Act, the lack of independence of the DHS Inspector General, and describing DHS privacy and civil rights officers as "advisers with no real investigative or enforcement power").

10. 148 Cong. Rec. S11359 (daily ed. Nov. 19, 2002).

11. That dragnet surveillance was a foreseeable consequence of the Homeland Security Act does not mean that the HSA should be read as authorizing the surveillance practices that this report describes. *See generally* Anil Kalhan, *Immigration Surveillance*, 74 Md. L. Rev. 1 (2014).

12. 148 Cong. Rec. S8046 (daily ed. Sept. 3, 2002).

13. 148 Cong. Rec. S11360 (daily ed. Nov. 19, 2002).

14. *Id.* at S11462.

15. *See* Tierney, *supra* note 3.

16. Personal Information, State and Local Agencies, Restrictions on Access: Hearing on H.B. 23 Before the Md. H. of Delegates Judiciary Committee (Jan. 27, 2021) (statement of Alex Vazquez of CASA), http://mgaleg.maryland.gov/mgawebsite/Committees/Media/false?cmte=jud&ys=2021RS&clip=JUD_1_27_2021_meeting_2&url=https%3A%2F%2Fmgahouse.maryland.gov%2Fmga%2Fplay%2Fb0a7b427-6719-4e6b-ac39-b03a4b8bd423%2F%3Fcatalog%2F03e481c7-8a42-4438-a7da-93ff74bdaa4c%26playfrom%3D2354420 (at 46:33, "certain death").

17. Erin Cox, *Gov. Hogan opposed to ending ICE's warrantless access to driver's license database*, Washington Post (Feb. 27, 2020), https://www.washingtonpost.com/local/md-politics/hogan-opposes-blocking-ice-from-drivers-licenses/2020/02/27/3e23bbcc-5903-11ea-9000-f3cffee23036_story.html.

18. *See id.*

19. *See* Drew Harwell, *ICE has run facial recognition searches on millions of Maryland drivers*, Washington Post (Feb. 26, 2020), https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers/; *Kevin Rector, ICE has access to Maryland driver's license records. State lawmakers want to limit it*, Baltimore Sun (Feb. 26, 2020), https://www.baltimoresun.com/politics/bs-md-pol-ice-mva-bill-20200227-rsgqqajmwne4hollsz4svgpa6m-story.html#:~:text=State%20lawmakers%20want%20to%20limit%20it.,-By%20Kevin%20Rector&text=Armed%20with%20new%20evidence%20that,their%20access%20in%20the%20future. The term "standard" license is used in Maryland to differentiate these identity documents from licenses that comply with the requirements of the federal REAL ID Act, which requires verification of immigration status. Maryland's face recognition repository, the Maryland Image Recognition System, or MIRS, includes all driver photos regardless of the kind of license. Bureau of Transp. Stat., U.S. Dep't of Transp., Maryland: Transportation by the Numbers 2 (2020), https://www.bts.gov/sites/bts.dot.gov/files/states2020/Maryland.pdf (4.4 million licensed drivers in 2018).

20. *See* Cox, *supra* note 17.

21. *See* Letter from Kevin Combs, Md. Dep't of Public Safety and Corr. Servs. to Sen. Susan C. Lee et al., Nov. 21, 2019 (explaining, in response to a query from legislators regarding the number of such searches, that Maryland does not have access to users' search results and instead offering the number of "sessions [that] were saved" by ICE users in 2018 and 2019).

22. *See generally infra* Section II.

23. *See* Vasudha Talla, *Documents Reveal ICE Using Driver Location Data from Local Police Departments,* ACLU NorCal (March 13, 2019), https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data ("Vigilant draws its license plate information from the 'most populous 5 metropolitan areas' in the country, corresponding to almost 60 percent of the U.S. population.").

24. *See generally infra* Section III.

25. *See generally infra* Section IV.

26. *See, e.g.,* U.S. Immigration and Customs Enforcement, *ICE announces results of latest operations targeting criminal aliens* (Sept. 1, 2020), https://www.ice.gov/news/releases/ice-announces-results-latest-operations-targeting-criminal-aliens ("[b]y focusing our efforts on perpetrators of crimes against people, we're able to remove these threats from our communities and prevent future victimization from occurring. Through our targeted enforcement efforts, we are eliminating the threat posed by these criminals, many of whom are repeat offenders.").

27. As a young man, Robert Byrd organized a chapter of the Ku Klux Klan. As a young senator, he made his name opposing civil rights laws. As an older Senator, however, he was deeply embarrassed by this and became a staunch proponent of the Voting Rights Act and other key civil rights laws. This grace, unfortunately, never extended to people like Mr. Hernandez. In fact, Senator Byrd spoke heatedly against efforts to give undocumented people a path to citizenship. In remarks on the floor of the Senate during an immigration debate, he warned that "any one" of the "undocumented, unchecked aliens . . . could be a potential terrorist." Regardless of his history or his motives, however, Senator Byrd's warning has proved frighteningly accurate. 109 Cong. Rec. S2794 (daily ed. Apr. 4, 2006) (statement of Sen. Robert Byrd).

28. *See generally* Anil Kalhan, *Immigration Surveillance*, 74 Md. L. Rev. 1 (2014).

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

30. *See* Drew Harwell, *Utility giants agree to no longer allow sensitive records to be shared with ICE*, Washington Post (Dec. 8, 2021), https://www.washingtonpost.com/technology/2021/12/08/utility-data-government-tracking/; Letter from Ron Wyden, U.S. Senator to The Hon. Rohit Chopra, Director, Consumer Financial Protection Bureau 1 (Dec. 8, 2021), https://www.washingtonpost.com/context/sen-wyden-letter-to-cfpb-on-sale-of-americans-utility-data/20df9dd1-bab1-4b2d-96f3-3b288c6d1905/; @JustFuturesLaw, Twitter (Dec. 8, 2021), https://twitter.com/JustFuturesLaw/status/1468590605668425729.

31. *See* Letter from Ron Wyden, U.S. Senator to The Hon. Rohit Chopra, Director, Consumer Financial Protection Bureau 2 (Dec. 8, 2021), https://www.washingtonpost.com/context/sen-wyden-letter-to-cfpb-on-sale-of-americans-utility-data/20df9dd1-bab1-4b2d-96f3-3b288c6d1905/?itid=lk_inline_manual_9.

32. Frank Bajak, *Groups demand end to info-sharing on asylum-seeking children*, Associated Press (Nov. 28, 2018), https://apnews.com/article/immigration-north-america-us-news-ap-top-news-international-news-81787a5897704a0cae82a9ceb0eea271.

33. Consolidated Appropriations Act of 2019, H.J.Res.31, 116th Cong. § 224 (2019), https://www.congress.gov/bill/116th-congress/house-joint-resolution/31/text.

34. U.S. Department of Homeland Security, *HHS and DHS Joint Statement on Termination of 2018 Agreement* (Mar. 12, 2021), https://www.dhs.gov/news/2021/03/12/hhs-and-dhs-joint-statement-termination-2018-agreement.

35. Although Maryland Governor Larry Hogan vetoed the bills in May 2021, the Maryland General Assembly overrode the veto in December of that year. Clara Garcia, *Maryland General Assembly Overrides Hogan's Vetoes of Immigration Bills*, NBC Washington (Dec. 8, 2021), https://www.nbcwashington.com/news/local/maryland-general-assembly-overrides-hogans-vetoes-of-immigration-bills/2904771/.

36. For example, the Criminal Alien Program (CAP) sends ICE officers into jails to interview detained people to determine if they may be deportable. CAP officers do not distinguish between people detained pre-trial and people who have been convicted of an offense. In fact, a significant number of people removed under CAP did not have criminal convictions. *See* Guillermo Cantor, Mark Noferi & Daniel E. Martinez, *Enforcement Overdrive: A Comprehensive Assessment of ICE's Criminal Alien Program*, American Immigration Council 2 (Nov. 1, 2015), https://www.americanimmigrationcouncil.org/sites/default/files/research/enforcement_overdrive_a_comprehensive_assessment_of_ices_criminal_alien_program_final.pdf ("Out of more than half a million CAP removals that took place between FY 2010 and FY 2013, ICE classified the largest share (27.4 percent) as not "definite criminals"—i.e., ICE recorded no criminal conviction.").

37. U.S. Immigration and Customs Enforcement, U.S. Department of Homeland Security, *Secure Communities: A Comprehensive Plan to Identify and Remove Criminal Aliens* 1-2 (2009), https://www.ice.gov/doclib/foia/secure_communities/securecommunitiesstrategicplan09.pdf (Through the deployment and use of the biometric-based identification systems, all persons booked into custody will be automatically checked for their immigration status as well as prior criminal history.)

38. This report distinguishes between "law enforcement," and "non-law enforcement" data, but because of the increasing interoperability of databases and networks across all levels and branches of government, as a practical matter it may make more sense to begin thinking of *all* data as potentially law enforcement data.

39. *See generally* Erika Lee, At America's Gates: Chinese Immigration During the Exclusion Era 1882-1943 (2003); Kelly Lytle Hernández, *The Crimes and Consequences of Illegal Immigration: A Cross-Border Examination of Operation Wetback, 1943 to 1954*, 37 Western Historical Quarterly 421, 426-443 (2006).

40. Patrisia Macías-Rojas, *Immigration and the War on Crime: Law and Order Politics and the Illegal Immigration Reform and Immigrant Responsibility Act of 1996*, 6 J. on

Migration and Security 1, 5 (2018) ("Overcrowded prisons and detention centers prompted legislators to introduce measures to deport 'alien felons' in order to free up beds … Mandatory minimum sentencing fueled overcrowding; yet Congress defined the problem as a bed space shortage … lawmakers and officials testified before Congress that they could 'almost solve our prison overcrowding if the Federal Government does what it needs to do to get these criminals and deport them.'"); Immigration Reform and Control Act of 1986, Pub. L. No. 99-603, § 701,100 Stat. 3445 (requiring the Attorney General "in the case of an alien who is convicted of an offense which makes the alien subject to deportation . . . [to] begin any deportation proceeding as expeditiously as possible after the date of the conviction."); William A. Kandel, Cong. Rsch. Serv., R44627, Interior Immigration Enforcement: Criminal Alien Programs 23 (2016) (discussing how the INS executed its congressional mandate by establishing the Institutional Removal Program (IRP) and the Alien Criminal Apprehension Program (ACAP) for the targeted deportation of criminal immigrants).

41. In 1988, Congress created a category of offenses known as aggravated felonies; at their creation, these included only crimes like murder or firearms and drug trafficking, but the definition of aggravated felony was broadly expanded by Congress between 1990 and 1996 with passage of a series of measures, most notably including the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA), to include other grounds for deportation, with retroactive application. Kandel, *supra* note 40 at 12; Immigration Act of 1990, Pub. L. No. 101-649, 104 Stat. 4978 (1990); Immigration and Nationality Technical Correction Act of 1994, Pub. L. No. 103-416, 108 Stat. 4305 (1994); Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1214 (1996); Illegal Immigrant Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, Div. C, 110 Stat. 3009–546 (1996). *See also* Cong. Rsch. Serv., RL32480, Immigration Consequences of Criminal Activity 3-5 (2009).

42. *See* Douglas S Massey & Karen A. Pren, *Unintended Consequences of US Immigration Policy: Explaining the Post-1965 Surge from Latin America*, 38 Popul. Dev. Rev. 8 (July 30, 2021) ("Prior to the mid-1990s the annual number of deportations had not exceeded 50,000 for decades, but with the passage of the 1996 legislation this threshold was breached and by the turn of the century deportations were running at just under 200,000 annually.").

43. *See* Walter Ewing, Daniel E. Martinez, Ruben G. Rumbaut, *The Criminalization of Immigration in the United States*, American Immigration Council 10–19 (July 13, 2015), https://www.americanimmigrationcouncil.org/research/criminalization-immigration-united-states.

44. *See* Marc R. Rosenblum & William A. Kandel, Cong. Rsch. Serv., R42057, Interior Immigration Enforcement: Programs Targeting Criminal Aliens 11-17 (2012); *id.* at 16 ("More than half (32 of 57) of the §287(g) agreements identified in December 2012 are jail enforcement agreements."); *The 287(g) Program: An Overview*, American Immigration Council (July 8, 2012), https://www.americanimmigrationcouncil.org/research/287g-program-immigration ("As of June 2020, there were 76 active jail enforcement model MOAs in 21 states and 65 warrant service officer model MOAs in nine states.").

45. U.S. Immigration and Customs Enforcement, Secure Communities: A Comprehensive Plan to Identify and Remove Criminal Aliens 1-2 (2009), https://www.ice.gov/doclib/foia/secure_communities/securecommunitiesstrategicplan09.pdf (Through the deployment and use of the biometric-based identification systems, all persons booked into custody will be automatically checked for their immigration status as well as prior criminal history.)

46. Julia Preston, *States Resisting Program Central to Obama's Immigration Strategy,* New York Times (May 5, 2011), https://www.nytimes.com/2011/05/06/us/06immigration.html ("The states' objections are setting up a confrontation with the Department of Homeland Security, whose secretary, Janet Napolitano, has said that Secure Communities is mandatory and will be extended to all jurisdictions in the country by 2013.").

47. U.S. Immigration and Customs Enforcement, Secure Communities (Feb. 9, 2021), https://www.ice.gov/secure-communities ("ICE completed full implementation of Secure Communities to all 3,181 jurisdictions within 50 states, the District of Columbia, and five U.S. Territories on January 22, 2013.").

48. *See* Letter from Jeh Charles Johnson, Secretary, U.S. Department of Homeland Security to Thomas S. Winkowski, Acting Director, U.S. Immigration and Customs Enforcement et al. 2–3 (Nov. 20, 2014), https://www.dhs.gov/sites/default/files/publications/14_1120_memo_secure_communities.pdf ("Accordingly, I am directing U.S. Immigration and Customs Enforcement (ICE) to discontinue Secure Communities. ICE should put in its place a program that will continue to rely on fingerprint-based biometric data submitted during bookings by state and local law enforcement agencies to the Federal Bureau of Investigation for criminal background checks . . . This new program should be referred to as the 'Priority Enforcement Program' or 'PEP.'").

49. Exec. Order No. 13,768, 82 Fed. Reg. 8799 (Jan. 25, 2017).

50. Exec. Order No. 13,993, 86 Fed. Reg. 7051 (Jan. 25, 2021).

51. In fiscal year 2011, the number of removals under S-Comm was 79,726. TRAC, *Removals under the Secure Communities Program* (2019), https://trac.syr.edu/phptools/immigration/secure/. In total, ICE ERO removed 396,906 individuals during fiscal year 2011. U.S. Immigration and Customs Enforcement, *FY 2011: ICE announces year-end removal numbers, highlights focus on key priorities* (Oct. 17, 2011), https://www.ice.gov/news/releases/fy-2011-ice-announces-year-end-removal-numbers-highlights-focus-key-priorities#:~:text=Overall%2C%20in%20FY%202011%20ICE's,of%20criminals%20since%20FY%202008.

52. Hillel R. Smith, Cong. Rsch. Serv., LSB10375, Immigration Detainers: Background and Recent Legal Developments 1 (2020).

53. These figures may also reflect the fact that removal statistics began including border deportations. *See* Bethania Palma & David Mikkelson, *Were More People Deported Under the Obama Administration Than Any Other?*, Snopes (Oct. 20, 2016) https://www.snopes.com/fact-check/obama-deported-more-people/.

[54] *Table 39. Aliens Removed or Returned: Fiscal Years 1892 to 2017*, Department of Homeland Security (Apr. 9, 2019), https://www.dhs.gov/immigration-statistics/yearbook/2017/table39.

[55] *See* Anil Kalhan, *Immigration Policing and Federalism Through the Lens of Technology, Surveillance, and Privacy*, 74 Ohio St. L.J. 1130-31 (2013).

[56] *See* National Immigration Law Center, Nlets: Questions and Answers 13 (Nov. 2020), https://www.nilc.org/wp-content/uploads/2020/11/Nlets-Q-and-A.pdf ("The NCIC is an FBI database containing, according to the FBI, 'an electronic clearinghouse of crime data that can be tapped into by virtually every criminal justice agency nationwide, 24 hours a day, 365 days a year.' Despite the FBI's designation of NCIC as a criminal database, it also includes civil immigration records, such as records of prior removal/deportation orders.").

[57] In *Chae Chan Ping v. United States*, the Supreme Court established deference to the executive and the legislative branches on matters of immigration enforcement, forming the basis of the plenary power doctrine. *See generally* Natsu Taylor Saito, *The Enduring Effect of the Chinese Exclusion Cases: The "Plenary Power" Justification for Ongoing Abuses of Human Rights*, 10 Asian Am. L. J. (2003).

[58] *See* U.S. Department of Homeland Security, Office of the Inspector General, OIG-07-34, An Assessment of United States Immigration and Customs Enforcement's Fugitive Operations Teams 3 (2007) ("The Office of Detention and Removal Operations deportation officers have always apprehended fugitive aliens on an ad hoc basis, but teams were not exclusively devoted to this task."). Two efforts to change this in the late 1990s did not succeed. *Id.* ("The plan called for the creation of "abscondee removal teams," and the 1996 Appropriation Bill provided funding for these new positions . . . the positions were absorbed into day-to-day INS detention and deportation operations . . . [another] initiative called for the creation of Fugitive Operations Teams . . . but no teams were ever established."); U.S. Department of Homeland Security, Office of the Inspector General, OIG-05-50, Review of the Immigration and Customs Enforcement Compliance and Enforcement Unit 6 (Sept. 2005) ("In an effort to reduce the number of illegal aliens residing in the United States who had violated the terms of certain types of visas, ICE established the [Compliance Enforcement Unit (CEU)] in June 2003"); *Visa Overstays: Can They Be Eliminated?: Hearing Before the House Committee on Homeland Security*, 111th Cong. 11 (2010) (statement of John T. Morton, Assistant Secretary, U.S. Immigration and Customs Enforcement, Department of Homeland Security) (CEU was "the first national program dedicated to the enforcement of nonimmigrant visa violators.").

[59] Memorandum from Michael R. Bromwich, Inspector General, Department of Justice, to Doris Meissner, Commissioner, Immigration and Naturalization Service (Sep. 4, 1997), https://oig.justice.gov/sites/default/files/legacy/reports/INS/e9708/i9708p1.htm ("Historically, the overstay issue has not been a primary consideration in the formulation and execution of immigration policy.").

[60] U.S. Department of Justice, Office of the Inspector General, Rep. No. I-96-03, Immigration And Naturalization Service Deportation of Aliens After Final Orders Have Been Issued 13 (Mar. 1996), https://oig.justice.gov/reports/INS/e9603/index.htm ("Nondetained aliens who do not comply with a surrender request are rarely pursued actively . . . [I]t has been national policy for [INS] Investigations not to work abscondee cases, unless an abscondee comes to their attention as part of a broader investigation."). This did not seem to trouble immigration officials at the time. In 1994, when INS commissioner Doris Meissner was interviewed on the subject by the *Times*, she would say that "[w]e are not successful where removal is concerned, by and large." Deborah Sontag, *Porous Deportation System Gives Criminals Little to Fear*, New York Times (Sept. 13, 1994), https://www.nytimes.com/1994/09/13/us/porous-deportation-system-gives-criminals-little-to-fear.html.

[61] U.S. Department of Justice, Office of the Inspector General, Rep. No. I-2003-004, The Immigration and Naturalization Service's Removal of Aliens Issued Final Orders iv n.7 (Feb. 2003), https://oig.justice.gov/reports/INS/e0304/final.pdf ("The INS defines absconders as aliens with unexecuted final orders of removal and whose whereabouts are unknown. Most absconders are nondetained aliens.").

[62] U.S. Department of Justice, Office of the Inspector General, Rep. No. I-96-03, *supra* note 60.

[63] Alien Registration Act, Pub. L. No. 76-670,54 Stat. 670 (1940). *See* U.S. Gov't Accountability Office, GAO-03-188, Homeland Security: INS Cannot Locate Many Aliens Because It Lacks Reliable Address Information (summarizing changes in the law from 1940-2002, all of which maintained some form of requirement to update address). Requirements to update addresses are still current today. U.S. Citizenship and Immigration Services, *Change of Address*, https://egov.uscis.gov/coa/displayCOAForm.do ("Except for those exempted, all aliens in the U.S. are required to report any change of address or new address.").

[64] *See* U.S. Gov't Accountability Office, GAO-03-188, *supra* note 63, at 12-13 (poor compliance and enforcement with address reporting requirements); Memorandum from Michael R. Bromwich to Doris Meissner, *supra* note 59, at 1 ("However, [Non-Immigrant Information System] data is inadequate to enable INS to identify, locate, and arrest individual overstays.").

[65] U.S. Department of Justice, Office of the Inspector General, Rep. No. I-96-03, *supra* note 60, at 13.

[66] National Commission on Terrorist Attacks upon the United States, The 9/11 Commission Report 384 (2004).

[67] Kevin Lapp, *Pressing Public Necessity: The Unconstitutionality of the Absconder Apprehension Initiative*, 29 N.Y.U. Rev. L. & Soc. Change 573, 574–75 (2005) ("The result was an egregious, government directed roundup consisting overwhelmingly of Muslim and Arab individuals.").

[68] Memorandum from Larry Dean Thompson, Deputy Attorney General, Department of Justice, to Commissioner, Immigration and Naturalization Service et al. (Jan. 25, 2002), https://www.shusterman.com/pdf/absconderapprehensioninitiative.pdf; U.S. Department of Homeland Security, Office of the Inspector General, OIG-07-34, *supra* note 58, at 1.

[69] Kevin Lapp, *supra* note 67, at 583–85.

[70] Memorandum from Larry Dean Thompson, *supra* note 68.

71. U.S. Gov't Accountability Office, GAO-03-188, *supra* note 63, at 13 ("Of the estimated 314,000 aliens with final orders of removal still at large in the United States, INS identified 5,046 who were from countries in which there has been an Al Qaeda terrorist presence or activity. To locate and apprehend these aliens, INS, in cooperation with the FBI, the Foreign Terrorist Tracking Task Force, and U.S. Attorneys, used INS address data and supplemented these data with address information from public source databases. According to a senior INS official, as of June 24, 2002, 4,334, or 86 percent, of the 5,046 alien absconders had not been apprehended, while 712, or 14 percent, had been apprehended.").

72. *Id.* at 12–16 (The AAI example "illustrate[s] one inherent limitation of an address reporting requirement that relies on self reporting, as the reliability and completeness of the address information is dependent on the extent to which aliens comply with the reporting requirement. . . . Lack of publicity, no enforcement of penalties for not filing change of address notifications, and inadequate processing procedures and controls explain in part why INS's alien address information is unreliable."); *id.* at 25 (recommending "purchasing address information from commercially available sources").

73. U.S. Department of Homeland Security, Office of the Inspector General, OIG-07-34, An Assessment of United States Immigration and Customs Enforcement's Fugitive Operations Teams 3–4 (2007).

74. *Id.* at 41–42.

75. U.S. Department of Homeland Security, Office of the Inspector General, OIG-05-50, Review of the Immigration and Customs Enforcement's Compliance Enforcement Unit 6 (Sept. 2005); *Industry Day*, National Security Investigations Division, Department of Homeland Security 9 (Oct. 31, 2017), https://www.brennancenter.org/sites/default/files/Industry%20Day%20Presentation_0.pdf (referencing CEU's rebranding as CTCEU).

76. This number does not include the cost of programs paid for by other agencies and used by ICE.

77. Mobilcomm, Vigilant Solutions (last visited Jan. 13, 2022), https://www.mobilcomm.com/vigilant-solutions/.

78. *See* Letter from U.S. Immigration and Customs Enforcement to Vasudha Talla 75 (Jul. 13, 2017), https://www.documentcloud.org/documents/5767094-ALPR-documents-from-ICE-FOIA.html.

79. *Id.*

80. *Id.* at 76-77; U.S. Census Bureau, Annual Estimates of the Resident Population for Metropolitan Statistical Areas in the United States and Puerto Rico: April 1, 2010 to July 1, 2019, https://www2.census.gov/programs-surveys/popest/tables/2010-2019/metro/totals/cbsa-met-est2019-annres.xlsx. *See also* Vasudha Talla, *Documents Reveal ICE Using Driver Location Data from Local Police Departments,* ACLU NorCal (March 13, 2019), https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data.

81. *See* Letter from U.S. Immigration and Customs Enforcement to Vasudha Talla 83 (Jul. 13, 2017), https://www.documentcloud.org/documents/5767094-ALPR-documents-from-ICE-FOIA.html.

82. Russell Brandom, *Exclusive: 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.

83. Charles Levinson, *Through apps, not warrants, 'Locate X' allows federal law enforcement to track phones*, Protocol (Mar. 5, 2020), https://www.protocol.com/government-buying-location-data ("In September 2018, ICE officials signed a one-year, $1.1 million contract with Babel Street. The deal included Locate X, according to a former Babel Street employee. Last August, ICE signed a fresh five-year deal worth up to $6.5 million with Babel Street for 'data subscription services,' records show."); USAspending, Contract Summary: THUNDERCAT TECHNOLOGY, LLC, https://www.usaspending.gov/award/CONT_AWD_70CMSD18FR0000226_7012_HSHQDC13D00002_7001.

84. USAspending, Contract Summary: L-1 IDENTITY SOLUTIONS, INC., https://www.usaspending.gov/award/CONT_AWD_HSCECR08P00090_7012_-NONE-_-NONE-/

85. USAspending, Contract Summary: CLEARVIEW AI, INC., https://www.usaspending.gov/award/CONT_AWD_70CMSD20P00000130_7012_-NONE-_-NONE-; Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, New York Times (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

86. Thomson Reuters, THE SMARTER WAY TO GET YOUR INVESTIGATIVE FACTS STRAIGHT, https://www.thomsonreuters.com/content/dam/openweb/documents/pdf/legal/fact-sheet/clear-brochure.pdf (Retrieved Nov. 26, 2021); Thomson Reuters, CLEAR for know your vendor, https://legal.thomsonreuters.com/en/products/clear-investigation-software/know-your-vendor (last visited Nov. 26, 2021).

87. USAspending, Contract Summary: WEST PUBLISHING CORPORATION, https://www.usaspending.gov/award/CONT_AWD_HSCEMD17F00008_7012_GS02F026DA_4732.

88. Sam Biddle, *LexisNexis to Provide Giant Database of Personal Information to ICE*, Intercept (Apr. 2, 2021), https://theintercept.com/2021/04/02/ice-database-surveillance-lexisnexis.

89. A total of 16 states and the District of Columbia have enacted laws allowing unauthorized immigrants to obtain driver's licenses: California, Colorado, Connecticut, Delaware, Hawaii, Illinois, Maryland, Nevada, New Jersey, New Mexico, New York, Oregon, Utah, Vermont, Virginia and Washington. National Conference of State Legislatures, States Offering Driver's Licenses to Immigrants (Aug. 9, 2021), https://www.ncsl.org/research/immigration/states-offering-driver-s-licenses-to-immigrants.aspx. Out of these 17 jurisdictions, 5 of them enable ICE to electronically query driver's license information for immigration enforcement purposes: Colorado, Delaware, New Mexico, Utah and Washington. *See infra* Section II.

90. Although ICE wiretaps fall under Title III of the Wiretap Act, which requires a warrant to intercept "wire, oral, or electronic communications," the list of predicate crimes make it easier for ICE to obtain this information. *See, e.g.,*

Jennifer S. Granick et al., Mission Creep and Wiretap Act 'Super Warrants': A Cautionary Tale, 52 Loy. L.A. L. Rev. 431 (2019); *ICE is Paying Millions to Surveillance Company to Spy on People's Communications*, Privacy International (May 24, 2019), https://privacyinternational.org/news-analysis/2995/ice-paying-millions-surveillance-company-spy-peoples-communications.

91. Privacy International, *supra* note 90; 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.

92. Sole Source Justification Request, Williamson County Purchasing Department (May. 11, 2021), https://agenda.wilco.org/docs/2020/COM/20200721_1545/24566_Sole_Source_Justification__Agenda.pdf; PLX Free Trial, PENLiNK, http://go.penlink.com/plxtrial (last visited Nov. 27, 2021); 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.

93. *See* U.S. Department of Homeland Security, DHS/ICE/PIA-045, Privacy Impact Assessment for ICE Investigative Case Management 7 (Jun. 16, 2016), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf ("TLS contains telecommunications information initially input into ICE's Pen-Link software, which serves as a field-level investigative tool enabling HSI to perform local analysis within a single case or across multiple cases. Pen-Link contains a custom module built for ICE that standardizes the telecommunications records from the myriad formats used by service providers and is used to export and import data files in a specific format that is used by TLS. TLS links related data by using key identifiers for this telecommunications information, such as phone numbers. This linkage enables HSI agents to discern relationships that may help to identify the parties of criminal networks under investigation, promoting further investigation and contributing to the eventual disruption or dismantling of the criminal organizations.").

94. *See* OIG-07-34, An Assessment of United States Immigration and Customs Enforcement's Fugitive Operations Teams (Mar. 2007), https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/OIG_07-34_Mar07.pdf at 25, 27 (FOSC "will assist the Office of Detention and Removal Operations process data received through negotiated information-sharing agreements in several ways."). *Id.* ("Under those agreements, ICE provides data on fugitive aliens from the Deportable Alien Control System to those agencies. The agencies then reconcile the data provided with information in their respective databases and any matches found are shared with ICE.").

95. Memorandum of Agreement among the Office of Refugee Resettlement of the U.S. Department of Health and Human Services and U.S. Immigration Enforcement and U.S. Customs and Border Protection of the U.S. Department of Homeland Security Regarding Consultation and Information Sharing in Unaccompanied Alien Children Matters (Apr. 13, 2018), https://www.texasmonthly.com/wp-content/uploads/2018/06/Read-the-Memo-of-Agreement.pdf; *See* 8 U.S.C § 1232(c)(2)(A) (2012) ("Subject to section 279(b)(2) of title 6, an unaccompanied alien child in the custody of the Secretary of Health and Human Services shall be promptly placed in the least restrictive setting that is in the best interest of the child.").

96. Anil Kalhan, *Immigration Surveillance*, 74 Md. L. Rev. 27 (2014).

97. *Id.* at 2.

98. Ana Muñiz, *Secondary ensnarement: Surveillance systems in the service of punitive immigration enforcement*, Punishment & Soc'y 2 (Feb. 11, 2020).

99. *See, e.g.*, 8 U.S.C. § 1357.

100. Anil Kalhan, *Immigration Policing and Federalism Through the Lens of Technology, Surveillance, and Privacy*, 74 Ohio St. L.J. 1105, 1130 (2013).

101. *Id.* at 1130.

102. Nina Shapiro, *Washington state regularly gives drivers' info to immigration authorities; Inslee orders temporary halt*, Seattle Times (Jan. 11, 2018), https://www.seattletimes.com/seattle-news/times-watchdog/washington-state-regularly-gives-drivers-info-to-immigration-authorities-inslee-orders-temporary-halt.

103. Joseph O'Sullivan, *Inslee signs order limiting Washington state's help in enforcing Trump's immigration policies*, Seattle Times (Feb. 23, 2017), https://www.seattletimes.com/seattle-news/politics/inslee-signs-order-limiting-states-involvement-in-immigration-enforcement.

104. *Id.*

105. Washington State Department of Licensing, https://info.dol.wa.gov.

106. Shapiro, *supra* note 102 ("20 to 30 times a month, a state agency has been giving residents' personal information to federal immigration-enforcement officers—information used to arrest and deport people in keeping with the president's policies.").

107. H.B. 1444, 1993 Reg. Sess. (Wa. 1993) (authorizing the issuance of a license based upon state residency, among other requirements, without consideration of immigration status).

108. Washington Governor Jay Inslee, *Inslee statement on Licensing policy changes to protect personal information of immigrants and refugees* (Jan. 15, 2018), https://www.governor.wa.gov/news-media/inslee-statement-licensing-policy-changes-protect-personal-information-immigrants-and.

109. Washington State Department of Licensing, *DOL takes immediate steps to stop disclosure of information to federal immigration authorities*, Washington State Department of Licensing: DOL Blog (Jan. 15, 2018), https://licensingexpress.wordpress.com/2018/01/15/dol-takes-immediate-steps-to-stop-disclosure-of-information-to-federal-immigration-authorities.

110. DOL Data Sharing, Presentation to the Joint Transportation Committee, Washington State Department of Licensing (May 17, 2018), https://leg.wa.gov/JTC/Meetings/Documents/Agendas/2018%20Agendas/May%202018%20Meeting/DOL.pdf.

111. Washington State Department of Licensing, DAPS ICE User List, Apr. 28, 2017, WADMV_002329 (28 ICE users with DAPS access).

112. Washington State Department of Licensing, ICE ERO DAPS Agency Access Request (Dec. 3, 2013), WADMV_002666 ("Access is neeed [sic] to verify and confirm identities of individuals that are ordered removed from the United States, insluding [sic] those that have re-entered the United States illegally after being deported and individuals [sic] with cimrinal [sic] convictions that pose a threat to society. With the provided information of both driver and vehicle access, it would make it easier to conduct survillance [sic] and apprehend these individuals.").

113. DAPS audit log in its original format for all license-plate searches made by users from U.S. Immigration and Customs Enforcement in Pacific County between January 1, 2016 and January 1, 2018, https://ln5.sync.com/dl/6bdb633a0/ji2h5a3z-q9aap7pp-p8rpxjyh-c9dxf4hz/view/default/10593125090006.

114. Drew Harwell, *FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches*, Washington Post (Jul. 7, 2019), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.

115. Washington State Department of Licensing, DAPS Contract Terminations, 2017/2018, WADMV_002563 ("US Dept. of Homeland Security, Immigration & Customs Enforcement / ERO Fugitive Ops Unit . . . TERMINATED - NO OPTION to sign a new contract . . . US Dept. of Homeland Security, Immigration & Customs Enforcement/DRO Yakima . . . TERMINATED - NO OPTION to sign a new contract . . . US Dept. of Homeland Security, Immigration & Customs Enforcement, Homeland Security Investigations . . . TERMINATED - WITH OPTION to sign a new contract").

116. Frank Bajak, *Washington DOL denies giving ICE access to facial recognition searches*, KING-TV (Jul. 8, 2019), https://www.king5.com/article/news/ice-used-facial-recognition-to-search-state-drivers-license-databases/507-3f905179-519d-4acc-bb92-a5ae6aaea275.

117. Washington State Department of Licensing, Email from Jeff Oehlerich, Investigator 3 to Border Patrol Agent (Mar. 30, 2017), WADMV_001963-WADMV_001964 ("In the past, we have been very liberal in accepting the justification of 'criminal investigation' from requestor's [sic] and not required more specific descriptions. This changed about a month ago as the result of an executive order from the governor. We now require the title or statutory citation of the actual crime being investigated before we will provide a photo. This is at the direction of our executive leadership team. The wording that authorizes a photo for verifying identity when an officer may request identification, was added to allow officers to have direct access to photos in their patrol cars and sue them when they stop a violator who does not have ID. The WSP ACCESS system does have a specific query format where they can get a photo when they request a driver's check. The actual method of making the query depends on the interface program the agency uses, so I don't know what limitations or requirements each department may have. I would suggest contacting one of the agencies in your local area to see if thaye [sic] can assist.").

118. Washington State Police, Response to Harrison Rudolph (Jan. 4, 2021), WANLETS_000007 ("Number of queries: 2015 - 398710, 2016 - 393666, 2017 - 539638, 2018 - 997069, 2019 - 1129711, 2020 - 680847").

119. Washington Department of Licensing, Response to Harrison Rudolph (Feb. 5, 2021), WADMV_3269-WADMV_3274; Washington Department of Licensing, Response to Harrison Rudolph (Feb. 5, 2021), WADMV_003275-WADMV_003281.

120. Washington Department of Licensing, Requests via NLETS and WSP access from Federal Immigration Agencies - FY2019, WADMV_002876-WADMV_002883 (In FY2019, 67,822 ICE-DOL queries (33,731 drivers), but 1,395,531 DHS queries overall).

121. *Id.* (17,940 image requests / 56,248 drivers = 32%).

122. Georgia DDS, ICE HSI Email to Georgia DDS (Jun. 8, 2018), GADMV_000198 ("Can you assist me with finding a person in GA? We don't have specific identifiers other than a cell number and the CLEAR results. Trying to determine if there is any dl on possible subject").

123. Georgia DDS, DHS Email to Georgia DDS (May 24, 2019), GADMV_000436 ("Please advise if [redacted] has a valid GA DL or state ID. I'm unable to verify in NLETS.").

124. *See* National Immigration Law Center, *How U.S. Immigration & Customs Enforcement and State Motor Vehicles Share Information* 3 (May 2016), https://www.nilc.org/wp-content/uploads/2016/06/Info-Sharing-FOIA-Summary-2016-05.pdf.

125. National Immigration Law Center, *Migrant Justice Settles Lawsuit with Vermont DMV* (Jan. 15, 2020), https://www.nilc.org/2020/01/15/migrant-justice-settles-discrimination-lawsuit-with-vermont-dmv/.

126. *See, e.g.,* Oregon DMV, Spreadsheet of ICE Requests for Driver Information (Aug. 7, 2020), ORDMV_000040-ORDMV_000048 (2015: 35 addresses run; 2016: 40 addresses run; 2017: 27 addresses run; 2018: 3 addresses run; 2019: 0 addresses run; 2020: 0 addresses run).

127. Georgia DDS, ICE Email to Georgia DDS (May 1, 2019), GADMV_000467 ("We have a surge coming up and need to ID these target [sic] for [redacted] . . . I am trying to but [sic] a batch since I have so many. I will fill out the form once you verify they have a photo. Thanks in advance.").

128. *See* Virginia DMV, Letter to Harrison Rudolph (Aug. 17, 2020), VADMV_000300.

129. *See* Arizona Department of Transportation, OIG/Professional Standards Unit Narrative (Mar. 29, 2017), AZDMV_000071.

130. *See* U.S. Department of Homeland Security, DHS/ICE/PIA-054, Privacy Impact Assessment for the ICE Use of

Facial Recognition Services 2 (May 13, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf ("HSI routinely encounters digital images of potential victims or individuals suspected of crimes but cannot connect those images to identifiable information through existing investigative means and methods. HSI, therefore, submits those images to government agencies and commercial vendors to compare against their digital image galleries via facial recognition processes.").

131. List of Agencies who requested data from the State of Alaska, 101210.

132. Spillman Flex records for requests received from U.S. Department of Homeland Security, including its components U.S. Immigration and Customs Enforcement, and U.S. Customs and Border Protection, AZDMV_000094.

133. Conor May, Hillary Bernhardt, Bethany Reece, Sam Thornton, Blake E. Reid & Violeta Chapin, *Colorado DMV Records & ICE: Preventing Unauthorized Disclosures*, Colorado Law 19 (Mar. 16, 2020) https://tlpc.colorado.edu/wp-content/uploads/2020/05/Colorado-DMV-Records-ICE-Preventing-Unauthorized-Disclosures.pdf.

134. Joey Roulette, *ICE, FBI among federal agencies searching Florida driver's licenses for facial recognition, records show*, Orlando Sentinel (July 12, 2019), https://www.orlandosentinel.com/politics/os-ne-ice-fbi-facial-recognition-florida-drivers-license-database-20190712-xs6acoda5zgy5nqsi6yqd2tgwi-story.html.

135. Justin Gray & Terah Boyd, *Have a Georgia ID? Your face has been searched hundreds of times to see if you look like a suspect*, WSB-TV Atlanta (Feb. 18, 2020), https://www.wsbtv.com/news/local/have-georgia-id-your-face-has-been-searched-hundreds-times-see-if-you-look-like-suspect/TF7V6VMC2RDOVEWMGY7HZG4WOE/.

136. Email from ICE to Illinois Secretary of State Police (Apr. 1, 2020), ILDMV_000139.

137. Drew Harwell & Erin Cox, *ICE has run facial-recognition searches on millions of Maryland drivers*, Washington Post (Feb. 26, 2020), https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers/.

138. Michigan DMV, MIDMV_000041 ("05/22/2019 Ran subject in COLD, Images aud File Net, spoke with ICE agent who requested facial recgoniztion [sic] and order certifications. MSP FR results no further matches. I received the certs on 05/292019 [sic].").

139. Ohio Attorney General, Facial-Recognition Inquires: A Special Report 2 (Aug. 2019), https://www.ohioattorneygeneral.gov/FacialRecognitionInquiriesReport ("Federal agencies that have used Ohio's facial-recognition database include the U.S. Border Patrol; U.S. Department of State Bureau of Diplomatic Security; U.S. Immigration and Customs Enforcement; the FBI; Federal Reserve Bank of Cleveland; Drug Enforcement Administration; the U.S. Marshals Service; and the Bureau of Alcohol, Tobacco, Firearms and Explosives; and others.").

140. Driving Pennsylvania Forward, *Secure Our Data: Protecting the Privacy of Pennsylvania Residents and Drivers* 17 (Sept. 2020), https://drivingpaforward.org/wp-content/uploads/2020/09/Secure-Our-Data-Driving-PA-Forward-2020-Hit-the-Brakes-on-Information-Sharing-Final-Pages-1.pdf.

141. Utah Department of Police Statewide Information & Analysis, Query Logs, 108850-108911.

142. Vermont Department of Motor Vehicles, Requests for Facial Recognition Investigation, 103714, 103739, 103761, 103763, 104241.

143. Washington State Department of Licensing, ICE-HSI Face Recognition Search requests, 100140-100143, 100147-100151, 100285-100288, 100289-100292, 100293-100296.

144. Wisconsin Department of Transportation, ICE Request for Facial Recognition to DOT DMV Fraud Unit (Jul. 18, 2018), WIDMV_000038.

145. Jared Polis, Governor, *Guidance to executive branch departments and agencies on data privacy*, State of Colorado (May 20, 2020), https://s3.documentcloud.org/documents/6923100/POLIS-EXECUTIVE-GUIDANCE.pdf.

146. S.B. 0225, 102d Gen. Assemb. (Il. 2021), *available at* https://www.ilga.gov/legislation/BillStatus.asp?DocNum=225&GAID=16&DocType=SB&SessionID=110&GA=102.

147. Maryland Driver Privacy Act, H.B. 23, Md. Gen. Assemb., 2021 Sess. (Md. 2021).

148. S.B. 34, 2021 Gen. Sess. (Ut. 2021), *available at* https://le.utah.gov/~2021/bills/static/SB0034.html.

149. S. 124, Vt. Gen. Assemb., 2020 Sess. (Vt. 2020), *available at* https://legislature.vermont.gov/bill/status/2020/S.124.

150. S.B. 5497, 2019 Reg. Sess. (Wa. 2019), *available at* https://app.leg.wa.gov/billsummary?BillNumber=5497&Year=2019.

151. USAspending, Contract Summary: L-1 IDENTITY SOLUTIONS, INC., https://www.usaspending.gov/award/CONT_AWD_HSCECR08P00090_7012_-NONE-_-NONE-/.

152. Across these 14 states, there are a total of approximately 82,822,300 drivers. Office of Highway Policy Information, Licensed Total Drivers, by Age (1), U.S. Department of Transportation Federal Highway Administration (2019), https://www.fhwa.dot.gov/policyinformation/statistics/2019/xls/dl22.xls.

153. Across these 14 states, approximately 81,632,770 drivers are adults. *Id.* In the U.S., there are a total of approximately 257,536,091 adults. U.S. Census Bureau, QuickFacts, https://www.census.gov/quickfacts/fact/table/US/POP010210#POP010210.

154. Wisconsin DOT, WISC email to WI DOT; Request for Facial Recognition (Mar. 16, 2017), WIDMV_001017 ("On behalf of the Department of Homeland Security, Homeland Security Investigations, I'd like to request a FR attempt

against the attached photos. The individual pictured was receiving false identity documents and the Milwaukee HSI office is attempting to determine his true identity. This is part of an ongoing fraud investigation they are working.").

155. Georgia DDS, Email to Georgia DDS (Mar. 2, 2018), GADMV_000157 ("Can you buddy try these? I can also go on Facebook and try to find a better one . . . Can you please give these photos another try through FR when it comes up?").

156. Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proceedings of Mach. Learning Rsch. (2018), https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

157. *See* Patrick Grother, Mei Ngan & Kayee Hanaoka, NIST Interagency Report 8280, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, National Institute of Standards and Technology (Dec. 12, 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf; Cynthia M. Cook, John J. Howard, Yevgeniy B. Sirotin, Jerry L. Tipton & Arun R. Vemury, *Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems*, 1 IEEE Transactions on Biometrics, Behavior, and Identity Sci. (Feb. 6, 2019), http://jjhoward.org/wp-content/uploads/2019/02/demographic-effects-image-acquisition.pdf; Lee Davidson, *Utah lawmakers scrutinize law enforcement's facial recognition scans of state driver licenses*, Salt Lake Tribune (Sept. 18, 2019), https://www.sltrib.com/news/politics/2019/09/18/utah-lawmakers-scrutinize/ ("officials conceded that Utah's system is out of date; prone to errors, especially with women and people of color; in need of more training for analysts and has no legal standards for operation").

158. *See* U.S. Department of Homeland Security, DHS/CBP/PIA-054, Privacy Impact Assessment for the ICE Use of Facial Recognition Services 9 (May 13, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf ("HSI will only submit probe photos to be used in furtherance of ongoing criminal investigations . . . HSI will not support ERO in using [face recognition] solely in furtherance of civil immigration enforcement.").

159. Joan Friedland, *How ICE Blurs the Line between Enforcement of Civil Immigration Violations and Enforcement of Criminal Laws*, National Immigration Law Center (Aug. 27, 2019), https://www.nilc.org/2019/08/27/ice-blurs-line-between-civil-and-criminal-enforcement/.

160. U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy (May 2016), https://www.gao.gov/assets/gao-16-267.pdf ("As of December 2015, the FBI has agreements with 7 states to search NGI-IPS, and is working with more states to grant access. In addition to the NGI-IPS, the FBI has an internal unit called Facial Analysis, Comparison and Evaluation (FACE) Services that provides face recognition capabilities, among other things, to support active FBI investigations. FACE Services not only has access to NGI-IPS, but can search or request to search databases owned by the Departments of State and Defense and 16 states, which use their own face recognition systems.").

161. Committee to Review Law Enforcement's Policies on Facial Recognition Technology, Committee on Oversight and Reform (Mar. 22, 2017), https://republicans-oversight.house.gov/hearing/law-enforcements-use-facial-recognition-technology/.

162. Federal Bureau of Investigation, *July 2021 Next Generation Identification (NGI) System Fact Sheet* (Jul. 2021), https://www.fbi.gov/file-repository/ngi-monthly-fact-sheet/view.

163. U.S. Customs and Border Protection, *CBP Trade and Travel Report*, Fiscal Year 2020 (Feb. 2021), https://www.cbp.gov/sites/default/files/assets/documents/2021-Feb/CBP-FY2020-Trade-and-Travel-Report.pdf; U.S. Department of Homeland Security, DHS/CBP/PIA-056, Privacy Impact Assessment for the Traveler Verification Service (Nov. 14, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf.

164. Catie Edmondson, *ICE Used Facial Recognition to Mine State Driver's License Databases*, New York Times (Jul. 7, 2019), https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html.

165. The system was formerly named the "National Law Enforcement Telecommunication System."

166. U.S. ICE, Replacement/Upgrade of Message Switching System (Sep. 23, 2006), https://drive.google.com/file/d/11M_G3wOwB7x0-U_LAVd5M0kw-XJcWGuj/view?usp=sharing ("The contract will replace and upgrade their proprietary OpenFox Message Switching System installed in 2000 at the ICE field activity [LESC] in Williston, VT. The system interfaces with national systems such as the National Law Enforcement Telecommunications System (NLETS) and the National Crime Information Center (NCIC) and other specialized protocols specific to the law enforcement community."); Bonnie Locke, Five Commonly Asked Questions About Nlets, Nlets Blog (May 27, 2021), https://nlets.org/resources/blog/five-commonly-asked-questions-about-nlets; Nlets, What We Do, https://www.nlets.org/about/what-we-do.

167. *See* Wisconsin DOT, WI NLETS Queries (2020), WINLETS_000010-WINLETS_000102.

168. Not sharing DMV information with Nlets (7 states): "Nevada, Hawaii, Oklahoma, Illinois, South Carolina, Connecticut, Vermont, Guam, and the Virgin Islands." Otherwise cutoff ICE use (7 states): Alaska (court order) California (non-immigration enforcement ok) New York (via ORI code) New Jersey (non-immigration enforcement ok) North Dakota (unclear why) South Dakota (unclear why) Oregon (non-immigration enforcement ok)); *See also* H.B. 2163, Va. Gen. Assemb., 2021 Sess. (Va. 2021), https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+HB2163 (Virginia law limiting release of DMV information for civil immigration enforcement purposes); Sanctuary Values Amendment Act of 2020, D.C. Law 23-282 § 3 (2020), https://code.dccouncil.us/us/dc/council/laws/23-282; Maryland Driver Privacy Act, H.B. 23, Md. Gen. Assemb., 2021 Sess. (Md. 2021).

169. Across these 35 states, there are a total of approximately 150,697,928 drivers. Office of Highway Policy Information, Licensed Total Drivers, by Age (1), U.S. Department of Transportation Federal Highway Administration (2019), https://www.fhwa.dot.gov/policyinformation/statistics/2019/xls/dl22.xls.

170. *See* Document 71-1, filed Jun. 17, 2020, in Lewis-McCoy, et al. v. Wolf, et al., Case 1:20-cv-01142-JMF, S.D.N.Y, https://www.nyclu.org/sites/default/files/wysiwyg/1_-_completed_administrative_record_public.pdf (Not sharing DMV information with Nlets (7 states): "Nevada, Hawaii, Oklahoma, Illinois, South Carolina, Connecticut, Vermont, Guam, and the Virgin Islands." Otherwise cutoff ICE use (7 states): Alaska (court order) California (non-immigration enforcement ok) New York (via ORI code) New Jersey (non-immigration enforcement ok) North Dakota (unclear why) South Dakota (unclear why) Oregon (non-immigration enforcement ok)); *See also* H.B. 2163, Va. Gen. Assemb., 2021 Sess. (Va. 2021), https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+HB2163 (Virginia law limiting release of DMV information for civil immigration enforcement purposes); Sanctuary Values Amendment Act of 2020, D.C. Law 23-282 § 3 (2020), https://code.dccouncil.us/us/dc/council/laws/23-282; Maryland Driver Privacy Act, H.B. 23, Md. Gen. Assemb., 2021 Sess. (Md. 2021).

171. Across these 40 jurisdictions, there are a total of approximately 193,643,467 drivers, of which approximately 191,079,036 are adults. 191M/257M = 74%. *See* Office of Highway Policy Information, Licensed Total Drivers, by Age (1), U.S. Department of Transportation Federal Highway Administration (2019), https://www.fhwa.dot.gov/policyinformation/statistics/2019/xls/dl22.xls (drivers by state); U.S. Census Bureau, QuickFacts, https://www.census.gov/quickfacts/fact/table/US/POP010210#POP010210 (total number of adults).

172. *See* Wisconsin DOT, WI NLETS Queries (2020), WINLETS_000010-WINLETS_000102.

173. Texas Department of Public Safety, Letter to Harrison Rudolph (Oct. 5, 2020), TXDMV_000160 (ICE TLETS Transaction Counts [for 01/01/2015 - 09/18/2020] DL: 223814 MVD: 118517).

174. Iowa Department of Public Safety, Email to Harrison Rudolph (Nov. 18, 2020), IANLETS_000003 (The tabulation of numbers of these specific queries since 2015 totals approximately 83,400.).

175. Washington Department of Licensing, Requests via NLETS and WSP access from Federal Immigration Agencies - FY2019, WADMV_002876-WADMV_002883 (In FY2019, 67,822 ICE-DOL queries (33,731 drivers)).

176. *See, e.g.,* National Immigration Law Center, Nlets: Questions and Answers (Nov. 2020), https://www.nilc.org/issues/immigration-enforcement/nlets-questions-and-answers/; Just Futures Law, *State Driver's License Data: Breaking Down Data Sharing and Recommendations for Data Privacy* (Mar. 2020), https://justfutureslaw.org/wp-content/uploads/2020/04/2020-3-5-State-DMV-Data-Sharing-Just-Futures-Law.pdf.

177. Letter from Christine E. Nizer, William P. Doyle, Ricky D. Smith & Pilar Helm to Hon. William C. Smith, Chairman, Senate Judicial Proceedings Committee Re: Letter of Opposition—Senate Bill 234—Personal Information—State and Local Agencies—Restrictions on Access (Jan. 28, 2021), https://drive.google.com/file/d/1siYx-yDkwggUQB3APZzqYmfKkg7BQHnF/view?usp=sharing.

178. Maryland DPSCS, Letter to Harrison Rudolph (Jan 21, 2021), MDNLETS_000007-MDNLETS_000008 ("I am writing to inform you that the Department of Public Safety and Correctional Services (DPSCS) is not the custodian of record for the data you seek. To facilitate the processing of your request, I have forwarded your inquiry to: Maryland Department of State Police").

179. Maryland State Police, Letter to Harrison Rudolph (Jan 27, 2021), MDNLETS_000009 ("Upon review of your request, it was determined that the MSP does not maintain anything related to queries. All logging of queries that would be running originating in and out of state are logged at the state message switch housed by DPSCS. They should be able to pull the logs").

180. Iowa Department of Transportation, Email to Harrison Rudolph (Aug. 24, 2020), IADMV_000081 ("The Iowa Department of Transportation is the source of driver and vehicle information that is accessed and used by DPS to fulfill its obligation to NLETS. DPS has a direct connection to the Iowa Department of Transportation where they access a web service (DPSService) to obtain driver information. DPS sends in a request for a specific customer, and based on the type of request, a response is generated using the Global Justice XML Data model (GJXDM) and returned to DPS. The responses are dynamic and vary by customer and request type. What and how the fields are used is a question for DPS, we simply make this information available to DPS via the DPSService.").

181. Idaho Transportation Department, Email to Harrison Rudolph (Aug. 25, 2020), IDDMV_000009-IDDMV_000011 ("ITD possesses no such documents. ITD is required through state Administrative RULE 39.02.41.200 (shown below) to send vehicle and driver information to the Idaho Law Enforcement Telecommunication Systems (ILETS) to provide vehicle and driver information to law enforcement. Idaho State Police have oversight of ILETS and how it interfaces with NLET; ITD is not involved in this process.").

182. Colorado Bureau of Investigation, Email from Kristina Gavit to Harrison Rudolph (Nov. 13, 2020), CONLETS_000019-CONLETS_000020.

183. Document 43-1, filed Apr. 24, 2020, in Lewis-McCoy, et al. v. Wolf, et al., Case 1:20-cv-01142-JMF, S.D.N.Y ("Generally, DMV information is retrieved through the National Law Enforcement Telecommunication System (Nlets)"); Public records back that up. One immigration agent asked the Georgia Department of Driver Services for assistance verifying a driver's license only after the agent was "unable to verify [it] in Nlets." Georgia DDS, DHS Email to Georgia DDS (May 24, 2019), GADMV_000436 ("Please advise if [redacted] has a valid GA DL or state ID. I'm unable to verify in NLETS."). Other public records show that another ICE agent asked the Illinois Secretary of State for driver's license information (including a photograph) only after attempting an Nlets search. Illinois Secretary of State, Email from ICE HSI Requesting Driver Records (Jul. 17, 2019), ILDMV_000207-ILDMV_000209 ("Homeland Security Investigations is requesting assistance in obtaining the DMV information and photo of the following individual . . . NLETS returned the following results . . . [Redacted] RES-PID CLASS/NONE DL/IP STA/VALID TDL/TIP STA/SEE /LOLNHELP CDL STA/SEE ILOLNHELP DIGITAL ISSUE . . . Subject is a possible witness in an ongoing criminal investigation. In violation of 21 USC § 848, continuing criminal enterprise.").

184. Adam Comis & Stuart Malec, *Thompson and Rice Announce Investigation After Administration Gave Inaccurate Testimony to Congress About Political Attack on New York*, Committee on Homeland Security (July 25, 2020), https://homeland.house.gov/news/press-releases/thompson-and-rice-announce-investigation-after-administration-gave-inaccurate-testimony-to-congress-about-political-attack-on-new-york.

185. Document 43-1, filed Apr. 24, 2020, in Lewis-McCoy, et al. v. Wolf, et al., Case 1:20-cv-01142-JMF, S.D.N.Y ("Some of the information contained in DMV databases may be available from other sources, but this data is not as accurate, current, or complete as in the DMV databases. With the expenditure of additional time and effort, some DMV information may be located in other databases, but some records are specific to DMV databases. For example, commercially available public databases, such as CP CLEAR, contain some residential records, dates of birth, and photographs; however, this information is often incomplete, incorrect, or outdated.").

186. *See* Joseph Cox, *DMVs Are Selling Your Data to Private Investigators*, VICE (Sept. 6, 2019), https://www.vice.com/en/article/43kxzq/dmvs-selling-data-private-investigators-making-millions-of-dollars; Joseph Cox, *The California DMV Is Making $50M a Year Selling Drivers' Personal Information*, VICE (Nov. 25, 2019), https://www.vice.com/en/article/evjekz/the-california-dmv-is-making-dollar50m-a-year-selling-drivers-personal-information.

187. McKenzie Funk, *How ICE Picks Its Targets in the Surveillance Age*, New York Times (Oct. 2,2019), https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.

188. The parent company of LexisNexis, RELX Group, is a major contractor that has provided ICE agents with access to massive databases of individuals' biographical information. *See* Sarah Lamdan, *When WestLaw Fuels ICE Surveillance: Legal Ethics in the Era of Big Data Policing*, 43 N.Y.U. Rev. of L. & Soc. Change (2018), https://socialchangenyu.com/review/when-westlaw-fuels-ice-surveillance-legal-ethics in the-era-of-big-data-policing/#iii-legal-research-companies-roles in ice-surveillance.

189. Dun & Bradstreet, Lexisnexis Risk Solutions Inc., https://www.dnb.com/business-directory/company-profiles.lexisnexis_risk_solutions_inc.65ade48305f9d7833f1a9cb0a6e627b7.html; LexisNexis Risk Solutions, About Us, https://risk.lexisnexis.com/about-us (last visited Nov. 21, 2021); LexisNexis, PowerPoint Deck for South Carolina DMV (May 11, 2016), SCDMV_000239-SCDMV_000249 ("12% of LexisNexis Risk Solutions Revenue comes from Government and Health Care").

190. U.S. Immigration and Customs Enforcement, Pre-solicitation Notice Law Enforcement Investigative Database Subscription (LEIDS) (2020), https://govtribe.com/opportunity/federal-contract-opportunity/law-enforcement-investigative-database-subscription-leids; Definitive Contract PIID 70CMSD21C00000001, USAspending, https://www.usaspending.gov/award/CONT_AWD_70CMSD21C00000001_7012_-NONE-_-NONE- (last visited Nov. 21, 2021).

191. Florida HSMV, LexisNexis Senior Vice President and General Counsel Letter to FLHSMV (Apr. 16, 2018), FLDMV_000111-FLDMV_000113 ("LexisNexis supports more than 5,000 Federal, State and local government agencies. Many of these agencies are responsible for homeland security initiatives and traditional law enforcement responsibilities . . . pursuant to F.S.A. §119.0712(2)(b) and 18 U.S.C. §(b)(l), LexisNexis provides Florida motor vehicle records and driver's license data to government agencies who use the data in carrying out their functions including, but not limited to, locating fugitives and determining an individual's eligibility for government benefits, licenses and permits.").

192. U.S. Immigration and Customs Enforcement, Pre-solicitation Notice Law Enforcement Investigative Database Subscription (LEIDS) (2020), https://govtribe.com/opportunity/federal-contract-opportunity/law-enforcement-investigative-database-subscription-leids.

193. Arizona DOT, Commercial Electronic Data Access Agreement with LexisNexis Risk Solutions Inc (Jul. 20, 2018), AZDMV_000015-AZDMV_000031.

194. While California's DMV requires authorized government requesters to refrain from using driver's license information for civil immigration enforcement purposes, it is unclear whether LexisNexis Risk Solutions has agreed to the condition. *See* VICE News, California DMV Commercial Requester Accounts, https://drive.google.com/file/d/1czK4QyHbZRhXivG29oLjk4pl1Ph2JhUp/view?usp=sharing (listing LexisNexis Risk Solutions as an authorized commercial requestor).

195. DC DMV, Sixth Addendum to Electronic Record Request Agreement Between DC DMV and LexisNexis Risk Solutions (Sep. 15, 2016), DCDMV_000014.

196. Florida HSMV, LexisNexis Senior Vice President and General Counsel Letter to FLHSMV (Apr. 16 2018), FLDMV_000111-FLDMV_000113.

197. Illinois Secretary of State, Driver Service Agency Sales Activity, Month of Feb. 2019, ILDMV_000064.

198. Minnesota DMV, Income Contract with LexisNexis Risk Solutions Inc (Aug. 1, 2019), MNDMV_000006-MNDMV_000016.

199. Nebraska DMV, Driver Record Purchase Agreement with LexisNexis Risk Solutions, Inc (Jul. 20, 2018), NEDMV_000082-NEDMV_000091.

200. Nevada DMV, LexisNexis Risk Solutions Inc. Application for Records Account (2019), NVDMV_000021-NVDMV_000022.

201. *See* Diane Willson, *NCDMV Sells Your Personal Information, Pockets Millions of Dollars*, ABC11 Eyewitness News (Feb. 5, 2020), https://abc11.com/lexis-nexis-dmv-nc-ncdmv/5903314/ ("A representative with NCDMV said the department sells your personal information to these three companies:" Explore Info Services, Envision-Data Driven Safety, and Lexis Nexis Corporation).

202. Oregon DMV, Disseminator Contract with LexisNexis Risk Solutions, Inc (May 22, 2020), ORDMV_000004-ORDMV_000012.

203. South Carolina DMV, Information Release Agreement (Data Manipulators) with LexisNexis Risk Solutions (Jun. 28, 2018), SCDMV_000152-SCDMV_000167; South Carolina DMV, Disclosure of Personal Information, SCDMV_000259-SCDMV_000262.

204. Adrian Mojica et al., *Personal Information of 7.2 million Tennessee Drivers Sold to Companies by State Agency*, Fox17 (Feb. 17, 2020), https://fox17.com/news/local/personal-information-of-72-million-tennessee-drivers-sold-to-companies-by-state-agency ("The next question we posed to the department was which companies were receiving our data? The department listed five companies: Acxiom Corporation, Drivers History, Explore Information Services, Lexis Nexis, and Samba Holdings.").

205. *See* Rhonda Foxx, *WisDOT Earned Millions by Providing Driver Information to Third Parties*, WeAreGreenBay.com (Feb. 10, 2020), https://www.wearegreenbay.com/news/local-news/wisdot-earned-millions-by-providing-driver-information-to-third-parties/ ("Driver Record Header File: Driver History Information, Explore Information Services, Insurance Information Exchange (IIX), Lexis Nexis, Acxiom, Early Warning Services, LLC, TransUnion, West Services (Thomson Reuters)").

206. Across these 13 jurisdictions, there are a total of approximately 88,250,040 drivers, of which approximately 87,182,428 are adults. 87M/257M = 34%. *See* Office of Highway Policy Information, Licensed Total Drivers, by Age (1), U.S. Department of Transportation Federal Highway Administration (2019), https://www.fhwa.dot.gov/policyinformation/statistics/2019/xls/dl22.xls (drivers by state); U.S. Census Bureau, QuickFacts, https://www.census.gov/quickfacts/fact/table/US/POP010210#POP010210 (total number of adults).

207. Law Enforcement Investigative Database Subscription (LEIDS), SAM.gov https://beta.sam.gov/opp/3f5c39eda56a4365b47a35f3ef0790bb/view?keywords=leids&sort=-relevance&index=&is_active=false&page=1 (last visited Nov. 16, 2021).

208. Pul Eckloff, *LexisNexis Receives US Department of Justice Award to Provide Legal and Criminal Investigation Solutions across Five Federal Agencies*, LexisNexis Risk Solutions (Jan. 14, 2020), https://risk.lexisnexis.com/about-us/press-room/press-release/20200114-doj-contract-award.

209. Federal Bureau of Investigation, Limited Sources Justification (FAR Part 8) (2018), https://beta.sam.gov/api/prod/opps/v3/opportunities/resources/files/bdfba8ff66a5638e821566343a8044a2/download?api_key=null&status=archived&token=.

210. *See, e.g.,* Release of DMV Information, Virginia DMV, https://www.dmv.virginia.gov/general/#records/release.asp.

211. 139 Cong. Rec. 29,469 (Nov. 16, 1993).

212. According to the U.S. Solicitor General and the Clerk of the House Judiciary Committee, the transcript of the two-day DPPA hearing was not preserved. *See* Petition for Writ of Certiorari, Okla. Dep't of Pub. Safety v. United States, 528 U.S. 1114 (No. 98-1760), https://www.justice.gov/sites/default/files/osg/briefs/1998/01/01/98-1760.resp.hold.pdf. *But see Protecting Driver Privacy: Hearings Before the Subcomm. on Civ. and Const. Rts. of the H. Comm. on the Judiciary* 103rd Cong. (1994) (statement of Janlori Goldman, Director, American Civil Liberties Union), *available at* 1994 WL 212813 (Feb. 3-4, 1994); 1994 WL 212833; 1994 WL 212834; 1994 WL 212836; 1994 WL 212696; 1994 WL 212701, 212712; 1994 WL 212720.

213. *See* Just Futures Law, *State Driver's License Data: Breaking Down Data Sharing and Recommendations for Data Privacy* 4 (Mar. 2020), https://justfutureslaw.org/wp-content/uploads/2020/04/2020-3-5-State-DMV-Data-Sharing-Just-Futures-Law.pdf.

214. H.B. 3464, 2017 Sess. (Or. 2017), https://gov.oregonlive.com/bill/2017/HB3464/.

215. Oregon DMV, Spreadsheet of ICE Requests for Driver Information (Aug. 7, 2020), ORDMV_000040-ORDMV_000048 (2015: 35 addresses run; 2016: 40 addresses run; 2017: 27 addresses run; 2018: 3 addresses run; 2019: 0 addresses run; 2020: 0 addresses run).

216. H.B. 2015, 2019 Reg. Sess. (Or. 2019), https://olis.oregonlegislature.gov/liz/2019R1/Measures/Overview/HB2015.

217. *See* Oregon DMV, Disseminator Contract with West Publishing Corporation (Feb. 21, 2020), ORDMV_000025-ORDMV_000033 (The Disseminator may resell or redisclose Personal Information only to a Person or government agency authorized to receive such information under ORS 802.179. [ORS 802.179(1) The Department of Transportation, upon request or as required by law, shall disclose personal information from a motor vehicle record to a government agency for use in carrying out its governmental functions.]); Oregon DMV, Disseminator Contract with LexisNexis Risk Solutions, Inc (May 22, 2020), ORDMV_000004-ORDMV_000012 (The Disseminator may resell or redisclose Personal Information only to a Person or government agency authorized to receive such information under ORS 802.179. [ORS 802.179(1) The Department of Transportation, upon request or as required by law, shall disclose personal information from a motor vehicle record to a government agency for use in carrying out its governmental functions.]).

218. Maryland Driver Privacy Act, S.B. 234, Md. Gen. Assemb., 2021 Reg. Sess. (Md. 2020) https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0234?ys=2021RS.

219. Clara Garcia, *Maryland General Assembly Overrides Hogan's Vetoes of Immigration Bills*, NBC Washington (Dec. 8, 2021), https://www.nbcwashington.com/news/local/maryland-general-assembly-overrides-hogans-vetoes-of-immigration-bills/2904771/.

220. AB-1747 (Ca. 2019), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1747.

221. Governmental Use of Facial Recognition Technology, S.B. 34, 2021 Gen Sess. (Ut. 2021), https://le.utah.gov/~2021/bills/static/SB0034.html.

222. *New California Law to Protect Personal Information on State Databases From Immigration Authorities*, NBC San Diego (Oct. 12, 2019), https://www.nbcsandiego.com/news/local/ice-drivers-license-gonzales/1966317/.

223. Dissemination of driver data to ICE for civil immigration enforcement purposes is not prohibited by law in Connecticut, Delaware, Illinois, New Mexico, Nevada, and Utah.

224. Nlets access by ICE for civil immigration enforcement purposes is not prohibited by law in Connecticut, Delaware, Hawaii, Illinois, New Mexico, Nevada, and Utah.

225. Sales of driver's data to data brokers and subsequent resale to ICE for civil immigration enforcement purposes is not prohibited at law in the District of Columbia, Colorado, Hawaii, Illinois, New Jersey, Nevada, and Vermont.

226. Face recognition searches of driver data for civil immigration enforcement purposes are not prohibited by law in Connecticut, Delaware, Hawaii, New Mexico, and Nevada.

227. Warrantless dissemination of driver data to ICE for non-civil immigration enforcement purposes is not prohibited by law in California, Colorado, New Jersey, Oregon, Vermont, and Virginia.

228. Warrantless Nlets access by ICE for non-civil immigration enforcement purposes is not prohibited by law in California, Colorado, New Jersey, Oregon, Vermont, Virginia, and Washington State.

229. Sales of driver data to data brokers and subsequent resale to ICE for non-civil immigration enforcement purposes is not prohibited at law by California, Connecticut, Delaware, Virginia, and Washington State.

230. Warrantless face recognition searches of driver data for non-civil immigration enforcement purposes are not prohibited by law in Colorado, the District of Columbia, Illinois, New Jersey, Utah, Virginia.

231. See The Maryland Driver Privacy Act, H.B. 23 §4-320(g)(2) (2021) (restricting sharing of driver data "to a federal agent or federal agency for the purpose of federal immigration enforcement"); id. at §4-320.1(B)(1) & (B)(2) (restricting access to face recognition systems by "any federal agency seeking access for the purpose of enforcing federal immigration law").

232. Driver's License Access and Privacy Act ("Green Light Law"), S.B. S1747B, 2019 Leg. Sess. (N.Y. 2019), https://www.nysenate.gov/legislation/bills/2019/s1747.

233. Doc 71-1, filed Jun. 17, 2020, in Lewis-McCoy, et al. v. Wolf, et al., Case 1:20-cv-01142-JMF, S.D.N.Y, https://www.nyclu.org/sites/default/files/wysiwyg/1_-_completed_administrative_record_public.pdf.

234. New York State Department of Motor Vehicles, Request for Certified DMV Records, https://dmv.ny.gov/forms/mv15.pdf.

235. An Overview of the Credit Reporting System: Hearing Before the Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, 113th Cong. (2014), https://www.govinfo.gov/content/pkg/CHRG-113hhrg91161/html/CHRG-113hhrg91161.htm. ("More than 50 million Americans have no credit score, are just credit-invisible. Another 50 million have scores that are lower than they should be because they do not have enough lines of debt to generate a score.").

236. *Id.*

237. *See* National Consumer Law Center, Full File Utility Credit Reporting: Harms to Low-Income Consumers (2013), https://www.nclc.org/images/pdf/credit_reports/ib_utility_credit_2013.pdf ("One of the efforts to promote alternative credit data urges that utility companies engage in monthly reporting of customer payments, including late payments, to the Big Three nationwide credit reporting agencies (CRAs), Equifax, Experian, and TransUnion. Currently, the vast majority of electric and natural gas utility companies only report to those three CRAs when a seriously delinquent account has been referred to a collection agency or written off as uncollectible.").

238. *See* An Overview of the Credit Reporting System: Hearing Before the Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, 113th Cong. 137–38 (2014), https://www.govinfo.gov/content/pkg/CHRG-113hhrg91161/html/CHRG-113hhrg91161.htm (letter from Buddy Flake, NCTUE Board President, and Micheal Gardner, Senior Vice President, Equifax, to Keith Ellison, Member, Committee on Financial Services) ("[The National Consumer Telecom & Utilities Exchange] is a nationwide, member-owned and operated, FCRA-compliant data exchange that houses both positive and negative alternative payment data (i.e., non-traditional financial payment reporting data, such as telecom and utility payments) on consumers, which is then available to NCTUE's members on a blind basis to aid in their credit decisioning and risk management . . .member companies currently report and share industry-specific payment data on more than 180 million consumers throughout the United States.").

239. *See* An Overview of the Credit Reporting System: Hearing Before the Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, 113th Cong. (2014), https://www.govinfo.gov/content/pkg/CHRG-113hhrg91161/html/CHRG-113hhrg91161.htm (statement of Hon. Keith Ellison) ("I am eager to see this Congress take action to improve our [credit reporting] system by making it more inclusive. . . . Mr. Fitzpatrick and I, in a bipartisan way, have a bill called the Credit Access and Inclusion Act, and this bill clarifies that current law does not prohibit utility and telecom firms from reporting their customers' on-time payments.").

240. An Overview of the Credit Reporting System: Hearing Before the Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, 113th Cong. (2014), https://www.govinfo.gov/content/pkg/CHRG-113hhrg91161/html/CHRG-113hhrg91161.htm.

241. *Id.*

242. *Id.*

243. Oversight Subcommittee Launches Investigation into Sale of Utility Customer Info to ICE for Deporting Immigrants, House Committee on Oversight and Reform (Feb. 26, 2021), https://oversight.house.gov/news/press-releases/oversight-subcommittee-launches-investigation-into-sale-of-utility-customer-info.

244. Georgia DDS, Email to Georgia DDS; B1/2 Visa Overstay by Immigrant, June 2, 2020, GADMV_001230.

245. *Id.*

[246] Ian Kullgren, *ICE to Scale Back Arrests During Coronavirus Pandemic*, Politico (Mar. 18, 2020) https://www.politico.com/news/2020/03/18/ice-to-scale-back-arrests-during-coronavirus-pandemic-13680. Then Acting DHS Secretary Ken Cuccinelli seemed to reverse this policy, but nonetheless implied that arrests would occur at a slower pace. *See* Ken Cuchinelli (@HomelandKen), Twitter (Mar. 19, 2020), https://twitter.com/HomelandKen/status/1240644749176037377.

[247] Georgia DDS, Email to Georgia DDS; B1/2 Visa Overstay by Immigrant (June 2, 2020), GADMV_001230.

[248] McKenzie Funk, *How ICE Picks Its Targets in the Surveillance Age*, N.Y. Times (June 7, 2021), https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.

[249] *See* About Us, NCTUE, https://www.nctue.com/about-us (last visited Nov. 27, 2021) (indicates that the NCTUE database includes information on over 218 million unique consumers); Equifax Insights, *What is the NCTUE*, Youtube (Oct. 13, 2020), https://www.youtube.com/watch?v=PqAZ5uoRsg0 (at 2:47, indicating percentage of population in NCTUE database for each state); U.S. Census Bureau, Estimates of the Total Resident Population and Resident Population Age 18 Years and Older for the United States, Regions, States, the District of Columbia, and Puerto Rico: July 1, 2020, https://www2.census.gov/programs-surveys/popest/tables/2010-2020/national/asrh/sc-est2020-18+pop-res.xlsx (indicating the total population and adult population by state in 2020).

[250] USAspending, *Contract to West Publishing Corporation*, https://www.usaspending.gov/award/CONT_AWD_HSCEMD11F00003_7012_GS23F0387K_4730 (last visited Nov 27, 2021).

[251] DHS and ICE rely on a network of private companies to synthesize and gather this information. *See generally* Mijente, National Immigration Project & Immigrant Defense Project, *Who's Behind ICE?: The Tech and Data Companies Fueling Deportations* (2018), https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf.

[252] Letter from Kyle Keene, Govt. CLEAR Specialist to Joshua, Thomson Reuters (Jan. 17, 2018), https://www.prorfx.com/Storage/110S34471_051/ProRFx/Upload/Attachments/General/Sole%20Source%20Letter%20-Thomas%20Reuters.pdf.

[253] *Id.*

[254] *Id.*

[255] Letter from Judy Whalley to Assistant Attorney Gen. Anne K. Bingaman (Dec. 9, 1993), https://www.justice.gov/sites/default/files/atr/legacy/2014/07/22/303389.pdf. The founding members of the exchange were: Allnet Communication Services, Inc., AT&T, Business Telecom, Inc., Cable & Wireless, Inc., LDDS Metromedia Communications Corporation, MCI Telecommunications Corporation, Sprint, and WilTel Business Networks.

[256] The process for obtaining approval is discussed in DOJ regulations. U.S. Department of Justice, What is a Business Review? (June 25, 2015), https://www.justice.gov/atr/what-business-review ("Persons concerned about the legality under the antitrust laws of proposed business conduct may ask the Department of Justice for a statement of its current enforcement intentions with respect to that conduct pursuant to the Department's Business Review Procedure. See 28 C.F.R. § 50.6").

[257] NCTUE, History of NCTUE, https://www.nctue.com/history (last visited Nov. 27, 2021).

[258] Press Release, Equifax Investor Relations, Equifax Extends Service Agreement with National Consumer Telecom and Exchange (Nov. 19, 2019), https://investor.equifax.com/news-events/press-releases/detail/89/equifax-extends-service-agreement-with-national-consumer. ("Under the terms of the current agreement, Equifax will continue its operation and management of the NCTUE database. Equifax will also maintain the exclusive right to deliver NCTUE products and services, including: Equifax Insight Scores for Credit, Rental Scores, Advanced Communications Plus, Advanced Energy Plus and many others through 2024. This extended service agreement continues Equifax operation and management of the NCTUE database, subject to the oversight of the NCTUE board of trustees."). The intention for Equifax to sell this data to outside entities also seems to have been present—and mutual—from the start. In a letter to the DOJ, the founding companies cited "Equifax's . . . commitment to find and exploit appropriate opportunities for third-party access to exchange data" as a reason for their partnership. The "revenues generated thereby [would pass] back to exchange members to defray their costs," they claimed, forming one of the "substantial, ever-increasing economic incentives" that motivated the arrangement. *See* Letter from Craig L. Caesar to Assistant Attorney Gen. Hon. Charles A. James 4 n.5 (Aug. 17, 2001), https://www.justice.gov/atr/page/file/1019991/download.

[259] Letter from Judy Whalley to Assistant Att'y Gen. Anne K. Bingaman (Dec. 9, 1993), https://www.justice.gov/sites/default/files/atr/legacy/2014/07/22/303389.pdf.

[260] A skip tracing report would "contain the customer's current address to enable the company…to trace the debtor to a new location and seek recovery." *Id.*

[261] Letter from Craig L. Caesar to Assistant Attorney Gen. Hon. Charles A. James 2 (Aug. 17, 2001), https://www.justice.gov/atr/page/file/1019991/download.

[262] NCTUE, History of NCTUE, https://www.nctue.com/history (last visited Nov. 27, 2021).

[263] Michael A. Turner, Robin Varghese, Patrick Walker, *Research Consensus Confirms Benefit of Alternative Data*, PERC 11 (Mar. 2015), https://www.microbilt.com/Cms_Data/Contents/Microbilt/Media/docs/Research Consensus.pdf.

[264] Equifax, NCTUE, https://www.equifax.com/business/data-network/nctue/ (last visited Nov. 27, 2021).

[265] Thomson Reuters, CLEAR Utility Filing (July 2020), https://drive.google.com/file/d/1R2i1fkW1TMLG75duQCpSlJhUFCEAqQ1a/view?usp=sharing (screenshot obtained by Aaron Lackowski from Empower LLC and shared with the Center on Privacy & Technology).

[266] Equifax Insights, *What is the NCTUE?*, YouTube (Oct. 13, 2020), https://www.youtube.com/watch?v=PqAZ5uoRsg0.

[267] Letter from Craig L. Caesar to Assistant Attorney General Hon. Charles A. James 3 (Aug. 17, 2001), https://www.justice.gov/atr/page/file/1019991/download.

[268] *Id.*

[269] *Id.* at 3 n.4.

[270] NCTUE Users Conference: We're Better Together (Nov. 2015), https://www.nctue.com/userimages/2015_NCTUE_Users_Conference_Agenda.pdf.

[271] NV Energy uses the Equifax Advanced Energy Risk Model to evaluate customer credit risk. Public Utilities Commission of Nevada, Response of Nevada Power Company d/b/a NV Energy and Sierra Pacific Power Company d/b/a NV Energy to Procedural Order No. 1 8 (Oct. 7, 2016), https://drive.google.com/file/d/1Jnf_Vny3n1xcKkpgp3l3HTN53Drjp-ev/view?usp=sharing. According to a product sheet from Equifax, the Advanced Energy Plus score draws on NCTUE data and is only accessible to NCTUE members. Equifax, Advanced Energy Plus (Mar. 3, 2017), https://resources.datadrivenmarketing.equifax.com/collateral/advanced-risk-score-for-utilities-product-sheet-2.

[272] Miami-Dade County Water and Sewer Department, Contract/Project Measure Analysis and Recommendation for Credit and Risk Assessment Services, Miami-Dade County (Mar. 22, 2019), http://www.miamidade.gov/smallbusiness/library/reports/sbe/bw9744-0-22-project-package.pdf (Miami-Dade County's Water and Sewer Department is a member of the National Consumer Telecom and Utilities Exchange (NCTUE), a consortium of over 95 member companies from the telecommunications, utilities and pay TV industries. NCTUE provides members with credit risk verification services designed specifically for utility companies.").

[273] Thomson Reuters, CLEAR Utility Filing (July 2020), https://drive.google.com/file/d/1R2i1fkW1TMLG75duQCpSlJhUFCEAqQ1a/view?usp=sharing; Thomson Reuters Response to 22033003 to Provide Online Legal Research to the Illinois Central Management Services, Thomson Reuters (June 12, 2014) http://www.purchase.state.il.us/ipb/master.nsf/all/D861DF95975DCE42862580360060EA32/$file/Pricing.pdf?OpenElement.

[274] Thomson Reuters, CLEAR Utility Filing (July 2020), https://drive.google.com/file/d/1R2i1fkW1TMLG75duQCpSlJhUFCEAqQ1a/view?usp=sharing.

[275] Equifax Insights, *Data-driven Credit & Risk Decisions with NCTUE(R)*, YouTube (Mar. 15, 2019), https://www.youtube.com/watch?v=L5waP7Ev1YU.

[276] Equifax Insights, *More Bang for Your Bucks with NCTUE(R)*, YouTube (Mar. 15, 2019), https://www.youtube.com/watch?v=yWdI1us2j8E.

[277] Equifax Enhances OneView™ Report for Businesses With Alternative Data Insights from DataX, Equifax (Oct. 25, 2021), https://investor.equifax.com/news-events/press-releases/detail/89/equifax-extends-service-agreement-with-national-consumer.

[278] Drew Harwell, *ICE investigators used a private utility database covering millions to pursue immigration violations*, Washington Post (Feb. 26, 2021), https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data.

[279] Sam Biddle, *LexisNexis to Provide Giant Database of Personal Information to ICE*, Intercept (Apr. 2, 2021), https://theintercept.com/2021/04/02/ice-database-surveillance-lexisnexis/.

[280] LexisNexis Risk Solutions, Collections and Recovery Products and Services (last visited Nov 27, 2021), https://www.secondalliance.com/wp-content/uploads/2017/11/LexisNexis.pdf.

[281] *See* Letter from Ron Wyden, U.S. Senator to The Hon. Rohit Chopra, Director, Consumer Financial Protection Bureau 2 (Dec. 8, 2021), https://www.washingtonpost.com/context/sen-wyden-letter-to-cfpb-on-sale-of-americans-utility-data/20df9dd1-bab1-4b2d-96f3-3b288c6d1905/. *See also* Drew Harwell, *Utility giants agree to no longer allow sensitive records to be shared with ICE*, Washington Post (Dec. 8, 2021), https://www.washingtonpost.com/technology/2021/12/08/utility-data-government-tracking/.

[282] *See* Letter from Ron Wyden, U.S. Senator to The Hon. Rohit Chopra, Director, Consumer Financial Protection Bureau 1 (Dec. 8, 2021), https://www.washingtonpost.com/context/sen-wyden-letter-to-cfpb-on-sale-of-americans-utility-data/20df9dd1-bab1-4b2d-96f3-3b288c6d1905/; @JustFuturesLaw, Twitter (Dec. 8, 2021), https://twitter.com/JustFuturesLaw/status/1468590605668425729.

[283] Drew Harwell, *Utility giants agree to no longer allow sensitive records to be shared with ICE*, Washington Post (Dec. 8, 2021), https://www.washingtonpost.com/technology/2021/12/08/utility-data-government-tracking/.

[284] Press Release, Office of Governor Gavin Newsom, Governor Newsom Takes Action on Legislation to Support California's Immigrant and Refugee Communities (Sept. 27, 2020), https://www.gov.ca.gov/2020/09/27/governor-newsom-takes-action-on-legislation-to-support-californias-immigrant-and-refugee-communities/.

[285] City News Service, *Newsom Signs Todd Gloria Bill to Limit ICE's Use of Customer Utility Data*, NBC San Diego (Sept. 28, 2020), https://www.nbcsandiego.com/news/local/newsom-signs-todd-gloria-bill-to-limit-ices-use-of-customer-utility-data/2414101/.

[286] Assemb. B. 2788, 2020-2021 Leg., Reg. Sess. (Cal. 2020) (Enacted) (codified at Cal Civ. Code § 1798.98), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB2788 ("An electrical corporation or gas corporation shall not sell a customer's electrical or gas consumption data or any other personally identifiable information for any purpose.").

[287] City News Service, *supra* note 285.

[288] Equifax Insights, *What is the NCTUE?*, YouTube (Oct. 13, 2020), https://www.youtube.com/watch?v=PqAZ5uoRsg0 (2:24) (indicates that 50.2% of CA residents' information is in the NCTUE database.).

[289] Federal Trade Commission, Individual Reference Services - A Report To Congress (1997), https://www.ftc.gov/reports/individual-reference-services-report-congress.

290. According to one study from 1996, approximately 1 in 3 Americans opted to have their phone company keep them unlisted. *Id.* at n.142 (citing Paul M. Schwartz & Joel R. Reidenberg, Data Privacy Law, Michie Law Publishers, Charlottesville, VA, 1996).

291. *Id.*

292. Notice of Termination of IRSG, WayBack Machine (last visited Nov. 27, 2021) http://web.archive.org/web/20020202103820/www.irsg.org/html/termination.htm ("It doesn't make sense to maintain a self-regulatory program when this information is now regulated under the Gramm-Leach-Bliley Ac . . . All IRSG members have agreed to continue to abide by the IRSG data use principles for data collected prior to July 1, 2001.").

293. *See, e.g.*, In re Trans Union Corp., 9255, 200 WL 257766 (F.T.C., Feb. 10, 2000).

294. *See* Uriel J. Garcia, *ICE arrests young immigrant's sponsor months after feds assured him he'd be safe*, Santa Fe New Mexican (Sept. 9, 2017), https://www.santafenewmexican.com/news/local_news/ice-arrests-young-immigrant-s-sponsor-months-after-feds-assured/article_428366f5-6d03-552c-a277-93b83d3005e2.html.

295. This passage is adapted from a translator's 2017 description of the standard ORR intake process. *See* Valeria Luiselli, *Tell Me How It Ends: An Essay in 40 Questions* 49 (2017).

296. *See* Garcia, *supra* note 294.

297. Department of Health and Human Services, Administration for Children and Families Budget Request 58 (2020), https://www.acf.hhs.gov/sites/default/files/documents/olab/acf_congressional_budget_justification_2020.pdf.

298. While many unaccompanied children are arriving at the border to claim asylum, many have stronger claims to relief under special immigrant juvenile protections. In fact, the vast majority of children arriving at the border have a claim to international protection. *See generally* United Nations High Commissioner for Refugees Regional Office for the United States and the Caribbean, *Children on the Run*, United Nations High Commissioner for Refugees (March 2014), https://www.unhcr.org/en-us/children-on-the-run.html.

299. Reno v. Flores, 507 U.S. 292 (1993).

300. Stipulated Settlement Agreement, Flores v. Reno, No. CV 85-4544- RJK(Px) (C.D. Cal. Jan. 17, 1997), *available at* https://www.aclu.org/sites/default/files/assets/flores_settlement_final_plus_extension_of_settlement011797.pdf.

301. Homeland Security Act of 2002 § 462, 6 U.S.C. § 279.

302. Trafficking Victims Protection Reauthorization Act (TVPRA) of 2003, Pub. L. No. 110-457, § 235(b)(3), 117 Stat. 5077 (2008).

303. TVPRA, § 235(c)(2).

304. *See id.*

305. *See* J.E.C.M. v. Lloyd, 352 F. Supp. 3d 559, 573–74 (E.D. Va. 2018); Government Accountability Office, GAO-19-163, Unaccompanied Children: Agency Efforts to Reunify Children Separated from Parents at the Border 9 (2018), https://www.gao.gov/reports/GAO-19-163/.

306. *See* Government Accountability Office, GAO-19-163, *supra* note 305 at 9–10.

307. *Id.* at 10.

308. Family Separation FOIA Response from ICE Key Documents, American Immigration Council 276 (2019), https://www.americanimmigrationcouncil.org/sites/default/files/foia_documents/family_separation_foia_request_ice_production_03.08.19.pdf.

309. National Immigration Law Center, Nlets: Questions and Answers 9 (Nov. 2020), https://www.nilc.org/wp-content/uploads/2020/11/Nlets-Q-and-A.pdf; *Family Separation FOIA Response from ICE Key Documents*, American Immigration Council 280 (2019) https://www.americanimmigrationcouncil.org/sites/default/files/foia_documents/family_separation_foia_request_ice_production_03.08.19.pdf.

310. Family Separation FOIA Response from ICE Key Documents, American Immigration Council 280 (2019), https://www.americanimmigrationcouncil.org/sites/default/files/foia_documents/family_separation_foia_request_ice_production_03.08.19.pdf; *see* Mijente, National Immigration Project & Immigrant Defense Project, *Who's Behind ICE?: The Tech and Data Companies Fueling Deportations* 31–32 (2018), https://mijente.net/wp-content/uploads/2018/10/WHO'S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf.

311. John Burnett, *ICE Has Arrested More Than 400 In Operation Targeting Parents Who Pay Smugglers*, NPR (Aug. 18, 2017), https://www.npr.org/2017/08/18/544523231/arrests-of-undocumented-parents-sparks-debate-between-federal-officials-and-immi.

312. *Id.*

313. *See* Neena Satija, Karoun Demirjian, Abigail Hauslohner & Josh Dawsey, *A Trump administration strategy led to the child migrant backup crisis at the border*, Washington Post (Nov. 12, 2019), https://www.washingtonpost.com/immigration/a-trump-administration-strategy-led-to-the-child-migrant-backup-crisis-at-the-border/2019/11/12/85d4f18c-c9ae-11e9-a1fe-ca46e8d573c0_story.html (The enhanced vetting of sponsors and the sharing of information between child welfare and immigration authorities . . . "caused thousands of unaccompanied minors to be stranded in U.S. custody and exacerbated the appearance of a crisis on the southern border"); *see also, e.g.,* Robert Moore, *Border Patrol argues child treatment at Clint migrant facility not as described, gives access to Texas station*, Washington Post (June 16, 2019), https://www.washingtonpost.com/immigration/border-patrol-argues-child-treatment-at-clint-migrant-facility-not-as-described-gives-access-to-texas-station/2019/06/26/69f1b754-9879-11e9-916d-9c61607d8190_story.html ("Lawyers and health-care workers who visited the Clint Border Patrol station earlier this month described 'appalling' conditions for unaccompanied minors who have been held here because of overcrowding in special shelters designed for children.").

314. *See generally* Letter from National Immigration Justice Center, Kids in Need of Defense, Lutheran Immigration

and Refugee Service, Catholic Legal Immigration Network, Inc., Women's Refugee Commission, Refugee and Immigrant Center for Education and Legal Services, Americans for Immigrant Justice & Make the Road New Jersey to Cameron Quinn, Officer of Civil Rights & Civil Liberties at Department of Homeland Security & John Kelly, Acting Inspector General at Department of Homeland Security (Dec. 6, 2017), https://immigrantjustice.org/sites/default/files/content-type/press-release/documents/2017-12/Sponsor%20Enforcement-OIG_CRCL_Complaint_Cover_Letter-FINAL_PUBLIC.pdf.

315. *See* Senator Jeff Merkley, *Merkley Reveals Secret Trump Administration Plan to Create Border Crisis*, Medium (Jan. 17, 2019), https://medium.com/@SenJeffMerkley/merkley-reveals-secret-trump-administration-plan-to-create-border-crisis-f72a7c3de2bd.

316. Memorandum of Agreement between the Office of Refugee Resettlement of the U.S. Department of Health and Human Services and U.S. Immigration and Customs Enforcement and U.S. Customs and Border Protection of the U.S. Department of Homeland Security Regarding Consultation and Information Sharing in Unaccompanied Alien Children Matters (Apr. 13, 2017) (on file with the House Committee on Energy & Commerce) https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/%2316%20-%202018.04.13%20MOA%20between%20HHS%20and%20DHS.pdf.

317. Immigration and Customs Enforcement Oversight Hearing: Hearing before the U.S. House of Representatives Committee on Appropriations, Subcommittee on Homeland Security (July 25, 2019) (statement of Matthew T. Albence), https://www.c-span.org/video/?463002-1/immigration-customs-enforcement-oversight-hearing.

318. Women's Refugee Commission & National Immigrant Justice Center, *Children as Bait: Impacts of the ORR-DHS Information-Sharing Agreement* (Mar. 2019), https://immigrantjustice.org/sites/default/files/content-type/research-item/documents/2019-03/Children-as-Bait.pdf.

319. *See* National Coalition of State Legislatures, Detention of Migrant Children (Nov. 24, 2020), https://www.ncsl.org/research/immigration/detention-of-migrant-children.aspx.

320. Caitlin Dickerson, *Detention of Migrant Children Has Skyrocketed to Highest Levels Ever*, N.Y. Times (Sept. 12, 2018), https://www.nytimes.com/2018/09/12/us/migrant-children-detention.html.

321. Examining the Trump Administration's Care for Unaccompanied Children: Hearing before the U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Oversight and Investigation 3 (Sept. 19, 2019) (testimony of John R. Modlin, Acting Deputy Chief of Law Enforcement Operational Programs at U.S. Border Patrol, U.S. Customs and Border Protection), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony%20-%20Modlin%20OI%2020190919.pdf (In June 2019, there were nearly 2,600 unaccompanied minors held in Border Patrol stations, roughly half of which were in custody for 72 hours or more).

322. *See* Letter to Secretary Kirstjen M. Nielsen, U.S. Department of Homeland Security, and Secretary Alex Azar, U.S. Department of Health & Human Services (Nov, 28, 2018), http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/govinfo/DHSLetter11.28.18.pdf.

323. Consolidated Appropriations Act of 2019, H.J.Res.31, 116th Cong. § 9 (2019), https://www.congress.gov/bill/116th-congress/house-joint-resolution/31/text.

324. Memorandum of Agreement between the Office of Refugee Resettlement of the U.S. Department of Health and Human Services and U.S. Immigration and Customs Enforcement and U.S. Customs and Border Protection of the U.S. Department of Homeland Security Regarding Consultation and Information Sharing in Matters Relating to Unaccompanied Children (Mar. 11, 2021) (on file with the American Immigration Lawyers Association) https://www.aila.org/infonet/dhs-and-hhs-terminate-2018-agreement-regarding.

325. Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the Chilling Effect*, 58 B.U.L.Rev. 685, 685–732 (1978).

326. Daniel J. Solove, *A Taxonomy of Privacy,* 154 U. Pa. L. Rev. 491–499 (2006).

327. Sarah Brayne, *Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment*, 79 Am. Socio. Rev. 367–391 (2014).

328. Asad L. Asad, *On the Radar: System Embeddedness and Latin American Immigrants' Perceived Risk of Deportation*, 54 L. & Soc'y Rev. 133–167 (2020).

329. Sarah Desai, Jessica Houston Su & Robert M. Adelman, *Legacies of Marginalization: System Avoidance among the Adult Children of Unauthorized Immigrants in the United States*, International Migration Rev. (Dec. 11 2019).

330. Jeffrey S. Passel & D'Vera Cohn, *U.S. Unauthorized Immigrant Total Dips to Lowest Level in a Decade*, Pew Research Center (Nov. 27 2018), https://www.pewresearch.org/hispanic/2018/11/27/u-s-unauthorized-immigrant-total-dips-to-lowest-level-in-a-decade/.

331. Mónica Ruiz-Casares, Cécile Rousseau, Ilse Derluyn, Charles Watters & François Crépeau, *Right and Access to Healthcare for Undocumented Children: Addressing the Gap Between International Conventions and Disparate Implementations in North America and Europe*, 70 Soc. Sci. & Med. 329–36 (2010).

332. K. Alaimo, C.M. Olson, E.A. Frongillo Jr., & R.R. Briefel, *Food Insufficiency, Family Income, and Health in U.S. Preschool and School-Aged Children*, 13 Fam. Econ. & Nutrition Rev. 44–53 (2001).

333. Stephanie Potochnick, Jen-Hao Chen & Krista Perreira, *Local-Level Immigration Enforcement and Food Insecurity Risk among Hispanic Immigrant Families with Children: National-Level Evidence*, 19 J. Immigrant & Minority Health 1042–1049 (2017).

334. Karen Hacker, Maria Anies, Barbara L. Folb, & Leah Zallman, *Barriers to Health Care for Undocumented Immigrants: A Literature Review*, 8 Risk Mgmt. & Healthcare Pol'y 175–83 (2015).

335. David Navas & Dede de Percin, *Decline in Access to Healthcare through Safety-Net Clinics by Immigrants and Refugees in Denver*, Mile High Health Alliance (2018), http://milehighhealthalliance.org/wp-content/uploads/2018/03/Immigrant-Health-Drop-Off-Report-FINAL-3.18.pdf.

336. Francisco I. Pedraza, Vanessa Cruz Nichols & Alana M. W. LeBrón, *Cautious Citizenship: The Deterring Effect of Immigration Issue Salience on Health Care Use and Bureaucratic Interactions among Latino US Citizens*, 42 (5) J. Heath Pol. Pol'y & L. 925–60 (2017).

337. Hamutal Bernstein, Dulce Gonzalez, Michael Karpman & Stephen Zuckerman, *Adults in Immigrant Families Report Avoiding Routine Activities Because of Immigration Concerns*, Urban Institute (Jul. 24, 2019), https://www.urban.org/research/publication/adults-immigrant-families-report-avoiding-routine-activities-because-immigration-concerns.

338. Tom K. Wong, Karina Shklyan, Anna Isorena & Stephanie Peng, *The Impact of Interior Immigration Enforcement on the Day-to-Day Behaviors of Undocumented Immigrants*, US Immigration Policy Center & UC San Diego (Apr. 3, 2019), https://usipc.ucsd.edu/publications/usipc-working-paper-1.pdf.

339. Hearing on S.B. 649 Before the M.D. Senate Judicial Proceedings Committee (Feb. 27, 2020) (statement of Maribel Cortez at 1:42:35).

340. *See* Erin Cox, *Gov. Hogan opposed to ending ICE's warrantless access to driver's license database*, Washington Post (Feb. 27, 2020), https://www.washingtonpost.com/local/md-politics/hogan-opposes-blocking-ice-from-drivers-licenses/2020/02/27/3e23bbcc-5903-11ea-9000-f3cffee23036_story.html.

341. *See, e.g.,* National Immigrant Justice Center, The New Way Forward Act: A Path Toward An Immigration System Based In Dignity and Racial Justice (2021), https://immigrantjustice.org/issues/new-way-forward-act-path-toward-immigration-system-based-dignity-and-racial-justice.

342. *See generally* The Census Act, 13 U.S.C. §1 et seq. (in particular §8 and §9); The Confidential Information Protection and Statistical Efficiency Act (CIPSEA), 44 U.S.C. §3501, Note; The Privacy Act, 5 U.S.C. §552a; The Internal Revenue Code, 26 U.S.C. §1 et seq. *See also* Kelly Percival, *Federal Laws That Protect Confidentiality*, Brennan Center for Justice (Feb. 20, 2019), https://www.brennancenter.org/our-work/research-reports/federal-laws-protect-census-confidentiality (overview of Census confidentiality laws).

343. *See* 13 U.S.C. §9(a)(1) (prohibiting "use the information furnished under the provisions of this title for any purpose other than the statistical purposes for which it is supplied"); §8(c) ("In no case shall information furnished under this section be used to the detriment of any respondent or other person to whom such information relates, except in the prosecution of alleged violations of this title.").

344. *See Table 39 Aliens Removed or Returned: Fiscal Years 1892 to 2019*, Department of Homeland Security (Oct. 28, 2020), https://www.dhs.gov/immigration-statistics/yearbook/2019/table39; U.S. Immigration and Customs Enforcement, History of ICE (Jan, 29, 2021), https://www.ice.gov/history.

345. *See* U.S. Department of Homeland Security, DHS/ICE/PIA-054, Privacy Impact Assessment for the ICE Use of Facial Recognition Services 22 (May 13, 2020) https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf.

346. *See* Mark Hugo Lopez, Jeffrey S. Passel & D'Vera Cohn, *Key facts about the changing U.S. unauthorized immigrant population*, Pew Research Center (Apr. 13, 2021), https://www.pewresearch.org/fact-tank/2021/04/13/key-facts-about-the-changing-u-s-unauthorized-immigrant-population/ ("From 2007 to 2017, the share of newly arrived unauthorized immigrants (those in the U.S. five years or less) from regions other than Central America and Mexico—the vast majority of whom are overstays—increased from 37% to 63%."); 8 U.S.C. § 1325(a) (misdemeanor of improper entry).

347. *See generally* Patrick Grother, Mei Ngan & Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, National Institute of Standards and Technology (Dec. 19, 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

348. *See generally, e.g.*, Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Face Recognition in America* (Oct. 16, 2016), https://www.perpetuallineup.org; Clare Garvie, *Garbage In, Garbage Out* (May 16, 2019), https://www.flawedfacedata.com; Clare Garvie & Laura Moy, *America Under Watch* (May 16, 2019), https://www.americaunderwatch.com/.

349. *See, e.g.,* Kashmir Hill, *Wrongfully Accused by an Algorithm*, New York Times (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, New York Times (Dec. 29, 2020), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html; Jeremy C. Fox, *Brown University student mistakenly identified as Sri Lanka bombing suspect*, Boston Globe (Apr. 28, 2019), https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html.

350. *See*, *e.g.*, Asad L. Asad, *On the Radar: System Embeddedness and Latin American Immigrants' Perceived Risk of Deportation* 54 L. & Soc. Rev. 135 ("Documentation affords some protection from deportation, but it can also heighten fears since the bureaucracies that 'document' immigrants have a greater perceived ability to surveil and expel them."); *id* at 162 ("Perceived legibility to the US immigration regime may sometimes result in system avoidance, as was the case for Josefina who viewed DACA as a pathway to her 'capture'"); *see also* Karen Hacker et al., *Barriers to Health Care for Undocumented Immigrants*, 8 Risk Mgmt. & Healthcare Pol'y 178 (2015) (Literature review showing that "[u]ndocumented immigrants reported avoiding health care and waiting until health issues were critical to seek services because of their concerns of being reported to authorities. This was seen in countries as diverse as France, the US, and Denmark.").

351. *See supra* Section III; Drew Harwell, *ICE investigators used a private utility database covering millions to pursue immigration violations*, Washington Post (Feb. 26, 2021), https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data.

[352] *See supra* Section II.

[353] Statement by the President, The White House (June 7, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/06/07/statement-president ("Now, the programs that have been discussed over the last couple days in the press are secret in the sense that they're classified. But they're not secret in the sense that when it comes to telephone calls, every member of Congress has been briefed on this program.").

[354] Jim Sensenbrenner, *This abuse of the Patriot Act must end*, The Guardian (Jun 9, 2013), https://www.theguardian.com/commentisfree/2013/jun/09/abuse-patriot-act-must-end.

[355] *See, e.g.*, U.S. Courts, *Wiretap Report 2020* (Dec. 31, 2020), https://www.uscourts.gov/statistics-reports/wiretap-report-2020.

[356] There are federal statutes that purport to prohibit state and local governments from themselves prohibiting the sharing if immigration status information with the federal government. Scholars, and recently some judges, have pointed out the questionable constitutionality of such statutes, and to date efforts to invoke them to limit the reach of sanctuary policies through the courts have had little success. But state and local policymakers should be aware of the existence of such laws and take steps to craft legislation and policy that will avoid running afoul of them.

[357] *See* The Sanctuary Values Act, D.C. Code § 24–211.07(a) (2020), *available at* https://code.dccouncil.us/us/dc/council/code/sections/24-211.07.html.

[358] *See, e.g.,* U.S. Immigration and Customs Enforcement, National Intellectual Property Rights Coordination Center (Jan. 12, 2021), https://www.ice.gov/partnerships-centers/iprc.

[359] *See* The Maryland Driver Privacy Act, H.B. 23 §4-320(g)(2) (2021) (restricting sharing of driver data "to a federal agent or federal agency for the purpose of federal immigration enforcement"); *id.* at §4-320.1(B)(1) & (B)(2) (restricting access to face recognition systems by "any federal agency seeking access for the purpose of enforcing federal immigration law").

[360] *See* New York Vehicle & Traffic Code, Ch. 71, Title 2, Art. 2, §201 at 12(b).

[361] *See* Improper Entry by Alien, 8 U.S.C. §1325; Robert Warren, *US Undocumented Population Continued to Fall from 2016 to 2017, and Visa Overstays Significantly Exceeded Illegal Crossings for the Seventh Consecutive Year*, Center for Migration Studies (Jan. 16, 2019), https://cmsny.org/publications/essay-2017-undocumented-and-overstays/.

[362] *See* Hawaii Rev. Stat. § 286-104.5(h).

[363] *See*, *e.g.*, The Public Information Act, Md. Code Ann. § 4-101, at (j)(3) (excluding from the definition of "public record" digital images stored by the Maryland Motor Vehicle Administration).

[364] *See* Cal. Gov. Code, Title 1, Div. 7, Ch. 15.25 at § 7284.6(a)(1)(D) (a restriction against law enforcement sharing of residents' addresses added by the California Values Act, SB 54, 2017); Cal. Veh. Code, Div. 6, Ch. 1, Art. 3, § 12801.9(j) (prohibition against sharing driver data, "except as required by law," as added by SB 244, 2018); Cal. Gov. Code, Title 2, Div. 3, Part 6, Ch. 2.5 at § 15160(b)(1) (clarifying that no users of the California Law Enforcement Telecommunications System may use it to access driver data or to enforce certain provisions of immigration law, added by AB 1747, 2019).

[365] *See* Cal. Veh. Code, Div. 2, Art. 1, Ch. 3 at § 1810.5. *See* Letter from Sonia Huestis, Deputy Dir., Commc'ns Programs Div., California Dep't of Motor Vehicles, to the Hon. Lorena Gonzalez, California Gen. Assembly (Feb. 4, 2019) (on file with Voice of San Diego); Maya Srikrishnan, *How California Laws Meant to Integrate Immigrants Can Open a Backdoor for ICE*, Voice of San Diego (Feb. 19, 2019), https://www.voiceofsandiego.org/topics/news/how-california-laws-meant-to-integrate-immigrants-can-open-a-backdoor-for-ice/ (explaining context of letter).

[366] *See* Hearing before the Maryland House of Delegates Environment & Transportation Committee (Feb. 27, 2020) (Testimony of Del. Dana Stein, D - Baltimore County, Dist. 11, for H.B. 892) ("Prior to a visit to the Department last year it had been my understanding that the Department could not determine when ICE was accessing MIRS. But during a legislative visit last October we were told that the Department in fact can determine when ICE accesses the system and we received a follow-up letter from the Department confirming that.").

[367] 8 U.S.C. § 1373 (2006).

[368] Amy Howe, *Court dismisses "sanctuary cities" petitions*, SCOTUSblog (Mar. 5, 2021), https://www.scotusblog.com/2021/03/court-dismisses-sanctuary-cities-petitions/.

[369] *See, e.g.,* California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100 et seq. (Ca. 2018); Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1301 et seq. (Co. 2021); Consumer Data Protection Act, H.B. 2307 (Va. 2021).

[370] National Consumer Telecom and Utilities Exchange, *Consumers*, https://nctue.com/consumers (last visited Nov. 30, 2021) ("National Consumer Telecom & Utilities Exchange (NCTUE) is a credit reporting agency that maintains data, such as payment and account history, reported by member service providers in the telecommunications, pay TV, and utility industries.").

[371] *See, e.g.,* Ariz. Admin. Code R14-2-203 (2021) ("2. Customer-specific information shall not be released without specific prior written customer authorization unless the information is . . . reasonably required for legitimate account collection activities, or is necessary to provide safe and reliable service to the customer"); Code Del. Regs. 26 3001 ("3.3.4 An Electric Supplier may disclose a Customer's billing, payment, and credit information for the sole purpose of facilitating billing, bill collection, and credit reporting."); Md. Code Regs. 20.53.07.02 ("B. A supplier may disclose a customer's billing, payment, and credit information for the sole purpose of facilitating billing, bill collection, and credit reporting.").

[372] *See, e.g.*, Colo. Code Regs. § 723-3:3027(b) (regulating electric utility companies: "A utility shall not disclose customer data unless such disclosure conforms to these rules, except as required by law or to comply with Commission rule. Illustratively, this includes responses to

requests of the Commission, warrants, subpoenas, court orders, or as authorized by § 16-15.5-102, C.R.S."); 4 Colo. Code Regs. § 723-3:3001(i) ("'Customer data' means customer-specific data or information, excluding personal information as defined in paragraph 1004(x) . . ."); 4 Colo. Code Regs. § 723-1:1004(x) ("'Personal information' means the following: . . . customer's name only in combination with any one or more other enumerated data elements that relate to such customer . . . .").

373. *See* Conn. Agencies Regs. 16-47a-1 at (3) (explicitly defining "customer information" to include address); Conn. Agencies Regs. 16-47a-3 at (b) ("Except as otherwise allowed under this Gas Code of Conduct, no gas company or affiliate shall not disclose customer information to any person or company, without the customer's consent, and then only to the extent specified by the customer."); at (f) ("Notwithstanding the prohibitions established in this section, a gas company may disclose customer information to an affiliate (including a CSC) or non-affiliated third party each without customer consent, but only to the extent necessary for the affiliate or non-affiliated third party to provide goods or services (including shared corporate support services such as customer service, billing and collection services) to the gas company and upon their explicit agreement to protect the confidentiality of such customer information.").

374. The Biden Plan for Securing Our Values as a Nation of Immigrants, Biden for President, https://joebiden.com/immigration/.

375. Nick Miroff & Maria Sacchetti, *Immigration arrests fell to lowest level in more than a decade during fiscal 2021, ICE data shows*, Washington Post (Oct. 26, 2021), https://www.washingtonpost.com/national/ice-arrests-biden-trump/2021/10/25/f33130b8-35b5-11ec-9a5d-93a89c74e76d_story.html.

376. ICE as an Awarding Agency—Fiscal Year 2008–2021, https://www.usaspending.gov/search/?hash=78b38388cb2a2618d0fcce25b2ddbae5.

377. USAspending, About, https://www.usaspending.gov/about.

378. WatchBlog, *USAspending.Gov Contains a Treasure Trove of Information, But How Reliable Is It?*, WatchBlog: Official Blog of the U.S. Government Accountability Office (Aug. 13, 2020), https://blog.gao.gov/2020/08/13/usaspending-gov-contains-a-treasure-trove-of-information-but-how-reliable-is-it/.; U. S. Government Accountability Office, *Data Act: Quality of Data Submissions Has Improved but Further Action Is Needed to Disclose Known Data Limitations*, https://www.gao.gov/products/gao-20-75 (last visited Jun. 21, 2021). *See also* Jack Poulson, *Reports of a Silicon Valley/Military Divide Have Been Greatly Exaggerated*, TechInquiry (July 7, 2020), https://techinquiry.org/SiliconValley-Military/ ("While FPDS is the definitive source for US federal procurement data, it is known to have numerous shortcomings, such as inconsistencies and and inaccuracies in award amounts, slow and incomplete uploads from contract officers (including 90 day delays for DoD procurement), and corrections frequently taking place years after the signing data.").

379. USAspending gathers its data from the Federal Procurement Data System (FPDS) which shares no data on ICE's actual payouts or *outlays*. As a result, ICE's outlays are not included in awards data. *See* Analyst's Guide to Federal Spending Data, USAspending Data Lab, https://datalab.usaspending.gov/analyst-guide/ (last visited Jun. 21, 2021).

380. An obligation is "a promise made by the government to spend funds." *Id.*

381. *See* Poulson, *supra* note 378.

382. *See* Appendix B.

383. USAspending, https://www.usaspending.gov/.

384. We decided on these categories as we looked at ICE surveillance contracts and noticed common surveillance functionalities procured by ICE.

385. *See, e.g.,* National Immigration Law Center, Glossary at a Glance: Immigration Databases, Information Sharing Systems, and Case Management Systems (Aug. 2021), https://www.nilc.org/wp-content/uploads/2018/01/databases-glossary.pdf; Mijente, National Immigration Project & Immigrant Defense Project, *Who's Behind ICE?: The Tech and Data Companies Fueling Deportations* (2018), https://mijente.net/wp-content/uploads/2018/10/WHO'S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf; Simon Migliano & Samuel Woodhams, *ICE Surveillance Technology Spending Report*, Top10VPN (Feb. 2, 2021), https://www.top10vpn.com/research/ice-surveillance-contracts/.

386. Any given contract may have multiple transactions associated with it. Whenever we flagged any transaction as relating to surveillance functionality, we flagged the entire contract.

387. *See* Electronic Frontier Foundation, Street-Level Surveillance (Aug. 28, 2017), https://www.eff.org/pages/cell-site-simulatorsimsi-catchers.

388. U.S. Census Bureau, North American Industry Classification System (Jan. 5, 2022), https://www.census.gov/naics/.

389. U.S. General Services Administration, Federal Procurement Data System Product and Services Codes (PSC) Manual (Oct. 2010), https://www.acquisition.gov/sites/default/files/manual/October%202020%20PSC%20Manual.pdf; *See also* FPDS, FPDS-NG FAQs, https://beta.fpds.gov/wiki/index.php/FPDS-NG_FAQs.

390. OpenRefine Documentation, Cluster and edit, https://docs.openrefine.org/manual/cellediting#cluster-and-edit.

391. Jack Poulson, Vendor to Parents, https://gitlab.com/tech-inquiry/gov-contract-embeddings/-/blob/fc0e4eda2e8ae05fac8a698117c746a551713847/data/vendor_to_parents.json.

392. USAspending, Contract Summary: NCS Technologies Incorporated, https://www.usaspending.gov/award/CONT_AWD_HSCETE12J00279_7012_HSHQDC07D00028_7001.

393. USAspending, Contract Summary: DTC Communications, Inc., https://www.usaspending.gov/award/CONT_AWD_HSCEMD12F00070_7012_DJD11C0002_1524.

394. Cobham, Product Quick Guide (Feb. 2014), https://www.cobham.com/media/1078613/Cobham_TCS_QuickGuide_Mar14.pdf.

395. USAspending, Contract Summary: Four Points Technology, L.L.C., https://www.usaspending.gov/award/CONT_AWD_70RCSA20FR0000097_7001_HSHQDC13D00003_7001.

396. Letter from Craig L. Caesar to Assistant Attorney Gen. Hon. Charles A. James 3 (Aug. 17, 2001), https://www.justice.gov/atr/page/file/1019991/download ("the Founding Members of what will become NCTUE are the following: AT&T Corp.; BellSouth Telecommunications, Inc.; Citizens Communications, Inc; Global Crossing, Inc.; Broadwing Communications, Inc.; Verizon Long Distance Company; Sprint Communications Company LP and MCI Telecommunications, Inc."); Equifax Insights, *More Bang for Your Bucks with the NCTUE(R)*, Youtube (Mar. 15, 2019), https://www.youtube.com/watch?v=yWdI1us2j8E.

397. NCTUE Users Conference: We're Better Together 2 (Nov. 2015), https://www.nctue.com/userimages/2015_NCTUE_Users_Conference_Agenda.pdf.

398. Letter from Craig L. Caesar, *supra* note 396; Equifax Insights, *More Bang for Your Bucks with the NCTUE(R)*, *supra* note 396. Some Verizon branches appear to not have had membership in NCTUE. For example, Verizon New York Inc.'s request to join NCTUE in 2016 was denied. State of New York Public Service Commission, CASE 13-C-0154—Petition of Verizon New York Inc. for Clarification or Waiver of Commission Requirements Related to the Provision of Customer Information to Credit Reporting Agencies (Apr. 22, 2016), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId=%7BB4A93370-7B4C-43EF-AC41-B6963122089C%7D.

399. Letter from Craig L. Caesar, *supra* note 396.

400. *Id.*

401. *Id.*

402. Equifax Insights, *supra* note 396.

403. Letter from Craig L. Caesar, *supra* note 396, at 3 n.4 (These designees represent American Electric Power; Baltimore Gas & Electric; Duke Power; and Southern Company, companies that have been active in the regional utility exchanges.").

404. *Id.*

405. *Id.*

406. Equifax, NCTUE Association Infographic, http://assets.equifax.com/assets/corp/nctue-association-infographic.pdf ("Along with lowering write-offs by $1,000,000, Georgia Power used NCTUE to anticipate results to help avoid debt").

407. *Id.* ("With this matched information from NCTUE, PSNC Energy has found that their contact rate is 41 percent higher than before.").

408. Equifax Insights, *supra* note 396.

409. NCTUE Users Conference: We're Better Together, *supra* note 397.

410. Equifax Insights, *supra* note 396.

411. NV Energy uses the Equifax Advanced Energy Risk Model to evaluate customer credit risk. Public Utilities Commission of Nevada, Response of Nevada Power Company d/b/a NV Energy and Sierra Pacific Power Company d/b/a NV Energy to Procedural Order No. 1 8 (Oct. 7, 2016), https://drive.google.com/file/d/1Jnf_Vny3n1xcKkpgp3l3HTN53Drjp-ev/view?usp=sharing. According to a product sheet from Equifax, the Advanced Energy Plus score draws on NCTUE data and is only accessible to NCTUE members. Equifax, Advanced Energy Plus (Mar. 3, 2017), https://resources.datadrivenmarketing.equifax.com/collateral/advanced-risk-score-for-utilities-product-sheet-2.

412. Michigan Public Service Commission, Consumers Energy Company Summary of Electric Benefits O&M Expenses for the years 2015, 2016, 2017 and 12 Months Ended September 30, 2018 7 (Mar. 2017), https://mi-psc.force.com/sfc/servlet.shepherd/version/download/068t0000001UXldAAG ("Using a combination of data in the NCTUE database (National Consumer Telecom & Utilities Experience [sic]) along with historical information in SAP, this project will use a risk scoring model to reduce our exposure by collecting money before they move in and target our higher risk customer with a more aggressive dunning procedure.").

413. Miami-Dade County Water and Sewer Department, Contract/Project Measure Analysis and Recommendation for Credit and Risk Assessment Services, Miami-Dade County (Mar. 22, 2019), http://www.miamidade.gov/smallbusiness/library/reports/sbe/bw9744-0-22-project-package.pdf (Miami-Dade County's Water and Sewer Department is a member of the National Consumer Telecom and Utilities Exchange (NCTUE), a consortium of over 95 member companies from the telecommunications, utilities and pay TV industries. NCTUE provides members with credit risk verification services designed specifically for utility companies.").

414. Duke Energy, *Duke Energy notifying Midwest customers of payment reporting error*, Duke Energy News Center (Oct. 7, 2014), https://news.duke-energy.com/releases/duke-energy-notifying-midwest-customers-of-payment-reporting-error (Duke Energy "no longer reports payment data to NCTUE, D&B or ECS. All information previously reported to NCTUE has been blocked and can no longer be used by others for credit-related decisions").

415. Before the Minnesota Office of Administrative Hearings for the Minnesota Public Utilities Commission In the Matter of the Application of Minnesota Energy Resource Corporation for Authority to Increase Rates for Natural Gas Utility Service in Minnesota 105 (Mar. 18, 2016), https://www.edockets.state.mn.us/EFiling/edockets/searchDocuments.do?method=showPoup&documentId=%7B0BE6F0A7-DEC7-42D5-9BC9-B626E74F4BDE%7D&documentTitle=20163-119256-01 ("However, in order to ensure compliance with the Minnesota Public Utilities Commission's June 24, 2014 Order Requiring Utilities to Adopt and Document Processes Regarding Personally Identifiable Information and Other Action and related Orders in Docket No. E,G999/CI-12-1344, MERC does not plan to participate in [NCTUE].").

GEORGETOWN LAW
Center on Privacy & Technology