REDES DE ARRASTRE AMERICANAS

DEPORTACIONES ACCIONADAS POR DATOS EN EL SIGLO XXI

GEORGETOWN LAW
Center on Privacy & Technology

www.americandragnet.org

10 DE MAYO DE 2022,
Actualizado en Mayo 2025 con un nuevo prólogo

Foto portada: Marisol sostiene a su hijo de 7 años mientras habla con abogados de inmigración en el Santa Fe Dreamers Project.
(Foto: Gabriela Campos/The New Mexican)

REDES DE ARRASTRE AMERICANAS

DEPORTACIONES ACCIONADAS POR DATOS EN EL SIGLO XXI

GEORGETOWN LAW
Center on Privacy & Technology

ACERCA DE ESTE INFORME

Nina Wang, Allison McDonald, Daniel Bateyko y Emily Tucker son los autores de este informe. Harrison Rudolph dirigió la investigación correspondiente.

CITA SUGERIDA

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).

INFORMACIÓN DE CONTACTO

privacy@georgetown.edu / 202-662-9779

DISEÑADO POR

Rootid

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

10 DE MAYO DE 2022

PRÓLOGO, MAYO 2025

Cuando publicamos el estudio *American Dragnet: Data-Driven Deportation in the 21st Century* en 2022, comprendíamos que algún día un representante del ejecutivo autoritario podría poner en marcha la infraestructura de vigilancia descrita en nuestro informe para coaccionar y controlar a la población de los EE. UU. a gran escala. No anticipamos que este día llegaría en tan sólo tres años. Teníamos la esperanza de que los hallazgos de nuestra investigación fueran útiles para las comunidades que se organizaban en contra de las acciones policiales migratorias y la vigilancia digital y que contribuyeran a generar un cambio en las políticas. Hoy en día, agentes federales con el rostro cubierto detienen a estudiantes en la calle a plena luz del día y el presidente se burla de una orden de la Suprema Corte para facilitar el regreso de un hombre deportado de manera ilegal a El Salvador mientras su administración amenaza con suspender el recurso de *habeas corpus*, por lo que esperar que la salvación provenga de un "cambio en las políticas" sería un consuelo sin sentido. Sería inútil esperar que la exposición de actos ilícitos o la revelación de brutalidad pudieran despertar al Congreso actual en beneficio de las personas. En cierto sentido, no hay nada más que revelar o exponer. O bien, para ser más precisos, la revelación y exposición de detalles nuevos no nos dicen nada adicional sobre la naturaleza de la situación política que estamos atravesando. La batalla actual no es para revelar la información correcta sino para comprender de manera adecuada el significado de la información que ya tenemos y enfrentar ese significado en conjunto.

Decidimos volver a publicar *American Dragnet* en este momento porque, si bien no tenemos hallazgos actualizados, el contexto presente exige un entendimiento actualizado de nuestros hallazgos originales.

En 2022 encontramos lo siguiente:

- El ICE había escaneado las fotografías de la licencia de conducir de 1 de cada 3 adultos.
- El ICE tenía acceso a los datos que aparecen en la licencia de conducir de 3 de cada 4 adultos.
- El ICE rastreaba los movimientos de los conductores en las ciudades en las que residían 3 de cada 4 adultos.
- El ICE podía ubicar a 3 de cada 4 adultos por medio de los registros de servicios públicos.
- El ICE construyó su red de vigilancia accediendo a datos de compañías privadas y administraciones estatales y locales.
- El ICE gastó aproximadamente $2.8 mil millones entre 2008 y 2021 en programas nuevos de vigilancia, obtención de datos y distribución de datos.

Dada la transgresión de la administración de Trump de las salvaguardas de los derechos civiles y la privacidad, tenemos la seguridad de que el porcentaje de personas cuya información se obtiene de los antecedentes de conducción y de los registros de servicios públicos a los que el ICE tiene acceso es mucho mayor actualmente. En meses recientes, también nos hemos enterado de que el DHS busca tener acceso a los datos de prácticamente cada nivel y categoría de administración gubernamental. Además de la muy publicitada solicitud de acceso a los datos del IRS por parte de la agencia, por ejemplo, el DHS también ha intentado acceder a una amplia base de datos de desempleo en Nuevo México[1] y a registros de una escuela primaria en Tennessee.[2]

Los corredores de datos y las empresas dedicadas a la minería de datos, cuyas excesivas ganancias siempre han provenido de manera parasitaria de los programas penitenciarios del estado, están recientemente desatados.

En abril, el ICE le asignó a Palantir un contrato por $30 millones para que le concediera al Gobierno la facultad de rastrear los movimientos de las personas con "una visibilidad casi en tiempo real."[3] En 2024, poco antes de la elección presidencial, el DHS celebró un contrato por $2 millones con la compañía israelí Paragon, que vende *spyware* que le permite al usuario acceder a información guardada en dispositivos celulares o transmitida mediante ellos[4] y que ha sido usada por los gobiernos en contra de periodistas y activistas violando así el derecho internacional de los derechos humanos.[5]

---

[1] Morgan Lee, *New Mexico denies ICE request for access to workforce data*, Associated Press (8 de agosto de 2019), https://apnews.com/general-news-393c3e48907b40d88f3313d7ff34184b.

[2] Steven Hale, *ICE sought student records from a Nashville elementary school*, Nashville Scene (10 de octubre de 2019), https://www.nashvillescene.com/news/pithinthewind/ice-sought-student-records-from-a-nashville-elementary-school/article_c787f8bd-c011-5ab5-bce9-f859bd6dc966.html [https://perma.cc/74T2-DAEY].

[3] Investigative Case Management - Additional Capabilities, SAM.gov, https://sam.gov/opp/f71acee6010c423db4902446a59a690c/view [https://perma.cc/J667-YPND]; PIID: 70CTD022FR0000170, Sistema Federal de Datos de Adquisiciones, https://www.fpds.gov/ezsearch/fpdsportal?q=PIID:%2270CTD022FR0000170%22&s=FPDS.GOV&templateName=1.5.3&indexName=awardfull&x=0&y=0&sortBy=SIGNED_DATE&desc=Y [https://perma.cc/ZTT6-LLQK]; Rosemarie Ho, *ICE just ordered $30 million worth of new technology from Palantir to track immigrants*, Business Insider (17 de abril de 2025), https://www.businessinsider.com/ice-palantir-new-technology-30-million-visa-overstays-self-deportation- 2025-4 [https://perma.cc/S78J-V6MP].

[4] Vas Panagiotopoulos, *ICE Signs $2 Million Contract With Spyware Maker Paragon Solutions*, WIRED (1 de octubre de 2024), https://www.wired.com/story/ice-paragon-solutions-contract/ [https://perma.cc/HF9U-VY85].

[5] Sandy Almarradweh, *Rights advocates raise concerns over Paragon spyware against journalists and activists in Europe*, JURIST (19 de marzo de 2025), https://www.jurist.org/news/2025/03/rights-advocates-raise-concerns-over-paragon-spyware-use-against-journalists-and-activists-in-europe/ [https://perma.cc/FZU8-VMS8].

Al leer *American Dragnet* en la actualidad y a la luz del momento histórico presente, surgen dos puntos importantes:

El primero es que es incorrecto considerar que lo que la administración de Trump hace en la actualidad es "cumplimiento de las normas de inmigración". Trump está haciendo uso de sus facultades en materia migratoria como vía para llevar a cabo las actividades de su fuerza policial militarizada, que actualmente está conformada por agentes del ICE y la CBP, así como de la policía local que, de manera oficial o no, ha sido designada para seguir las órdenes del Gobierno federal. El motivo por el invoca sus facultades en materia migratoria no es que esté llevando a cabo algo que razonablemente podría describirse como el cumplimiento de las leyes migratorias, sino porque estas facultades son un arma que puede blandir en muchas direcciones y con violencia sin tener que enfrentar obstáculos como la transparencia, la rendición de cuentas o los mecanismos de supervisión. La red de datos que se describe en el informe, y de la cual casi nadie puede escaparse ahora, no es el resultado colateral de los programas de vigilancia migratoria del DHS, sino que es el propósito evidente de dichos programas.

El segundo es que resistir la autocracia en la era digital va a requerir un concepto de la privacidad que vaya más allá de un derecho individual. La enorme cantidad de datos sobre las personas a la que tiene acceso el Gobierno, combinada con los productos a base de algoritmos que crean las compañías para hacer más eficiente la vigilancia a partir de datos, significa que cualquier nueva información que se conoce sobre una persona rápidamente genera información sobre muchas otras o sobre categorías enteras de personas. Debido a que Trump manipula cada base de datos que puede encontrar con el propósito explícito de perseguir e intimidar políticamente a las personas, el peligro no es sólo que se acose a personas específicas, sino que nuestra capacidad para actuar en conjunto como pueblo quedará destruida. Los movimientos no pueden crecer sin un espacio de seguridad mínima dentro del que puedan reunirse, deliberar y organizarse. A fin de crear esos espacios, tendremos que encontrar la forma de recuperar la privacidad, no principalmente como el derecho a estar en soledad, sino como el derecho de reunirnos en búsqueda del bien común.

ÍNDICE DE CONTENIDOS

RESUMEN EJECUTIVO 1

INTRODUCCIÓN: ROBERT BYRD Y JOSÉ HERNANDEZ 10

I. ICE CONSTRUYÓ SU RED DE VIGILANCIA Y ARRASTRE MEDIANTE LA ACUMULACION DE DATOS GENERADOS POR AGENCIAS BUROCRÁTICAS ESTATALES Y LOCALES. 19

II. ICE APROVECHA LA CONFIANZA QUE EXISTE EN LOS DEPARTAMENTOS DE VEHÍCULOS MOTORIZADOS DE LOS ESTADOS PARA REALIZAR DEPORTACIONES Y EVADIR LAS POCAS PROTECCIONES ESTABLECIDAS CONTRA ESA PRÁCTICA. 30

III. ICE APROVECHA LAS NECESIDADES BÁSICAS DE CALEFACCIÓN, ELECTRICIDAD Y AGUA DE LA GENTE AL RECOLECTAR EXPEDIENTES DE LOS SERVICIOS PÚBLICOS A TRAVÉS DE AGENCIAS DE DATOS POCO TRANSPARENTES OPERACIONES TURBIAS Y SIN REGULACIÓN. 48

IV. ICE ABUSÓ DE LA CONFIANZA DE MENORES SIN ACOMPAÑANTE Y DE SUS FAMILIARES CON EL FIN DE SEÑALAR A ESTOS ÚLTIMOS COMO BLANCOS DE DEPORTACIÓN. 63

CONCLUSIÓN Y RECOMENDACIONES 73

APÉNDICE 85

NOTA DE TRADUCCIÓN 94

AGRADECIMIENTOS 95

NOTAS FINALES 96

RESUMEN EJECUTIVO

Al pensar en la vigilancia gubernamental en Estados Unidos, es común que se nos venga a la mente la Agencia de Seguridad Nacional o el FBI. También podríamos pensar en una agencia policiaca poderosa, como el Departamento de Policía de Nueva York. Sin embargo, a no ser que usted o alguien que conoce haya sido blanco de una tentativa de deportación, es probable que no piense inmediatamente en el Servicio de Control de Inmigración y Aduanas (ICE, por sus siglas en inglés).

El argumento de este informe es que hay que hacerlo. Nuestra investigación de dos años, en la que se incluyen cientos de peticiones realizadas bajo la *Freedom for Information Act* (Ley de Libertad de Información) y una revisión comprehensiva de los expedientes de contrataciones y adquisiciones de ICE, revela que ésta funciona ahora como una agencia de vigilancia nacional. Desde su fundación en 2003, ICE no solo ha consolidado su propia capacidad de usar la vigilancia para realizar deportaciones, sino que ha desempeñado un papel clave en el esfuerzo generalizado del gobierno federal de recolectar toda la información que pueda sobre nuestras vidas. Al tener acceso a los registros digitales de los gobiernos estatales y locales, así como al comprar bases de datos con miles de millones de puntos de datos de empresas privadas, ICE ha desarrollado una infraestructura de vigilancia que le permite crear expedientes detallados sobre casi todos, aparentemente en cualquier momento. Como parte de sus esfuerzos por arrestar y deportar, ICE—sin supervisión judicial, legislativa o por parte del público—se ha metido en conjuntos de datos que contienen información personal acerca de la vasta mayoría de las personas que viven en Estados Unidos, cuyos registros pueden terminar en las manos de las agencias migratorias por el sencillo hecho de solicitar una licencia de manejo; conducir un automóvil; o registrarse en los servicios públicos de calefacción, agua potable y electricidad.

ICE ha construido su sistema de vigilancia y arrastre cruzando líneas legales y éticas, aprovechando la confianza que la gente deposita en las agencias estatales y proveedores de servicios esenciales, y explotando la vulnerabilidad de personas que proporcionan de manera voluntaria su información con tal de reunirse con sus familias. A pesar del alcance increíble y los evidentes conflictos de derechos humanos de las prácticas de vigilancia de ICE, la agencia ha logrado envolver aquellas prácticas en un secretismo casi total, incluso evadiendo los controles de las pocas leyes y políticas que podrían invocarse para imponer límites. En su mayoría, los legisladores federales y estatales no han enfrentado esta realidad.

Este informe sintetiza lo que ya se sabe acerca de la vigilancia de ICE a partir de nueva información de miles de registros previamente no vistos y analizados, que ilustran el impacto real de la vigilancia de ICE a través de tres estudios de caso: el acceso de ICE a los datos de los conductores, a los datos de los servicios públicos, y a los datos recolectados acerca de las familias de los menores sin acompañante. El informe se construye sobre la base de—y no habría sido posible sin—la potente investigación,

organización y apoyo de las organizaciones de derechos de migrantes como *CASA,* el *Immigrant Defense Project* (Proyecto de Defensa al Inmigrante), *Just Futures Law* (el proyecto legal 'Futuros Justos'), *Mijente,* el *National Immigration Law Center* (Centro Nacional de Derecho de Inmigración o NILC, por sus siglas en inglés), *Project South* (Proyecto Sur) y la *America Civil Liberties Union of Northern California* (Unión Americana de Libertades Civiles de California del Norte, ACLU, por sus siglas en inglés); entre muchas otras, las cuales han encabezado el esfuerzo de exponer y desmantelar la red de arrastre de ICE en Estados Unidos.

ICE ha escaneado las fotografías de las licencias de manejo de 1 de cada 3 adultos.

ICE tiene acceso a los datos de las licencias de manejo de 3 de cada 4 adultos.

ICE rastrea los movimientos de los conductores en ciudades donde viven 3 de cada 4 adultos.

ICE podría localizar 3 de cada 4 adultos a través de sus registros de servicios públicos.

A. HALLAZGOS

La vigilancia de ICE es más amplia que lo que piensa la gente; es una red de arrastre.

La mayoría de los estadounidenses no se imagina que su información es capturada por las redes de vigilancia de ICE. De hecho, ICE ha utilizado tecnología de reconocimiento facial para examinar las fotografías de las licencias de manejo de alrededor de 1 de cada 3 (32%) de todos los adultos en EE.UU. La agencia tiene acceso a los datos de las licencias de manejo de 3 de cada 4 (74%) adultos y rastrea los movimientos de los coches en ciudades donde viven casi 3 de cada 4 (70%) adultos. Cuando 3 de cada 4 (74%) adultos en EE.UU. conectaron el gas, la electricidad, el teléfono o el servicio de internet en un nuevo domicilio, ICE pudo descubrir de manera automática su nueva dirección. Casi todo eso se ha hecho sin orden judicial y en secreto.

ICE construyó su red de vigilancia y arrastre al procurar datos de empresas privadas y burocracias estatales y locales.

Durante la mayor parte de su historia, el control migratorio en Estados Unidos se efectuaba con pocos datos, ya que dependía de informantes ad hoc y acuerdos de compartición de información con agencias de seguridad estatales y locales. Después del 11 de septiembre, ICE emparejó esos programas con iniciativas mucho más amplias, obteniendo acceso a vastas bases de datos poseídas por agencias privadas de datos, además de burocracias estatales y locales que históricamente no se habían involucrado en asuntos de seguridad. A través de esas iniciativas, ICE actualmente usa flujos de información mucho más extensos y actualizados con mucho mayor frecuencia, incluyendo registros de los Departamentos de Vehículos Motorizados

(DMV por sus siglas en inglés) e información de los clientes de servicios públicos, así como registros de llamadas, registros de asistencia social infantil, encabezados de informes crediticios, registros de empleo, información de geolocalización, registros de seguro social, registros de vivienda y posts en redes sociales. El acceso a esas nuevas bases de datos, combinado con el poder de las herramientas algorítmicas para ordenar, emparejar, buscar y analizar, ha aumentado de manera dramática el alcance y la regularidad de la vigilancia de ICE.

ICE ha invertido mucho en vigilancia y adquirió tecnología de vigilancia avanzada mucho antes de lo que piensa la gente.

Nuestra revisión de más de 100,000 operaciones de gastos de ICE revela que entre 2008 y 2021 la agencia gastó aproximadamente $2.8 mil millones en nuevas iniciativas de vigilancia, recolección y compartición de datos. Esas operaciones también revelan que ICE estuvo consolidando capacidades avanzadas de vigilancia alrededor de media década antes de lo que se sabía. Hasta ahora, los registros más antiguos obtenidos por el *Center on Privacy & Technology* (Centro de Derecho de la Privacidad y Tecnología) sugerían que ICE había empezado a solicitar y realizar búsquedas de reconocimiento facial en bases de datos estatales y locales en 2014. Sin embargo, nuestra investigación descubrió un contrato de 2008 entre ICE y el contratista de biometría L-1 Identity Solutions. El contrato permitió a ICE a obtener acceso a la base de datos de reconocimiento facial del Departamento de Vehículos Motorizados del estado de **Rhode Island** para "reconocer indocumentados criminales". Eso ubica las primeras búsquedas documentadas de reconocimiento facial de ICE en los últimos días del gobierno de George W. Bush.

ICE explota la vulnerabilidad de la gente y su confianza en las instituciones para hacerse de más datos.

Para ubicar a las personas que pretende deportar, ICE toma datos que la gente otorga a las agencias e instituciones estatales y locales a cambio de servicios básicos. A menudo, ICE obtiene acceso a esos datos sin permiso, o incluso sin que la entidad que originalmente recolectó esa información lo sepa. ICE también ha aprovechado la vulnerabilidad de los menores sin acompañante que buscan reunirse con sus familias.

ICE aprovecha la confianza de la gente en los DMV estatales para señalar blancos de deportación.

A lo largo del país, 16 estados y Washington, D.C. han permitido a las personas indocumentadas solicitar licencias de manejo, siempre y cuando proporcionen un rango de información personal que incluya sus nombres legales, fechas de nacimiento y direcciones. Cientos de miles de personas indocumentadas han confiado en los departamentos de vehículos motorizados estatales para solicitar el derecho a manejar. Sin embargo, en por lo menos cinco de esas 17 demarcaciones, ICE puede buscar entre los registros estatales de conductores sin orden judicial alguna con el fin de aplicar medidas de control migratorio civil. En por lo menos seis de esas 17 demarcaciones, ICE ha utilizado el reconocimiento facial para escanear las fotografías de las licencias de manejo de los conductores y así realizar deportaciones. Cuando las personas indocumentadas solicitan permisos de manejo, depositan mucha confianza en el estado de que esa información no será usada en su contra. Permitir a ICE usar los registros de conductores para tomar medidas contra los inmigrantes representa una profunda traición de esa confianza.

- **ICE aprovecha las necesidades de la gente de agua, gas, electricidad, teléfono y servicio de internet para señalar blancos de deportación.**

  Además de obtener datos de los departamentos de vehículos motorizados, ICE también compra y rastrea registros de clientes de las empresas de servicios públicos para buscar personas para deportar. La agencia ha podido acceder a información de los registros de servicios públicos a través de un contrato con Thomson Reuters, una agencia privada de datos. Aunque las personas indocumentadas pueden evitar compartir su información con entidades como los DMV, se crea una situación de adversidad extrema cuando no pueden conectar sus casas a los servicios de agua, gas, electricidad, teléfono e Internet. "Para personas que no son fáciles de rastrear a través de medios convencionales," dice una carta de mercadotecnia de Thomson Reuters, "la información de localización de los registros de conexión de los servicios públicos podría proporcionar los únicos datos domiciliarios y telefónicos actualizados y disponibles". A través de sus contratos con las agencias privadas de datos, ICE ha obtenido acceso a la información de los registros de servicios públicos pertenecientes a más de 218 millones de clientes de servicios públicos en todos los 50 estados y el distrito federal.

- **ICE aprovechó las entrevistas con menores sin acompañante para buscar y arrestar a sus familiares.**

  En las últimas dos décadas, el número de menores sin acompañante que cruzan la frontera de Estados Unidos huyendo de la violencia y la pobreza ha aumentado por un orden de magnitud. Cuando los niños llegan a la frontera, están sufriendo un trauma físico y emocional. El Congreso ha intentado proteger a esos niños a través de una ley bipartidista que transfiere la responsabilidad de su cuidado y manutención de las agencias de seguridad al Departamento de Salud y Servicios Humanos (HHS, por sus siglas en inglés). Para poder asignar hogares adecuados a los niños, el HHS les pregunta si tienen algún pariente en Estados Unidos que pudiera cuidarlos. En lo que es quizá el ejemplo más duro de ICE explotando la confianza de gente vulnerable, la agencia firmó un acuerdo de compartición de datos con el HHS para usar la información proporcionada por esos niños y sus parientes para arrestar a por lo menos 400 de estos últimos. Aunque el Congreso modificó una ley de partidas presupuestarias para terminar el programa de manera parcial y el Secretario del Departamento de Seguridad Nacional (DHS, por sus siglas en inglés) Alejandro Mayorkas después lo rescindió formalmente, este arreglo ilustra lo que ICE es capaz de hacer para encontrar información sobre blancos potenciales de deportación.

ICE explota la confianza y vulnerabilidad de la gente para hacerse de más datos.

La vigilancia de ICE ha evadido la supervisión del Congreso.

La mayoría de los líderes del Congreso no sabían de los escaneos de ICE de las fotografías de los DMV hasta que el periódico The Washington Post publicó un reportaje sobre la práctica, con base en registros obtenidos

por el *Center on Privacy & Technology*. El reportaje salió en 2019, más de una década después de que ICE firmara su primer contrato conocido de reconocimiento facial, en 2008, para obtener acceso a la base de datos de conductores del estado de **Rhode Island**.

El hecho de que ICE estuviera realizando escaneos de reconocimiento facial en las fotografías de las licencias de manejo tomó desprevenidos a los legisladores de alto rango; incluso a los que tenían el mayor conocimiento de las actividades del DHS. Al enterarse de los escaneos faciales, la representante Zoe Lofgren, presidenta del *House Judiciary Subcommittee on Immigration and Citizenship* (Subcomité Judicial de Inmigración y Ciudadanía) de la Cámara de Representantes, denunció la práctica como "una intrusión masiva e injustificada a los derechos de privacidad de los estadounidenses por parte del gobierno federal, realizada de manera secreta y sin autorización legal". De forma regular, las iniciativas de vigilancia de ICE han pasado desapercibidas por el Congreso. Aunque unos cuantos líderes políticos han presionado a ICE por medio de cartas de supervisión, y han agregado cláusulas a las leyes de partidas presupuestarias para terminar con sus acciones más agresivas, hasta la fecha no ha habido una sola audiencia en el Congreso o un solo informe de la Oficina de Responsabilidad Gubernamental (GAO, por sus siglas en inglés) enfocado en la vigilancia de ICE.

Las autoridades estatales casi no se han percatado de la vigilancia de ICE sobre sus residentes.

Los legisladores estatales casi nunca están al tanto de la vigilancia de ICE en sus estados, y normalmente se terminan enterando de las acciones de la agencia en los noticieros. Cuando la representante de Utah, Angela Romero, supo que ICE y el FBI habían examinado los registros de conductores en su estado, contestó como lo hacen muchos legisladores cuando sale a la luz información sobre la vigilancia de ICE: "Esto no se había compartido con nosotros anteriormente y la legislatura no lo ha aprobado". La falta de conocimiento de los líderes políticos se agrava con la incapacidad de las agencias estatales de controlar o rastrear el acceso de ICE a los datos de sus residentes. En **Maryland**, por ejemplo, cuando los legisladores pidieron información a dos agencias—la *Maryland State Police* y *Maryland Motor Vehicle Administration* (Policía Estatal de Maryland y la Administración de Vehículos Motorizados de Maryland respectivamente)—acerca de las búsquedas de ICE de datos de las licencias de manejo, las agencias negaron la responsabilidad y cada una remitió a la otra la custodia de información relacionada al acceso de ICE.

ICE ha evadido las leyes estatales y los esfuerzos de los legisladores de refrenar sus capacidades de vigilancia.

Cuando los gobiernos estatales aprueban leyes y políticas para poner fin a la compartición de datos de sus estados con ICE, ésta última continuamente lograr evadir esas restricciones y a menudo aprovecha puntos de acceso alternos dentro de la compleja red de sistemas que vincula las bases de datos estatales y federales. En **Washington**, el gobernador Jay Inslee promulgó una política general para limitar la cooperación de las agencias estatales con ICE, solo para descubrir que los encargados de emitir las licencias estaban violando esa política de forma rutinaria. Cuando los funcionarios del estado cortaron el acceso de ICE a la base de datos estatal de conductores, documentos previamente desconocidos muestran que las búsquedas del DHS en otra red de datos de conductores—no operada por el estado—casi se

duplicaron. En **Oregon**, poco después de que los legisladores aprobaran una ley que ponía fin a la difusión a ICE de los datos estatales, el DMV firmó acuerdos para vender sus registros de licencias de manejo a Thomson Reuters y a LexisNexis Risk Solutions, las dos principales agencias de datos que venden a ICE el acceso a la información de conductores.

La vigilancia de ICE disuade a la gente a solicitar servicios básicos.

Históricamente, los "efectos disuasorios" de la vigilancia gubernamental se refieren a la manera en que la vigilancia disuade a los individuos a participar en actividades protegidas por la Primera Enmienda, como la libertad de expresión y asociación. Sin embargo, una cantidad cada vez mayor de investigación sugiere que el miedo a la vigilancia de ICE también disuade a los inmigrantes y a sus familias de participar en una amplia gama de actividades necesarias para la salud y el bienestar no solo de individuos, sino también de las comunidades de las que forman parte. Las inquietudes en torno a la vigilancia de ICE a menudo provocan que las personas eviten proporcionar su información a los sistemas gubernamentales, aún si tales sistemas no tienen relación con asuntos de seguridad. En otras palabras, ese temor inhibe a la gente a registrarse en servicios críticos para su propia salud y la de sus hijos, y también impide que participen en el sistema de justicia, por ejemplo, reportando crímenes o testificando en las cortes.

B. RECOMENDACIONES

Congreso

- **El Congreso debería reformar las leyes migratorias de EE.UU. para reducir de manera radical el número de personas que podrían estar sujetas a la deportación.**

  La mejor, y quizá la única manera de desmantelar la red de arrastre de ICE es aboliendo las leyes con base en las cuales el poder ejecutivo pone en la mira a cientos de miles de personas cada año para su deportación. El Congreso podría reducir de manera considerable el número de personas sujetas a deportación si—por ejemplo—creara un camino a la ciudadanía para las personas indocumentadas; si redujera dramáticamente las causales de expulsión basadas en la participación delictiva; y si aplicara un periodo de prescripción a las deportaciones. Aunque esas reformas no se dirigen a la vigilancia en sí, representan la manera más directa de socavar la autoridad de vigilancia de ICE.

- **El Congreso debería proteger a las personas que confían sus datos al gobierno federal.**

  El gobierno federal opera una serie de programas que efectivamente pide a las personas indocumentadas descubrirse y confiar su información personal al gobierno federal. Unos cuantos ejemplos incluyen el programa Acción Diferida para los Llegados en la Infancia (DACA, por sus siglas en inglés), el uso de los números de identificación del contribuyente del Servicio de Impuestos Internos (IRS, por sus siglas en inglés), y las visas U y T disponibles a las víctimas de ciertos crímenes. Es poco ético, y probablemente una violación del debido proceso, usar esos programas

como trampas para los indocumentados. El Congreso podría fácilmente crear un estatuto comprehensivo que protegiera ese tipo de datos. El Congreso podría basar el estatuto en las leyes federales que protegen la confidencialidad de los datos del censo, las cuales prohíben el uso de éstos para fines no estadísticos, y claramente ordenan que "en ningún caso la información proporcionada [a la Oficina del Censo] podrá usarse en detrimento de un encuestado o de otra persona a quien se relaciona tal información".

El Congreso podría basar una ley para proteger los datos ofrecidos por los inmigrantes indocumentados en los estatutos de confidencialidad del censo.

Hasta que se apruebe un estatuto comprehensivo de ese tipo, el Congreso podría proteger la información guardada en programas específicos a través de enmiendas individuales a los estatutos relevantes o leyes de partidas presupuestarias. Por su parte, el DHS podría aplicar esas protecciones como política departamental.

- **El Congreso debería prohibir que ICE use los datos de los DMV como una mina de oro para las deportaciones.**
  El Congreso aprobó la *Driver's Privacy Protection Act* (Ley de Protección de la Privacidad del Conductor *o* DPPA, por sus siglas en inglés) años antes de la moderna era de deportaciones en masa. ICE no ha dudado en usar las amplias excepciones para el acceso gubernamental incluidas en la DPPA para escanear las fotografías de las licencias de manejo pertenecientes a millones de estadounidenses, sin orden judicial, además de realizar búsquedas con las direcciones de la gran mayoría de los residentes en EE.UU. que se proporcionan en sus registros de conductor. El Congreso debería actualizar la DPPA para prohibir (o requerir una orden o un mandato judicial para) cualquier uso de los datos de los DMV para aplicar leyes migratorias.

- **El Congreso debería realizar una feroz supervisión de la vigilancia de ICE.**
  Los presidentes de los comités y subcomités no necesitan una votación mayoritaria o supermayoritaria para exigir que ICE responda por la expansión masiva de sus iniciativas de vigilancia y el vasto secretismo que las rodea. La vigilancia de ICE hace surgir una amplia gama de preocupaciones constitucionales fundamentales desde el comercio hasta el federalismo, y cada cámara del Congreso tiene múltiples comités y subcomités que podrían realizar una supervisión feroz de la agencia. Temas posibles para audiencias o un informe de la GAO incluyen: (1) cómo y por qué ICE esquiva las leyes estatales que protegen los datos de los conductores y otros residentes; (2) cómo la dependencia de ICE en las agencias de datos limita al escrutinio público y ayuda a la agencia a evadir las protecciones legales y constitucionales; y (3) cómo ICE actualmente usa la biometría, incluyendo el reconocimiento facial, las huellas digitales y el ADN, y cómo piensa usarla en el futuro. Una lista más completa puede encontrarse en la sección **Recomendaciones**.

DHS & ICE

- **ICE debería poner fin a todos sus programas de vigilancia y arrastre, incluyendo el uso del reconocimiento facial con los datos de los DMV para el control migratorio.**

  Todos los programas de vigilancia de ICE deberían someterse a un escrutinio intenso. Sin embargo, ICE debería poner fin inmediatamente a todos los programas de vigilancia y arrastre—tanto los que están dirigidos por ICE como los que funcionan a través de las agencias de datos—que recolectan datos de manera indiscriminada sobre tantas personas en EE.UU. como sea posible. Los programas que deberían ser categorizados como este tipo especialmente problemático de vigilancia y arrastre incluyen por lo menos (1) la práctica del escaneo de las fotografías en la licencia de manejo para la aplicación de medidas de control migratorio; (2) la recolección de grandes volúmenes de información postal y otros registros del DMV y de compañías de servicios públicos y (3) la recolección de grandes volúmenes de fotografías de matrículas que capturan los trayectos de los conductores en las áreas metropolitanas más importantes de EE.UU.; (4) la compra de grandes conjuntos de datos de agencias privadas.

- **ICE debería dejar de usar los registros de agua, calefacción, luz, teléfono e internet para emprender deportaciones.**

  La gente necesita calefacción, agua y electricidad para sobrevivir. También precisa de líneas telefónicas para emergencias y acceso al internet para trabajar y asistir a la escuela. El DHS no debería esperar a que los inmigrantes empiecen a cortar esos servicios por miedo a ser deportados antes de emitir una clara prohibición al uso de los registros de servicios públicos para asuntos migratorios.

Los legisladores estatales pueden desempeñar un papel fundamental en proteger a sus electores contra la vigilancia sin orden judicial de ICE.

Estados

- **Los estados deberían proteger a las personas que confían sus datos a los gobiernos estatales y locales.**

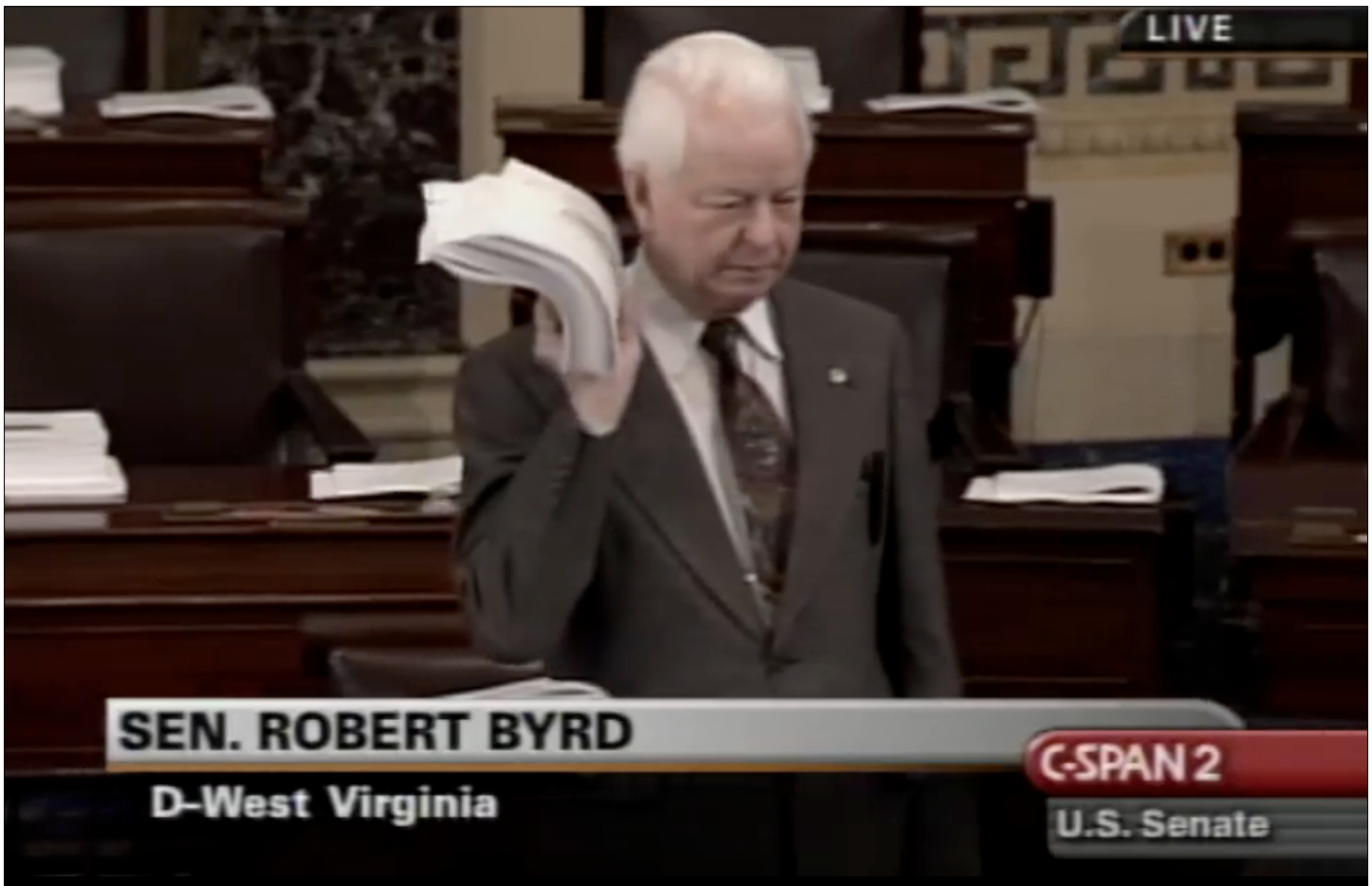
  De las 17 demarcaciones que ofrecen a los residentes indocumentados la oportunidad de solicitar licencias de manejo, siete han aprobado leyes que buscan protegerlos contra las búsquedas y los escaneos faciales—realizados sin orden judicial por parte de ICE—para dar con datos y fotografías de los conductores. Desafortunadamente, pocos estados han aplicado restricciones verdaderamente comprehensivas al acceso de la agencia a los datos de conductores. Estas leyes deberían: (1) enfocarse en los datos, no en quien los custodia; (2) enfocarse en el propósito del intercambio, no en el receptor; (3) proteger contra toda forma de compartición de datos; (4) no distinguir entre la aplicación "civil" y "criminal" de leyes migratorias; (5) asegurarse de que el reconocimiento facial se incluya claramente en esas restricciones; y (6) eliminar las

excepciones generales para el acceso "con fines de seguridad" a los datos guardados a nivel estatal o local.

- **Los estados deberían prohibir que se usen los registros de agua, gas, electricidad, teléfono e Internet para aplicar leyes migratorias.**
  Las autoridades estatales y locales deberían prohibir la divulgación, venta o reventa de esos datos para asuntos migratorios. Otra vez, aunque unos pocos estados tienen buenas normas que se aplican a un servicio en particular (p. ej. gas o electricidad), ninguno ha promulgado protecciones de privacidad significativas y comprehensivas para clientes de todos los servicios públicos. Al aplicar estas protecciones, las autoridades estatales y locales deberían: (1) restringir la divulgación a las agencias de datos, no solo al gobierno; (2) evitar excepciones generales para fines de historiales y evaluaciones crediticias; (3) proteger contra todas formas de divulgación; y (4) asegurarse de proteger las direcciones de los clientes. De todas las leyes disponibles, las leyes de Connecticut que rigen la privacidad de la información guardada por las empresas de gas probablemente representan la norma más protectora hasta la fecha.

- **Los estados deberían configurar sus sistemas para poder rastrear el acceso de ICE e inspeccionar cuidadosamente ese acceso.**
  Cualquier administrador estatal de bases de datos debería poder contestar dos preguntas: ¿tiene ICE acceso a esta base de datos? Si es así, ¿cómo y por qué la ha utilizado ICE? En la tercera década del siglo XXI, no hay excusa para que una base de datos de un gobierno estatal o local con datos sensibles no cuente con un sistema que registre cuidadosamente los tiempos y frecuencia de los accesos de los usuarios, así como sus búsquedas y resultados de búsqueda. Las autoridades estatales y locales deberían revisar de manera regular esas bases de datos para determinar si, cómo y con qué frecuencia ICE está ingresando a ellas. Si las autoridades no realizan esas inspecciones por su cuenta, los legisladores deberían enviar cartas de supervisión a las agencias estatales y realizar audiencias de supervisión para obligar a que los funcionarios de estas agencias actúen.

INTRODUCCIÓN: ROBERT BYRD Y JOSÉ HERNÁNDEZ



Sen. Robert Byrd sostiene el texto de la Ley de Seguridad Nacional de 2002 mientras argumenta en contra del proyecto. (Foto: C-SPAN 2).

El 19 de noviembre de 2002, un proyecto de ley para crear el DHS tuvo su último voto en el Senado de EE.UU. Hasta entonces había recibido poca oposición. Tal y como dijo su oponente principal, la *Homeland Security Act* (Ley de Seguridad Nacional) estaba "pasando a toda velocidad por el Congreso como un camión Mack, amenazando con atropellar a cualquiera que se atreviera a interponerse."[1]

Aquel crítico no era el león liberal Ted Kennedy, ni Russ Feingold de Wisconsin, el senador que había sido el único en votar en contra de la USA PATRIOT ACT (LEY PATRIOTA DE EE.UU.), que se había aprobado 98-1 el año anterior.[2] En su lugar, la voz de oposición pertenecía al senador Robert Byrd de West Virginia, hombre que había dedicado décadas de su trayectoria en el Congreso a construir precisamente el tipo de burocracia federal que el proyecto de ley crearía.[3]

Quizá el senador estaba preocupado que la repentina reorganización de docenas de agencias federales y más de 150,000 empleados en un solo departamento disminuiría su control

sobre esas burocracias y los empleos que habían aportado a su estado. A lo largo de medio siglo en el Congreso, Byrd había llevado instalaciones federales a su estado nativo de manera sistemática, incluyendo centros de capacitación militar y el laboratorio de huellas digitales del FBI. En los años venideros, cambiaría el Centro Marítimo Nacional de la Guardia Costera a Martinsburg, West Virginia, un lugar que carece de litoral.[4]

Pero eso no fue de lo que habló Byrd cuando atacó el proyecto de ley en la cámara del Senado.[5] En cambio, rechazó categóricamente la principal justificación retórica de la ley, es decir, la idea de que estuviera respondiendo a una urgente necesidad de seguridad nacional. Los funcionarios encargados de defender al país ya estaban "ahí afuera . . . ahora mismo, hoy mismo", explicó.[6] También rechazó el argumento de que la ley era necesaria para pagar la seguridad nacional al señalar que el Congreso había aprobado $5.1 mil millones de dólares en gastos de urgencia anteriormente en ese año, proyecto que el presidente George W. Bush se había negado a promulgar.[7]

En lugar de eso, Byrd sonó la alarma: la Ley de Seguridad Nacional representaba un "enorme otorgamiento de poder al poder ejecutivo".[8] El DHS funcionaría como "una cámara masiva de secretos", inmune a la transparencia, las auditorías internas y la supervisión externa.[9] La ley no proporcionaría al presidente "ningún mecanismo real para asegurarse de que esos poderes no se abusen".[10]

El senador Byrd advirtió que el programa "fisgaría en las transacciones diarias y vidas privadas de todo estadounidense".

En su advertencia más grave, Byrd dijo que el resultado de este secretismo e impunidad sería un sistema de vigilancia y arrastre.[11] Había advertido previamente que la ley daría al Secretario del DHS "un acceso casi ilimitado a la inteligencia… sin protecciones adecuadas contra el mal uso" de esos datos.[12] El 19 de noviembre, dijo tajantemente: "[La Casa Blanca] nos dijo que no está planeando crear una nueva agencia de espionaje nacional en Estados Unidos", y sin embargo la ley autorizaría un programa del Pentágono que "fisgaría en las transacciones diarias y vidas privadas de todo estadounidense"."[13]

Aquella tarde, los colegas de Byrd votaron 90 a 9 a favor de la Ley de Seguridad Nacional.[14] Cuando le preguntaron por qué se había opuesto con tanto fervor a una ley que estaba destinada a aprobarse, Byrd contestó: "El asunto quedará registrado por mil años. Yo defendí la Constitución. Yo defendí la institución. Si no se escucha hoy, habrá algún miembro en el futuro que pasará por aquí y . . . leerá estos volúmenes".[15]

José Santos Quintero Hernández de Rockville, Maryland, frente a la sede de CASA en Adelphi, Maryland
(Fotografía: Alex Vazquez, CASA)

José Santos Quintero Hernández y Maribel Cortez llevan 22 años de casados. Se conocieron en EE.UU. después de emigrar de manera separada desde El Salvador, huyendo de la violencia y de lo que Hernández clasificó como una muerte segura.[16] La pareja llevaba una vida tranquila criando a sus cinco hijos en Rockville, Maryland, un suburbio que queda a menos de una hora en coche del Capitolio estadounidense.[17]

Una mañana a principios de febrero de 2020, poco más de 17 años después de los comentarios de Byrd, alguien tocó a la puerta de la familia Hernández. Uno de los niños abrió. Segundos después, los hijos del matrimonio Hernández Cortez vieron a unos agentes de ICE entrar a su hogar, arrestar a su padre y llevárselo.

Hay millones de personas indocumentadas en EE.UU. ¿Cómo es que ICE arrestó a Hernández? ¿Acababa de llegar y había faltado a una audiencia en la corte? No, llevaba décadas viviendo ahí. ¿Había llegado a la atención de ICE a través de las agencias locales de seguridad? No: ni Hernández ni Cortez había tenido encuentros con la policía o los agentes migratorios.

"No", explicaron los agentes a Hernández mientras lo conducían a su coche. Lo habían encontrado porque acababa de obtener una licencia de manejo de Maryland. Usaron la información que proporcionó a la Administración de Vehículos Motorizados de Maryland para encontrarlo, arrestarlo, encerrarlo en un centro de detención de inmigrantes e iniciar un procedimiento de deportación en su contra.[18]

“No lo sabíamos. Lo habríamos hecho bien desde el principio si lo hubiéramos sabido.”

Posteriormente ese mes, The Washington Post y The Baltimore Sun revelaron que, además de buscar en la información personal de los conductores de Maryland—sus nombres, direcciones y fechas de nacimiento—ICE también había escaneado los *rostros* de los conductores del estado para realizar búsquedas de reconocimiento facial con las fotos de sus licencias. Esas búsquedas, que carecían de orden judicial, no se restringían a los inmigrantes indocumentados u otros solicitantes de lo que se llaman licencias “estándar”, ICE había ingresado a una base de datos estatal de reconocimiento facial y escaneado los rostros de los conductores de todo el estado, más de cuatro millones de personas en total.[19]

Los legisladores de Maryland estaban escandalizados, sobre todo los que habían capitaneado el esfuerzo en 2013 para permitir que los residentes indocumentados pudieran solicitar licencias. La delegada Joseline Peña-Melnyk del Condado Prince George se sintió consternada al saber que ICE estaba rastreando inmigrantes en Maryland por medio de un programa que ella había apoyado. “Te rompe el corazón,” dijo a The Washington Post. “No lo sabíamos: lo habríamos hecho bien desde el principio si lo hubiéramos sabido”.[20] Hasta la fecha, los funcionarios estatales parecen no tener idea de cuántas veces ICE haya escaneado los rostros de los conductores de Maryland.[21]

Lo que le sucedió a Hernández—y lo que sucedió en Maryland—no es único. Estos descubrimientos forman parte de un patrón común. De manera silenciosa, ICE realiza escaneos de reconocimiento facial no solo con los residentes de Maryland y no solo con inmigrantes, sino con millones de conductores a lo largo del país.[22] ICE también ha pagado a una agencia de datos para poder obtener acceso a una gran colección de fotos de matrículas de automóviles que registra los movimientos diarios de los conductores en 50 de las áreas metropolitanas más grandes de EE.UU.[23] ICE también pagó a otra agencia de datos para poder buscar datos domiciliarios en los registros de las empresas de agua, gas, electricidad, teléfono y cable, de tal forma que en el momento en que una familia, inmigrante o nativa, se muda a una nueva casa, conecta el agua o enciende las luces, ICE puede rastrearlos.[24] Cuando los menores llegaron solos a la frontera, ICE incluso utilizó la información de las entrevistas con esos niños para encontrar, arrestar y deportar a sus familiares.[25]

De manera consistente, ICE se retrata como una agencia cuyos esfuerzos están "enfocados" y "centrados" en individuos específicos o grupos limitados de personas, pero estos descubrimientos revelan una historia muy diferente.[26] Cuando ICE usa los datos masivos provenientes de los registros de licencias de manejo o de información de los clientes de servicios públicos, o cuando lleva a cabo el monitoreo regular de la vasta mayoría de las personas en EE.UU., la relación entre el supuesto propósito de seguridad de ICE y sus verdaderas prácticas de seguridad se empieza a debilitar considerablemente. En lugar de estar enfocada o centrada en cualquier otra perspectiva significativa, la vigilancia actual de ICE es una extensa red de arrastre.

El alcance pleno de la red de vigilancia y arrastre de ICE permanece todavía en secreto. La cobertura de los medios de comunicación presenta imágenes instantáneas de iniciativas específicas, a menudo con poca diferenciación entre los programas que maneja la Oficina de Aduanas y Protección Fronteriza (CBP, por sus siglas en inglés) y los que opera ICE. Pocos defensores de la privacidad consideran a la aplicación de leyes migratorias como un espacio de vigilancia en masa, mientras que los defensores y organizadores de los derechos de los migrantes, sobrecargados ellos mismos con el trabajo de resistir a las deportaciones masivas, a menudo carecen de recursos para investigar los programas de vigilancia que están alimentando al sistema. Por su parte, el Congreso aún no ha dedicado una audiencia completa de supervisión a la vigilancia de ICE. Como resultado, preguntas básicas sobre el arsenal de vigilancia de ICE siguen sin contestarse:

- ¿Cuán seguido escudriña ICE la información de conductores de los Departamentos de Vehículos Motorizados (DMV) de los estados?
- ¿Los rostros de cuántas personas ha escaneado ICE?
- ¿Las direcciones de cuántas personas han sido vendidas a ICE después de que los clientes se conectaran al agua, electricidad, gas, teléfono o cable? Y ¿cómo exactamente obtuvo ICE esos datos?
- ¿Por qué ICE de repente acumuló ese arsenal cuando su predecesor, el Servicio de Inmigración y Naturalización (INS, por sus siglas en inglés) hizo pocas inversiones importantes en tecnología?
- ¿La ley permite esta vigilancia y, si es así, por qué?

Este informe rellena muchas de estas brechas, ya que es fruto de una investigación de dos años que engloba más de 200 solicitudes realizadas bajo la *Freedom of Information* (Ley de Libertad de Información), así como los resultados de una revisión de más de 100,000 transacciones de adquisición, y una serie de encuestas legales exhaustivas. De igual manera, explica el contexto histórico y legal que ha permitido a ICE crear su red de arrastre, y ofrece a legisladores y defensores un marco a través del cual poder entenderlo. El informe también ilustra el alcance de la vigilancia de ICE por medio de estudios de caso del uso que ICE hace de: (1) datos y fotografías de los DMV, (2) datos de los servicios públicos y (3) datos de entrevistas con los menores sin acompañante detenidos en la frontera.

ICE ha escaneado las fotos de las licencias de manejo de 1 de cada 3 adultos.

ICE tiene acceso a los datos de las licencias de manejo de 3 de cada 4 adultos.

ICE rastrea los movimientos de los conductores en ciudades donde viven 3 de cada 4 adultos.

ICE podría localizar a 3 de cada 4 adultos a través de sus registros de servicios públicos.

Los resultados de nuestra investigación han revelado un duro panorama de vigilancia y arrastre, pues indican que ICE no solo ha utilizado la tecnología de reconocimiento facial para escanear las fotografías de las licencias de manejo de **1 de cada 3** adultos, sino que tiene acceso a los datos de las licencias de manejo de **3 de cada 4** adultos; es capaz de rastrear los movimientos de los conductores en ciudad donde viven **3 de cada 4** adultos; y podría localizar a **3 de cada 4** adultos a través de sus registros de servicios públicos. Secretismo, impunidad, vigilancia y arrastre: 19 años después de que Byrd censurara la Ley de Seguridad Nacional desde la cámara del Senado, sus advertencias se han hecho realidad.[27]

Este informe no es el primero en describir la red de vigilancia y arrastre de ICE. Durante años, organizaciones como *CASA, Immigrant Defense Project, Just Futures Law, the Legal Aid Justice Center, Make the Road, Mijente, National Immigrant Justice Center (NIJC), ACLU, Project South* (CASA, el Proyecto de Defensa del Inmigrante, Just Futures Law, el Centro de Justicia de Asistencia Legal, Se Hace Camino, Mijente, el NILC, el Centro Nacional de Justicia para Inmigrantes—NIJC—, la Unión Americana de Libertades Civiles—ACLU—, Proyecto Sur, respectivamente) y docenas más han advertido y realizado campañas en contra de la vigilancia de ICE. Sin embargo, este documento es el primero que pretende *cuantificar* el alcance de la vigilancia de ICE en "las transacciones diarias y vidas privadas de todo estadounidense", como vaticinó Byrd. Con base en estas nuevas investigaciones y análisis, el informe hace un llamado al Congreso para investigar y supervisar la vigilancia de ICE, a la vez que ofrece a legisladores y comunidades un conjunto de recomendaciones concretas para desmantelar esta red de arrastre estadounidense.

A. ÁMBITO Y METODOLOGÍA

1. Ámbito

Casi todas las operaciones de seguridad y control del DHS se han vuelto de alta tecnología, no solo las que maneja ICE. Esos sistemas son complejos y entrelazados, haciendo que sea difícil tener una imagen clara de la capacidad de vigilancia de una agencia en particular.[28] Este informe se enfoca específicamente en ICE, la agencia encargada de aplicar las leyes migratorias en el interior de EE.UU. No toca, por ejemplo, las capacidades de vigilancia de la CBP, cuyas responsabilidades incluyen revisar a los viajeros que llegan del extranjero y prohibir la entrada al país de personas que no han sido inspeccionadas en la frontera. Este informe trata de la capacidad legal y técnica de ICE de identificar y poner en la mira a personas *dentro* del país para su deportación, y explica cómo la aplicación nacional de las leyes migratorias ha experimentado transformaciones profundas, pero usualmente poco advertidas en el siglo XXI.

Al principio del informe se ofrece un marco para entender la transformación de la vigilancia de ICE. A continuación, se presentan tres estudios de caso acerca de algunas iniciativas de vigilancia de ICE. Dos de estos estudios de caso—el acceso de ICE a las bases de datos de los DMV de los estados y a los registros de las empresas de servicios públicos—ilustran el alcance de ICE más allá de los sistemas de seguridad estatales y locales, hasta llegar a registros creados por un rango mucho más amplio de agencias estatales y locales. Esos registros engloban a la mayoría de la población adulta de un estado y no distinguen (en algunos casos porque las leyes o políticas prohíben tales distinciones) entre personas según su estatus migratorio. El tercer estudio de caso, que describe el uso de ICE de la información recolectada de los inmigrantes menores de edad y sin acompañante que llegan a la frontera, subraya la negativa de ICE de observar normas legales y éticas básicas, y cómo las maneras contemporáneas de entender los efectos disuasorios no abarcan el alcance completo de los daños que produce la vigilancia.

2. Metodología

Para poner la vigilancia de ICE en un contexto legal e histórico, los autores y aproximadamente una docena de investigadores de apoyo, incluyendo personal y becarios del Centro, estudiantes de la Facultad de Leyes de Georgetown y estudiantes de licenciatura de Georgetown, emplearon una diversidad de métodos de investigación.

En primer lugar, hicimos más de 200 solicitudes bajo la Ley de Libertad de Información con entidades estatales y locales. Estas solicitudes se clasifican en tres categorías:

- 51 solicitudes a los DMV para todos los 50 estados y Washington, D.C., enfocadas al uso que hacen los DMV de los sistemas de reconocimiento facial y la divulgación de información de los conductores a las agencias de datos;
- 60 solicitudes a las empresas más grandes de la nación de servicios municipales de gas, agua y electricidad, enfocadas en la divulgación de información de sus clientes a ICE y a las agencias de datos; y
- 102 solicitudes a los DMV y a las principales agencias de seguridad de los estados en todos los 50 estados y el distrito federal, enfocadas en las preguntas realizadas a sus empleados tanto por parte de ICE, como por medio del acceso directo a las bases de datos de esas entidades.

Aquellas peticiones dieron como resultado más de 9,000 páginas de documentos de respuesta. Nuestro **Apéndice** incluye el modelo de lenguaje utilizado en cada una de esas peticiones. Complementamos nuestra revisión de las respuestas con un estudio separado de reportes y hallazgos regulatorios de las agencias, del Congreso y de otras proveniencias acerca de los enfoques del INS e ICE en torno a la seguridad nacional.

En segundo lugar, realizamos tres estudios legales para entender el panorama actual de leyes estatales y federales que restringen el acceso de ICE a diferentes tipos de datos. Éstos incluyeron:

- un estudio de las leyes de privacidad aplicables a las empresas de gas, agua, electricidad, cable y teléfono en todos los 50 estados y el distrito federal;
- un estudio de las leyes de privacidad estatales para los datos de conductores guardados en las 17 demarcaciones (16 estados y el distrito federal) que ofrecen licencias de manejo o tarjetas de privilegio a los residentes indocumentados; y
- un estudio de las leyes federales de privacidad, incluyendo la DPPA y las leyes federales de privacidad que aplican a las empresas de cable y teléfono.

En tercer lugar, para calcular las capacidades e inversiones de ICE en cuanto a la vigilancia, revisamos cada transacción de adquisición disponible al público en el portal *USAspending* de 2008 a 2021; un total de más de 100,000 transacciones. Eso incluyó una revisión inicial manual para identificar inversiones en vigilancia, recolección y compartición de datos, seguida por una segunda revisión apoyada por un algoritmo enfocado en esas transacciones conocidas relacionadas con la vigilancia. Para más información acerca de nuestro uso de procedimientos para identificar las transacciones de vigilancia de ICE y un resumen detallado de nuestra metodología de revisión de las adquisiciones, ver el **Apéndice**.

En cuarto lugar, realizamos un estudio de fuentes públicas de toda la información acerca de la base de datos CLEAR de Thomson Reuters, la base de datos LexisNexis y la agencia de datos Equifax para entender mejor cómo esas entidades lograron obtener acceso a las direcciones de clientes guardadas por las empresas de servicios públicos. Nuestra investigación reveló que aquellas empresas probablemente estaban obteniendo acceso a datos guardados por un grupo comercial poco conocido, el *National Consumer and Telecom Utilities Exchange* (Centro Nacional del Consumidor de Telecomunicaciones y Servicios o NCTUE, por sus siglas en inglés), y probablemente sin el conocimiento de los millones de personas cuyos datos estaban guardados por esa organización. Nos sentimos éticamente obligados a divulgar esa información lo antes posible, por lo que en febrero de 2021 se la revelamos a The Washington Post.[29] La publicación de nuestros hallazgos, en conjunto con el trabajo de *Just Futures Law* y *Mijente*, lograron que el senador Ron Wyden de Oregón presionara a NCTUE a poner fin a la venta de más de 170 millones de nombres, direcciones y otra información personal de los clientes de servicios públicos.[30] Como resultado a esos esfuerzos, NCTUE ordenó a Equifax en octubre del 2021 que dejara de vender estos datos.[31]

En quinto lugar, para entender el daño que esta vigilancia ha causado, revisamos publicaciones sociológicas y de otras ramas académicas sobre el impacto de las acciones modernas y basadas en datos por parte de las agencias migratorias en las

vidas diarias de los inmigrantes: su disposición para ir al médico, para llevar a sus niños a la escuela o permitirles jugar en un parque público. Esas investigaciones, basadas en evidencia y con revisión de colegas, ofrecen percepciones críticas sobre el impacto de la vigilancia, que a menudo no se toma en cuenta en el diseño contemporáneo de políticas de vigilancia.

Finalmente, antes y a lo largo de este periodo de dos años, realizamos dos iniciativas de apoyo y defensa que nos proporcionaron un entendimiento más profundo de las autoridades federales y estatales que pueden limitar las actividades de vigilancia de ICE y realizar una supervisión para refrenar la agencia. Trabajamos con el *Brennan Center for Justice* (Centro Brennan para la Justicia), NIJC y otras organizaciones de la sociedad civil para movilizar una coalición de organizaciones nacionales de defensa de la privacidad y derechos de los migrantes que instara al Congreso a bloquear la utilización por parte de ICE de los datos obtenidos de niños sin acompañante detenidos para poner a sus tutores en la mira para su arresto y deportación.[32] Por medio de ese esfuerzo, se logró la aprobación de una modificación a una ley de partidas presupuestarias en 2018 que prohibió que ICE usara los datos en muchos, pero no en todos los casos.[33] El secretario del DHS Alejandro Mayorkas finalmente terminó el programa en 2021.[34]

También trabajamos en conjunto con CASA, la organización más destacada en derechos de inmigrantes en la región del Atlántico medio, y con *Georgetown Law's Federal Legislation Clinic* (Clínica de Legislación Federal de la Facultad de Leyes de la Universidad de Georgetown) para la aprobación de leyes de privacidad en Maryland que protejan los registros de clientes de servicios públicos, registros de conductores y otros datos guardados por el estado contra su divulgación sin orden judicial a ICE o a otras agencias migratorias. Por medio de esos esfuerzos se logró la aprobación de la *Maryland Driver Privacy Act* (Ley de Protección a la Privacidad del Conductor de Maryland, HB 23, SB 234).[35]

Este informe tuvo una revisión de colegas elaborada por diez expertos, un grupo de académicos, defensores y exfuncionarios del gobierno, incluyendo a individuos previamente empleados por el DHS. Aunque algunos de nuestros revisores escogieron permanecer en el anonimato, otros están nombrados en nuestros **Agradecimientos**.

I. ICE CONSTRUYÓ SU RED DE VIGILANCIA Y ARRASTRE MEDIANTE LA ACUMULACION DE DATOS GENERADOS POR AGENCIAS BUROCRÁTICAS ESTATALES Y LOCALES.

Desde su creación en 2003, ICE se ha promovido de manera consistente como una agencia de seguridad que busca a los *criminal aliens* (extranjeros criminales), término usado por la agencia para describir a los no ciudadanos que han tenido contacto con los aparatos de seguridad, independientemente de si fueron o no condenados por un crimen.[36] ICE utiliza el lenguaje del sistema de justicia penal para defender las deportaciones retóricamente, pero también depende mucho de la infraestructura de este sistema para llevar a cabo sus operativos de seguridad. A lo largo de las últimas dos décadas, el movimiento de derechos de los migrantes ha hecho una gran labor para revelar cómo ICE utiliza a la policía y las cárceles para investigar a las personas para fines de deportación, incluyendo el desgraciadamente famoso y obligatorio programa de compartición de huellas digitales "Comunidades Seguras" (S-Comm, por su abreviatura en inglés), que estableció un sistema por medio del cual los escaneos de las huellas digitales tomados por las agencias de seguridad estatales y locales se comparan automáticamente con una base de datos operada por el DHS, alertando a ICE de posibles violaciones migratorias.[37]

Lo que ha recibido menos atención, sin embargo, es el despliegue de ICE de una mucho más amplia variedad de programas de compartición y recolección de datos que acumula información desde fuentes *ajenas* al ámbito de seguridad.[38] Conforme las ciudades y los estados han ido aplicando políticas santuario que limitan la cooperación de sus agencias de seguridad con los funcionarios migratorios, ICE ha aumentado de manera progresiva su juego de herramientas para incorporar grandes colecciones de datos más allá de lo que pueden proporcionar las policías estatales y locales. ICE se ha dirigido a agencias gubernamentales como los DMV, y ha pedido información de los conductores y solicitado búsquedas de reconocimiento facial en bases de datos enteras de fotografías de licencias. Del mismo modo, ha incrementado sus inversiones en contratos con las agencias privadas de datos, comprando el acceso a miles de millones de datos conseguidos de fuentes como las agencias crediticias y las empresas de servicios públicos.

Esta sección traza la evolución de la vigilancia de ICE y de su predecesor, INS. Ilustra el desplazamiento de programas que dependen de información recolectada por las agencias de seguridad a programas que sacan sus datos de una mucho más amplia variedad de fuentes, incluyendo a empresas privadas y a entidades gubernamentales sin competencia en asuntos de seguridad. A continuación, se traza esta expansión en términos de gasto en dólares, mostrando un aumento dramático en la inversión en este segundo tipo de programas de vigilancia. Como se explica con mayor detalle en **Hallazgo 2** y **Hallazgo 3**, son los datos recolectados de fuentes ajenas al contexto de la seguridad los que ICE ha usado para tejer su red de vigilancia y arrastre.

A. EL GOBIERNO FEDERAL CONSTRUYÓ EL SISTEMA DE CONTROL DE IMMIGRACION, POR ENCIMA DE UN SISTEMA DE VIGILANCIA Y CASTIGO QUE YA ERA INJUSTO.

Durante la mayor parte del siglo XX, las deportaciones a gran escala eran ad hoc y episódicas, típicamente motivadas por reacciones xenófobas a eventos políticos en particular. Ejemplos incluyen las primeras deportaciones realizadas bajo la Ley de Exclusión China y las barridas militarizadas de la frontera para regresar a los trabajadores mexicanos bajo la iniciativa de mediados del siglo XX que el gobierno llamaba *Operation Wetback* (Operación Mojado), por el insulto racial.[39]

Sin embargo, en 1986 el gobierno empezó a construir una burocracia para la aplicación sistemática de medidas de control migratorio, explotando cada vez más las mismas consignas de "ley y orden" que dieron lugar a una época de encarcelación masiva para justiciar la criminalización de los inmigrantes. Aquel año, impulsado por las presiones creadas por las normas de penas mínimas de la época de Reagan que atestaron las cárceles, el Congreso aprobó la *Immigration Reform and Control Act* (Ley de Control y Reforma de la Inmigración, IRCA, por sus siglas en inglés), la cual estipuló que los no ciudadanos condenados por ciertos crímenes debían ser deportados "tan diligentemente como sea posible".[40] Diez años después, en 1996, la *Illegal Immigration Reform and Immigrant Responsibility Act* (Ley de Reforma de la Inmigración Ilegal y de Responsabilidad del Inmigrante, IIRIRA, por sus siglas en inglés), amplió de manera radical el número y los tipos de crímenes que podían hacer que una persona estuviera sujeta a ser detenida y deportada, a menudo de manera obligatoria.[41] Después de la aprobación de IIRIRA, el número de personas detenidas y deportadas se expandió dramáticamente juntamente con el aumento de personas encarceladas a través del sistema penal.[42] En años subsecuentes, el Congreso siguió usando el constructo de la criminalidad para ampliar los fundamentos de la deportación y reducir las protecciones legales para las personas bajo custodia migratoria o en los tribunales migratorios.[43]

Mientras la legislatura usaba el marco del sistema de justicia penal para ampliar las bases reglamentarias de la deportación, las agencias encargadas de la aplicación de las leyes migratorias dependían de los recursos de las policías estatales y locales para investigar a las personas con fines de deportación. En 1988, el INS lanzó un par de programas, los cuales eventualmente fueron consolidados en el *Criminal Alien Program* (Programa de Extranjeros Criminales, CAP, por sus siglas en inglés), que mandaba a funcionarios federales de seguridad en asuntos migratorios a las cárceles para identificar y arrestar a las personas para ser deportadas. Ocho años después, el Congreso autorizó los acuerdos 287(g), nombrados así por la cláusula de autorización en la *Immigration and Nationality Act* (Ley de Inmigración y Nacionalidad) que facultaba a las policías estatales y locales a aplicar las leyes migratorias. Aunque muchos programas 287(g) autorizaban a los policías que operaban en el campo, la mayoría los capacitaba para operar en las cárceles, en donde se dedicaban a identificar a aquellos individuos bajo custodia que el INS podía deportar.[44] Luego su creación en 2003, ICE ha continuado dependiendo de CAP y los acuerdos 287(g) para investigar a potenciales blancos de deportación entre los individuos que han sido presentados ante el sistema de justicia penal.

Una consecuencia de construir sistemas de control migratorio además de sistemas penales, es que las comunidades de inmigrantes negras o mulatas que ya sufren de ataques brutales y discriminatorios por parte de las fuerzas del orden público son doblemente vigiladas, y cuando estas vigilancias resultan en arrestos, también son doblemente castigadas.

En 2008, ICE expandió su cooptación de infraestructura policial para que también incluya infraestructura digital con el lanzamiento del programa de Comunidades Seguras (S-Comm). La piedra angular de S-Comm es una iniciativa de compartición de huellas digitales que automáticamente manda las huellas de cualquier persona acusada por las agencias de seguridad federales, estatales o locales al FBI o ICE.[45] Aunque muchos estados se negaban al principio a registrarse en S-Comm, el gobierno de Obama decretó que la participación era obligatoria.[46] Como resultado, todas las 3,181 demarcaciones de seguridad en el país—en todos los 50 estados, el distrito federal y cinco territorios—se registraron en el programa.[47] En el 2014, después de años de presiones intensas del movimiento de derechos de los migrantes, el presidente Obama y el Secretario del DHS, Jeh Johnson, suspendieron S-Comm pero lo remplazaron con algo muy parecido, el *Priority Enforcement Program* (Programa de Aplicación Prioritaria de la Ley, PEP por sus siglas en inglés), dejando los procesos de compartición de información biométrica sin cambios a lo largo del país.[48] Eso permitió que el presidente Trump emitiera una orden ejecutiva que volvió a arrancar S-Comm de manera inmediata cinco días después de su toma de posesión.[49] Aunque el presidente Joe Biden revocó esa orden a principios de 2021,[50] el programa de compartición de huellas digitales permanece en vigor hasta el día de hoy.

Estos programas de compartición de datos y acuerdos de cooperación con las agencias de seguridad se volvieron piedras angulares en la aplicación de las leyes migratorias en EE.UU. Apenas tres años después del lanzamiento de S-Comm, el número de personas deportadas bajo el programa conformaba un 20% de las deportaciones totales de ese año.[51] Para 2020, alrededor de 70% de los arrestos de ICE surgieron de notificaciones enviadas a funcionarios de ICE sobre la próxima liberación de alguien de la cárcel.[52] El creciente grado de cooperación entre los funcionarios migratorios y las agencias de seguridad también coincidió con un aumento drástico en el número de deportaciones de EE.UU. Entre 1955 y 1988, año en que el INS lanzó los programas previos al CAP, EE.UU. nunca deportó más de 30,000 personas en un año. Después de 1988, las agencias de migración nunca deportaron *menos* de ese número de personas en un año. A partir de la creación de ICE en 2003, el número de personas deportadas anualmente nunca fue por debajo de 200,000, alcanzando un máximo de 432,448 en 2013[53], año en que Obama intentó que se aprobara una ley para reformar el sistema migratorio.[54]

A pesar de lo arraigada que se ha vuelto la dependencia de ICE en las agencias de seguridad estatales y locales, la autoridad legal para muchas de estas iniciativas permanece borrosa. Ninguna ley autoriza de manera explícita el programa de compartición de huellas digitales ni obliga a que las agencias estatales y locales participen.[55] Lo mismo es cierto en el caso de muchas otras formas de compartición de información, como la inclusión de los registros civiles de inmigración con el nombre de *Immigration Violator Files* (Archivos de infractores de las leyes migratorias) en la base de datos de crímenes del FBI.[56] Las

estrategias de vigilancia descritas en este informe, hechas posibles por la tecnología digital y la infraestructura desarrolladas en los últimos 20 años, sencillamente no fueron contempladas en los marcos legales y de diseño de políticas relacionadas con la inmigración, y mucho menos en los temas de privacidad y derechos civiles en general. Limitar las prácticas de ICE a través de la litigación ha sido una difícil batalla desde los primeros desafíos legales a la Ley de Exclusión China, que estableció el precedente de una sumisión extrema al poder ejecutivo en asuntos de inmigración.[57]

B. DESPUÉS DEL 11 DE SEPTIEMBRE, ICE AMPLIÓ AGRESIVAMENTE SUS FUENTES DE DATOS MÁS ALLÁ DE LA POLICÍA Y LAS AGENCIAS PENITENCIARIAS.

Aunque las iniciativas de ICE que trataban de sacar información de las policías estatales y locales fueron desplegadas con mucha publicidad, sus esfuerzos de alcanzar flujos de datos desde fuentes *ajenas* a las agencias de seguridad han sido extremadamente herméticos. ICE empezó a ampliar el alcance de su recolección de datos como respuesta a los acontecimientos del 11 de septiembre del 2011, como parte de una iniciativa federal generalizada de aumentar radicalmente la vigilancia nacional bajo los auspicios de "la guerra al terror". Antes del 11-S, las autoridades migratorias raramente investigaban casos fuera del contexto criminal. El INS no tenía personal dedicado a encontrar y deportar a personas que se habían quedado más tiempo de lo permitido en sus visas, o a individuos con órdenes finales de remoción pendientes (conocidos como *abscondees*).[58] De manera explícita, el INS afirmaba que manejar ese tipo de casos no era una prioridad.[59] La agencia pocas veces perseguía a personas con órdenes de remoción, y sus investigadores no trabajaban con casos de *abscondees* como política institucional.[60]

Una de las razones principales por las que el INS generalmente no perseguía a los que habían permanecido más tiempo de lo permitido en sus visas, o a los que tenían órdenes de remoción pendientes, es que se le dificultaba encontrarlos. Tal y como notó la agencia, los *abscondees* mayormente vivían en las comunidades en lugar de estar encarcelados.[61] Cuando el Inspector General del Departamento de Justicia (DOJ, por sus siglas en inglés) auditó el *Detention & Deportation Program* (Programa de Detención y Deportación) del INS, descubrió que la falta de direcciones era una de las razones más frecuentemente citadas al informar sobre la incapacidad de emitir un aviso de rendición, el cual notificaba a las personas la fecha de su deportación.[62] Aunque desde los años 1940 la ley federal había obligado a los residentes permanentes y a los poseedores de visas a registrar sus direcciones con el gobierno y a notificar a los funcionarios federales de cualquier cambio de dirección,[63] esos requisitos raramente se aplicaban y pocas personas cumplían con ellos, lo cual significaba que los registros federales de direcciones eran de poca utilidad para las investigaciones del INS.[64]

El INS consideró nuevas maneras de acumular más información para dirigirse a esos casos, pero al final no dio seguimiento para implementarlas. Por ejemplo, algunos funcionarios del INS sugirieron que la agencia acudiera a los DMV y a las agencias de datos para conseguir los datos de las direcciones:

> Si no hay una última residencia o dirección laboral para el extranjero, las búsquedas frecuentemente no son prácticas . . . El Director Distrital en Miami, junto con los gerentes D&D en otras partes, notaron que el

> acceso a las bases de datos de vehículos motorizados y burós de crédito a nivel nacional, además del acceso a los datos de Seguridad Social, ayudarían a localizar a los extranjeros.[65]

Las recomendaciones no fueron adoptadas.

Todo cambió después del 11-S. Cuando se descubrió que dos de los quince secuestradores se habían quedado más tiempo de lo permitido en sus visas, los funcionarios gubernamentales aprovecharon ese hecho para remodelar el discurso sobre la aplicación estadounidense de las leyes migratorias. "Para los terroristas, los documentos de viaje son tan importantes como las armas", escribió la Comisión del 11-S y concluyó que "un uso más eficaz de la información disponible en las bases de datos del gobierno estadounidense pudo haber identificado hasta a tres de los secuestradores".[66]

De repente, rastrear a los que se habían quedado más tiempo de lo permitido en las visas y a los que tenían órdenes de remoción pendientes se convirtió en una prioridad máxima, con un claro enfoque hacia las personas de origen musulmán y árabe.[67] En enero de 2002, el subfiscal general Larry Thompson lanzó la *Absconder Apprehension Initiative* (Iniciativa Aprehensión de Fugitivos, AAI por sus siglas en inglés), estableciendo 40 puestos de agentes migratorios en siete ciudades para "localizar, arrestar, entrevistar y deportar" a personas en la comunidad más amplia.[68] Según los lineamientos del programa, los agentes migratorios debían priorizar a las personas que venían de "países en los que ha habido la presencia o actividad terrorista de Al Qaeda".[69]

No obstante, al cabo de un año, quedó claro que el programa enfrentaba las mismas limitaciones que habían obstaculizado iniciativas parecidas en el pasado: la falta de datos confiables. Al principio, el INS había fijado como meta deportar a todos los 314,000 no ciudadanos con órdenes finales de remoción en EE.UU,[70] pero después de seis meses, los equipos de la AAI solo habían podido localizar a 712 personas.[71] La Oficina de Responsabilidad Gubernamental (GAO por sus siglas en inglés) realizó un análisis que mostró que los esfuerzos de la iniciativa se habían visto frustrados por registros no confiables de direcciones en las bases de datos gubernamentales y, otra vez, recomendó que el gobierno adoptara otros métodos de obtener esa información, como comprarla de las agencias de datos.[72]

En última instancia, el INS habría de pasar a su sucesor la tarea de investigar a los que se habían quedado más tiempo de lo permitido en sus visas, así como a las personas con órdenes finales de remoción pendientes. ICE heredó los equipos que el INS creó en febrero de 2002 para localizar a inmigrantes con órdenes finales de remoción pendientes, los cuales estaban organizados en el *National Fugitive Operations Program* (Programa Nacional de Programas contra Fugitivos).[73] De manera puntual, ICE también creó dos nuevas oficinas, la *Fugitive Case Management Unit* y la *Fugitive Operations Support Center* (Unidad de Manejo de Casos Fugitivos y el Centro de Apoyo para Operaciones contra Fugitivos respectivamente), para enviar información y pistas a los equipos acerca de personas que podrían ser deportadas.[74] En junio de 2003, ICE también estableció la primera unidad para identificar y remover a los que se habían quedado más tiempo de lo permitido en las visas: la *Compliance Enforcement Unit* (Unidad de Aplicación del Cumplimiento), la cual fue renombrada como la *Counterterrorism and Criminal Exploitation Unit* (Unidad de Explotación Criminal y Antiterrorismo) en 2010.[75]

De manera sistemática, ICE empezó a adquirir nuevas colecciones de datos que podían usar para jalar a las personas hacia la detención y la

deportación. A diferencia de los que alimentaban las iniciativas anteriores, estos nuevos datos provenían de manera aplastante de fuentes ajenas a las agencias de seguridad, incluyendo agencias y oficinas al interior de los gobiernos federales, estatales y locales, así como del sector privado. A medida que ICE intentaba remediar las carencias de datos que obstaculizaron los esfuerzos anteriores para perseguir casos, acumuló registros que iban mucho más allá de los que proporcionaban las policías estatales y locales, permitiendo así a la agencia rastrear un número mucho más grande de personas. Por medio de estos esfuerzos, el alcance de la vigilancia de ICE excedió, por mucho, el de las bases de datos de por sí masivas que se mantenían sobre los detenidos y poseedores de visas, usurpando de este modo conjuntos de datos que fácilmente incluían la mayoría de las personas en EE.UU.

C. LOS CONTRATOS DE ICE REVELAN UNA ENORME EXPANSIÓN EN SU CAPACIDAD DE VIGILANCIA.

A lo largo de la última década, ICE ha invertido mucho en programas para rastrear grandes franjas de la población general. Nuestra revisión de más de 100,000 transacciones de gastos de 2008 al 2021 revela que el gasto anual de la agencia en programas de vigilancia aumentó más de cinco veces durante este periodo, disparándose de alrededor de $71 millones de dólares a alrededor de $388 millones cada año.[76] Para analizar los gastos en vigilancia a lo largo de este periodo en mayor detalle, categorizamos cada una de las transacciones contractuales de la agencia a partir del servicio primario de vigilancia que proporcionó. Esas categorías se definen en el **Recuadro 1**. La lista completa de los contratos de vigilancia que identificamos y nuestros cálculos de los gastos de ICE se encuentran en el **Apéndice**.

Nuestra categorización de las transacciones de ICE nos permite comprender mejor la magnitud de los gastos de la agencia en programas de vigilancia, así como el alcance de la información que proporcionan estos programas. Por ejemplo:

- En total, ICE gastó poco más de $1.3 mil millones en proveedores de **geolocalización** del 2008 a 2021. El contrato más amplio y polémico de todos los firmados permite a ICE acceder a una base de datos de escaneos de matrículas de automóviles proporcionado por Vigilant Solutions. La base de datos contiene fotos de alta velocidad de las matrículas de los vehículos en movimiento, así como la fecha, hora y coordenadas GPS del sitio donde se capturó la imagen.[77] La base de datos de Vigilant consiste en dos tipos de escaneos de matrículas: los que fueron recolectados por empresas privadas—conocido como datos de matrículas comerciales—y los que fueron recolectados por las agencias de seguridad.[78] Según documentos obtenidos por la ACLU de California del Norte, la recolección de Vigilant de los escaneos de matrículas comerciales ocurre en lugares como autopistas de peaje, estacionamientos y garajes, así como por medio de agentes de embargo de vehículos privados en 47 estados,[79] cubriendo áreas metropolitanas que abarcan aproximadamente 54% de la población de EE.UU.[80] Usando esa base de datos, ICE puede cotejar automáticamente nuevos escaneos de matrículas con una "lista caliente" de vehículos que está buscando.[81] En 2014, el Secretario del DHS del gobierno de Obama, Jeh Johnson, había argumentado

RECUADRO 1.
CATEGORIZACIÓN DE LOS GASTOS EN VIGILANCIA DE ICE

A menudo, ICE usaba un solo contrato para obtener múltiples sistemas de vigilancia. Un contrato con el vendedor Babel Street, por ejemplo, podría proporcionar a ICE el acceso tanto a información de geolocalización, como a un conjunto complementario de herramientas de análisis de datos.[82] Asignamos a cada transacción contractual una funcionalidad primaria, cada una de las cuales se describe a continuación.

Biometría. Esta categoría abarca contratos para tecnologías que permiten a ICE recolectar y analizar los datos biométricos, incluyendo herramientas para el reconocimiento facial y pruebas de huellas digitales o de ADN.

Análisis de datos. Esta categoría abarca contratos para tecnologías que permiten a ICE vincular fuentes diversas de datos, analizar grandes volúmenes de datos y realizar el manejo de casos.

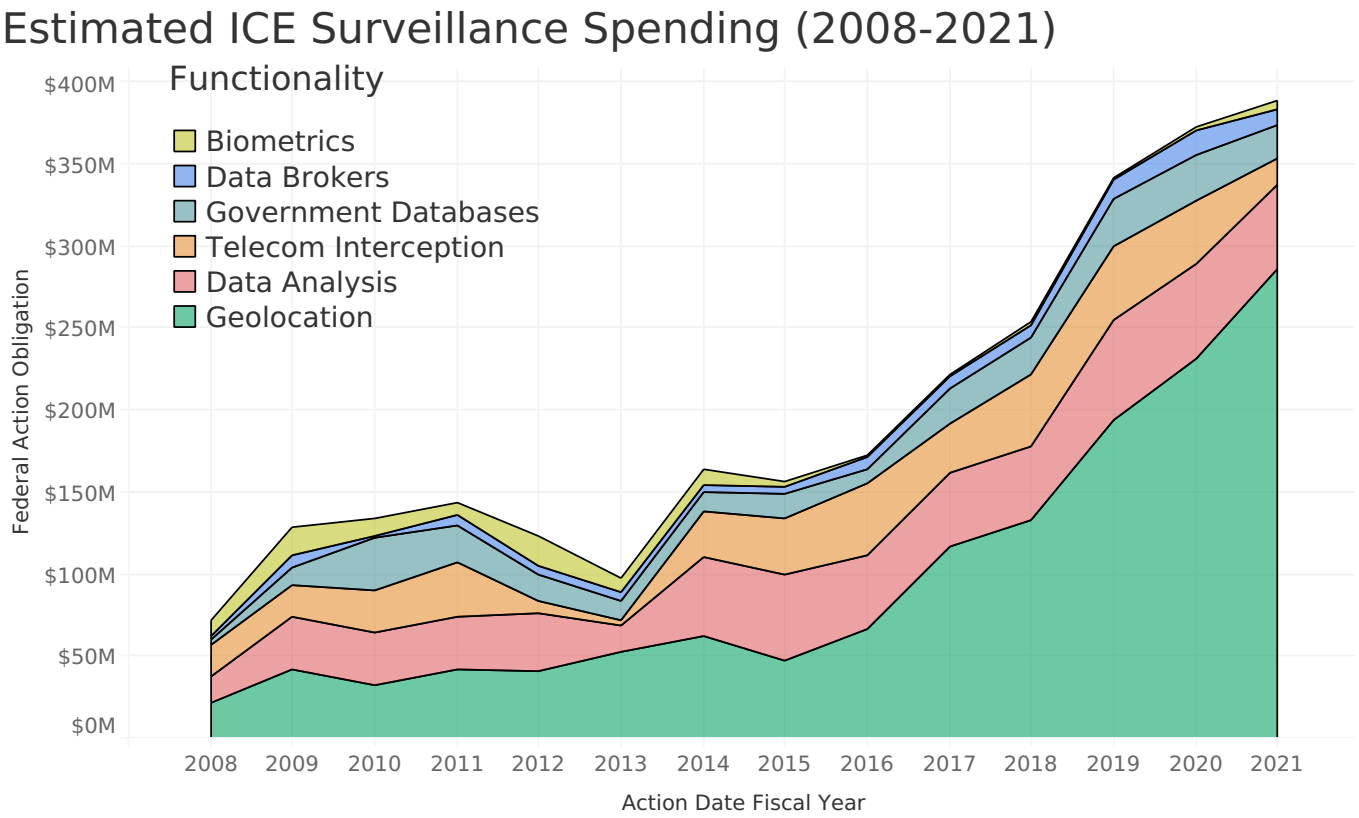
Geolocalización. Esta categoría abarca contratos de ICE relacionados con los lectores automáticos de matrículas de automóviles, información proporcionada por televisión de circuito cerrado, unidades de rastreo GPS, simuladores de torres de telefonía celular y monitores de tobillo utilizados en los programas Alternativas a la Detención.

Agencias de datos. Esta categoría abarca contratos que permiten a ICE acceder a las bases de datos privadas operadas por empresas que juntan y venden información individual, incluyendo los encabezados de informes crediticios y los registros de servicios públicos.

Bases de datos gubernamentales. Esta categoría abarca contratos para bases de datos estatales y locales, sistemas para obtener un acceso indirecto a estas bases de datos y herramientas que facilitan la compartición dentro de las mismas.

Intercepción de telecomunicaciones. Esta categoría abarca contratos para tecnologías que permiten a ICE analizar e interceptar telecomunicaciones, incluyendo dispositivos de intervención telefónica Título III y servicios de traducción Título III, así como tecnologías de intercepción para Wi-Fi. Esto no abarca los compiladores de información que podrían incluir vigilancia de telecomunicaciones o video.

Figura 1. Inversiones estimadas de ICE por funcionalidad, 2008-2021



Biometricas=Biometría, Data Broker=Agencias de datos, Government Database=Bases de datos gubernamentales, Telecom Interception=Intercepción de telecomunicaciones, Data Analysis=Análisis de datos, Geolocation=Geolocalización, Federal Action Obligation=Obligación de acción federal, Action Date Fiscal Year=Fecha de acción Año fiscal

preocupaciones de privacidad para que se cancelaran los planes de que la agencia entera de ICE tuviera acceso a la base de datos, pero funcionarios del DHS del gobierno de Trump firmaron un contrato para el acceso global a los datos de Vigilant a finales de 2017.[83]

- ICE gastó más de $96 millones en **biometría** en este periodo. Uno de los primeros contratos de biometría de ICE, con fecha del 18 de julio de 2008, otorgó $3,000 para un contrato de cinco años para "servicios con los servicios RMV [Registro de Vehículos Motorizados] del estado de Rhode Island para obtener acceso a la base de datos de reconocimiento facial con el objeto de reconocer a extranjeros criminales"[84] (las primeras búsquedas conocidas de ICE de un departamento de vehículos motorizados se ubican en los últimos días del gobierno de Bush, unos seis años antes de lo que se sabía previamente). Uno de los contratos más recientes de biometría, de septiembre de 2020, asignó $224,000 para la oficina de apoyo de ICE en Dallas para usar software de reconocimiento facial de Clearview AI, empresa que había enfocado sus algoritmos en imágenes extraídas de sitios web públicos y páginas de redes sociales sin el conocimiento de sus sujetos.[85]

- ICE gastó alrededor de $97 millones en **agencias de datos** en este periodo. El contratista principal que proporcionó este servicio es Thomson Reuters, que ofrece una base de datos de búsqueda de personas

llamado CLEAR. La versión de CLEAR construida para las agencias de seguridad incluye datos de un rango masivo de fuentes diferentes, incluyendo licencias de manejo y matriculaciones de vehículos; encabezados de informes crediticios que contienen nombres, direcciones, números de teléfono y otra información personal en la parte superior del informe, recolectados en tiempo real de las tres principales agencias de informes crediticios, tal y como se comenta en el **Hallazgo 3**, así como registros de domiciliarios de clientes de más de 80 empresas nacionales y regionales de teléfono, cable, gas, electricidad y agua en todo el país.[86] El contrato de ICE para acceder a la base de datos CLEAR inició en 2017 y dejaron que caducara en febrero de 2021.[87] Al parecer, la agencia remplazó este servicio con un nuevo contrato con LexisNexis Special Services, que ofrece una base de datos similar.[88]

ICE empezó a usar escaneos faciales en las fotos de licencias de los DMV en los últimos días del gobierno de George W. Bush.

- ICE gastó alrededor de $252 millones para acceder a las **bases de datos gubernamentales** en este periodo. La base de datos clave en esta categoría es NLETS, la *International Public Safety and Justice Network* (Red Internacional de Seguridad Pública y Justicia), anteriormente conocida como el *National Law Enforcement Telecommunications System* (Sistema Nacional de Telecomunicaciones para la Seguridad). Tal y como se comenta en el **Hallazgo 2**, NLETS es una red operada por una organización sin fines de lucro que permite a los agentes de ICE a lo largo del país buscar sin orden judicial en las bases de datos de los DMV de 34 estados para propósitos de control migratorio, incluyendo las bases de datos de cinco de los 16 estados que ofrecen a las personas indocumentadas la posibilidad de solicitar licencias de manejo.[89] Bajo Trump, ICE aumentó muchas de sus inversiones en vigilancia; en pocas áreas fue más marcado este aumento que en el acceso de ICE a las bases de datos gubernamentales.

- ICE gastó alrededor de $389 millones en la **intercepción de telecomunicaciones** en este periodo.[90] Los vendedores principales que aumentaron las capacidades de vigilancia de ICE fueron JSI Telecom y Penlink, que venden equipo de intercepción.[91] ICE usa el equipo de Penlink para rastrear llamadas o el uso de internet en tiempo real, así como recolectar las actividades de correo electrónico y redes sociales de los individuos para búsquedas posteriores.[92] Aunque se autoriza caso por caso, cada intervención se beneficia de las reservas de información de ICE. ICE comparte registros obtenidos en las intervenciones de su sistema de manejo de casos usando un software hecho a la medida por Penlink, el cual permite a la agencia mapear los vínculos entre las personas.[93] ICE intercepta las comunicaciones a tal magnitud que precisa de media docena de proveedores para darle sentido: servicios de traducción de la información obtenida de las intervenciones y contratos de almacenamiento constituyen más de la mitad del gasto total de ICE en la intercepción de telecomunicaciones.

- ICE gastó alrededor de $569 millones en el **análisis de datos** en este periodo. Este monto incluye el pago erogado al tercer contratista más grande de ICE en términos de dólares: Palantir Technologies. De 2008 a 2021, ICE otorgó un total de $186.6 millones solo a Palantir. Los programas hechos a la medida de Palantir vinculan bases de datos de un vasto rango de fuentes gubernamentales y privadas, lo cual permite a los agentes de ICE obtener acceso y visualizar una red interconectada de datos sacados de casi todos los aspectos de la vida de un individuo. ICE tiene acceso a tantos datos, de tantas fuentes, que su tercer proveedor más grande ni siquiera es un proveedor de datos, sino una empresa que ayuda a ICE a darle sentido a dichos datos.

Además de apropiarse de información de los gobiernos estatales y el sector privado, ICE también penetró en las fuentes federales. Poco después de su fundación, el *ICE's Fugitive Operations Support Center* (Centro de Apoyo para Operaciones contra Fugitivos de ICE) empezó a escudriñar la información sobre estadounidenses guardada en las bases de datos federales en el *Department of State, Department of Labor* y el *Department of Housing and Urban Development*, (Departamento de Estado, Departamento del Trabajo y Departamento de Vivienda y Desarrollo Urbano respectivamente), usando esa información para encontrar personas a detener y deportar.[94]

Tal y como se comenta en el **Hallazgo 4**, la agencia incluso aprovechó datos de los niños sin acompañante en la frontera para investigar a personas para fines de deportación. Empezando como una prueba en 2017, y luego como política formal a partir de 2018, ICE usaba la información proporcionada por los menores sin acompañante, así como por cualquier guardián que se ofreciera a acogerlos, para encontrar y arrestar a esos guardianes. ICE realizó esa práctica bajo un Memorándum de Entendimiento con la *Office of Refugee Resettlement* (Oficina de Reasentamiento de Refugiados, ORR por sus siglas en inglés) del Departamento de Salud y Servicios Humanos, agencia encargada por ley federal de la protección del bienestar de los niños que llegan sin acompañante a la frontera.[95]

D. AL OBTENER DATOS DE TODAS LAS FUENTES DISPONIBLES, LOS PROGRAMAS DE VIGILANCIA DE ICE HAN LANZADO UNA RED DE ARRASTRE SOBRE LA POBLACIÓN ENTERA DE EE.UU.

La escala masiva de los programas de vigilancia de ICE han convertido a la agencia en una pieza clave de lo que Anil Kalhan, profesor en la facultad de leyes Drexel Kline, ha llamado "el estado de vigilancia migratoria".[96] Según Kalhan, la vigilancia de ICE ha "transformado un régimen de control migratorio (que operaba principalmente sobre los no ciudadanos en la frontera) en parte de un régimen más expansivo de vigilancia de la migración y la movilidad que opera sin fronteras geográficas tanto en ciudadanos como en no ciudadanos".[97] La profesora Ana Muñiz de la Universidad de California en Irvine identificó un cambio parecido dentro de un sistema específico de control migratorio, la *Enforcement Integrated Database* (Base de Datos Integrada del Orden Público). Ella argumenta que el incremento de acuerdos para la recolección y compartición de datos transformaron la base de datos de "un sistema de manejo de casos en un sistema de vigilancia masiva".[98]

Aunque el Congreso ha autorizado a ICE el ejercicio de ciertos poderes limitados de investigación,[99] nunca ha autorizado de manera explícita la escala masiva de programas de vigilancia. Consideremos, por ejemplo, el programa S-Comm. Como notó Kalhan en 2013, la *Visa Reform Act* (Ley de Reforma de las Visas) encargó a las agencias federales la tarea de asegurarse de que las bases de datos estén "accesibles fácilmente y sin inconvenientes" a los funcionarios federales de inmigración que son "responsables de determinar la admisibilidad . . . o deportabilidad de un extranjero".[100] Pero el Congreso nunca autorizó de manera explícita la "transmisión rutinaria y al por mayor al DHS de todos los registros de identificación estatales y locales" incluidos en S-Comm;[101] que es el mismo caso para los otros programas de vigilancia de ICE. El Congreso nunca ha autorizado explícitamente a ICE solicitar de manera rutinaria registros en masa acerca del público a agencias estatales o empresas privadas.

II. ICE APROVECHA LA CONFIANZA QUE EXISTE EN LOS DMV DE LOS ESTADOS PARA REALIZAR DEPORTACIONES Y EVADIR LAS POCAS PROTECCIONES ESTABLECIDAS CONTRA ESA PRÁCTICA.

El gobernador Jay Inslee firma la Orden Ejecutiva Núm. 17-01 en Olympia el 23 de febrero, 2017.
(Fotografía: Oficina del Gobernador de WA)

En enero del 2018, Jay Inslee tenía una crisis en las manos. Estaba en su segundo periodo como gobernador del estado de Washington, tenía ambiciones presidenciales y la última cosa que necesitaba era un escándalo relacionado con la inmigración; pero acababa de llegar uno. Según un reportaje publicado en el periódico The Seattle Times, el *Department of Licensing* estatal (Departamento de Licencias) había estado entregando, de manera regular, información personal de los conductores de Washington—incluyendo sus nombres, direcciones y las fotos de sus licencias—a agentes de ICE que investigaban a los residentes del estado para su deportación.[102]

La oficina de Inslee fue tomada por sorpresa. El gobernador había intentado proteger la privacidad de los inmigrantes en el estado, afirmando poco después de la toma de posesión de Trump que

Washington no sería un "participante voluntario" en sus "políticas malintencionadas que rompen familias".[103] En el 2017, Inslee había puesto esta promesa en acción al firmar una orden ejecutiva que prohibía a las agencias estatales cooperar con las autoridades migratorias federales.[104] Eso incluía el Departamento de Licencias de Washington, que prometía a aquellos que solicitaban licencias de manejo que el estado era un lugar seguro donde los inmigrantes podrían "vivir, trabajar, manejar y prosperar".[105]

Pero para Baltazar "Rosas" Aburto Gutiérrez, de 35 años, y otros inmigrantes como él, la agencia no había cumplido esa promesa.[106] Según registros descubiertos por The Seattle Times, agentes de ICE habían ido al Departamento de Licencias para buscar información sobre Gutiérrez—residente del Condado Pacific durante quince años—como parte de los preparativos para su arresto, que sucedió cuando iba a una tienda de abarrotes para comprar café y huevos. Sospechaban que Gutiérrez era indocumentado, en parte, porque había usado un acta de nacimiento mexicana para solicitar su licencia de manejo, lo cual está autorizado en el estado de Washington desde 1993.[107]

La revelación de que ICE podía acceder a la base de datos de los conductores de Washington

Aburto Gutiérrez cosechando almejas cerca de la Bahía de Wallapa en la costa de Washington. (Foto: Gladys Díaz)

reverberó a lo largo del estado. Inslee emitió una disculpa personal, admitiendo que el estado "se quedó corto" en su compromiso de proteger a los inmigrantes.[108] También actuó con presteza para prevenir que algo así volviera a ocurrir. Inslee ordenó inmediatamente a los empleados del Departamento de Licencias dejar de compartir con ICE información sobre los conductores en la ausencia de una orden judicial y ordenó al departamento realizar una revisión interna exhaustiva de sus prácticas de compartición de datos.[109]

De la revisión efectuada por el Departamento de Licencias llegó un primer vistazo del alcance completo de la vigilancia de ICE sobre los conductores de Washington. Los resultados mostraron que el Departamento de Licencias había otorgado a ICE el acceso directo a su *Driver and Plate Search* (Base de Datos Búsqueda de Conductores y Matrículas, DAPS, por sus siglas en inglés), el cual contenía registros detallados de los conductores y vehículos registrados en el estado.[110] Según documentos descubiertos por el *Center on Privacy & Technology*, por lo menos 28 agentes de ICE[111] habían usado DAPS para "realizar vigilancia y detener" a inmigrantes que vivían en Washington.[112] Los registros de DAPS revelan que la *Enforcement and Removal Operation* (Oficina de Detención y Deportación, ERO, por sus siglas en inglés) realizó más de 100,000 búsquedas en un periodo de dos años entre el 1 de enero de 2016 y el 1 de enero de 2018.[113]

Registros adicionales descubiertos por el *Center on Privacy & Technology* e incluidos en un reportaje de The Washington Post mostraron que, con fines migratorios, agentes de ICE también solicitaron búsquedas de reconocimiento facial de la base de datos de fotografías de las licencias de manejo del estado.[114]

Para cuando los resultados de la investigación se hicieron públicos, el Departamento de Licencias había decidido cortar el acceso de ICE a la base de datos DAPS.[115] El departamento ya no permitía búsquedas de reconocimiento facial en las fotografías de las licencias de manejo de los conductores para propósitos de control migratorio. Washington estaba asegurando a los conductores que había cerrado con llave la puerta a la información de las licencias de manejo del estado. "Realmente queremos dejar en claro," dijo la oficina de Inslee a la prensa, "que no vamos a permitir que el gobierno federal se apropie de nuestros recursos estatales como parte de sus esfuerzos migratorios".[116] El mensaje de Washington a todos los conductores era claro: les cuidaremos las espaldas.

Pero las tentativas de Inslee de cortar el acceso de ICE a los registros de las licencias de manejo solo parece haber motivado a la agencia a buscar una puerta lateral secreta.

La orden ejecutiva del gobernador con fecha de 2017 había terminado con la política "muy liberal" del Departamento de Licencias de compartir las fotos de las licencias de manejo,

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 individals 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.

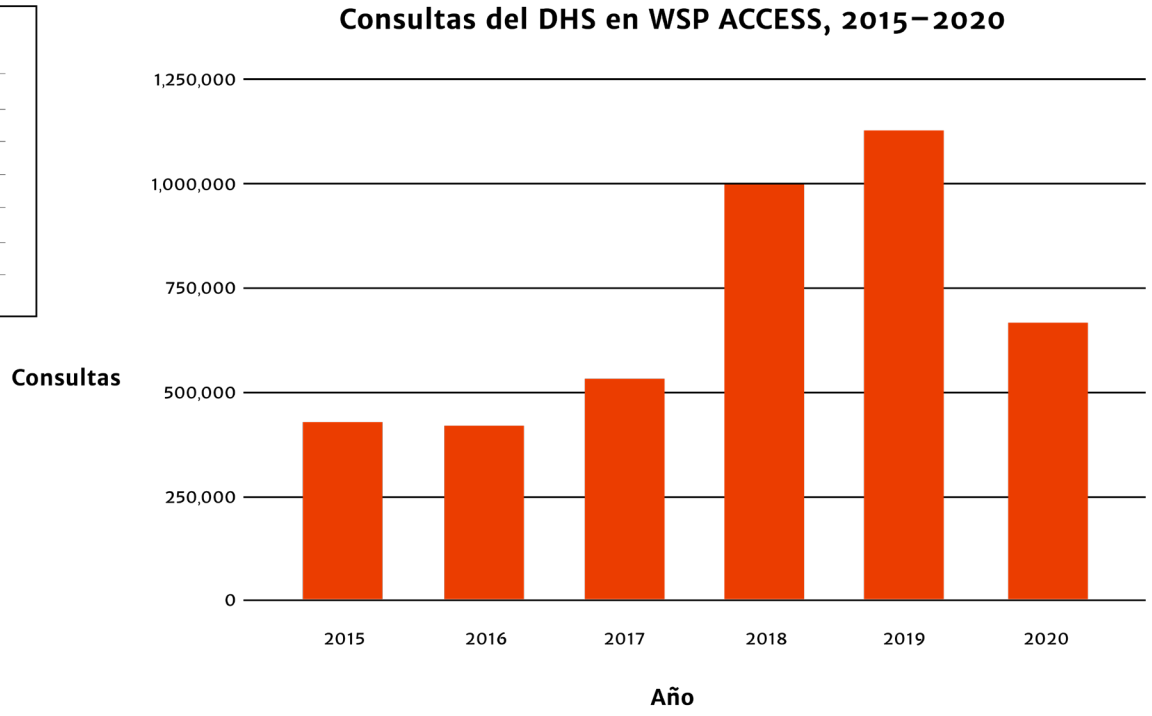
Fragmento de una solicitud del 14 de noviembre de 2013 enviada por un agente de ICE para el acceso directo a la base de datos de conductores y matrículas del estado de Washington. (Fotografía: Center on Privacy and Technology de documentos FOIA.)

pero tal y como lo explicó un empleado a un agente de la CBP, había otra manera. El Departamento de Licencias no era la única agencia en el estado que podía otorgar el acceso a los registros de conductores y fotos de licencias, la Policía Estatal de Washington operaba un sistema electrónico de compartición de datos conocido como WSP ACCESS, y según el empleado, los agentes podían usarlo para solicitar y recibir electrónicamente las fotografías de las licencias de los conductores de Washington.[117] Registros nunca antes vistos de Washington sugieren que el DHS, la agencia matriz de ICE, no dudó en aprovechar esa vía alterna para tener acceso a los datos de los conductores. El número de solicitudes de información para licencias de manejo que el DHS envió a través de WSP ACCESS se disparó en los años posteriores a la orden ejecutiva. Como se demuestra en la **Figura 2**, de 2016 a 2019 el número de consultas anuales del DHS aumentó de aproximadamente 400,000 a la asombrosa cifra de 1.1 millones.[118]

También, ICE ha usado WSP ACCESS de manera prolífica para acceder a los datos de los conductores de Washington, a veces con el apoyo de los funcionarios estatales. Tan recientemente como octubre de 2019, agentes de ICE que solicitaban fotografías de las licencias de manejo para propósitos de control migratorio fueron informados por funcionarios del Departamento de Licencias que la imagen de un conductor "podría estar disponible para ustedes en tiempo real en el sistema ACCESS de WSP a través de la búsqueda de conductores".[119] Según una auditoría interna del Departamento de Licencias no publicada previamente, ICE presentó aproximadamente 68,000 solicitudes WSP ACCESS para información sobre licencias de manejo en el 2019,[120] en un tercio de los casos buscaba de fotografías de las licencias de manejo.[121]

Figura 2.

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



A pesar de los mejores esfuerzos del gobernador Inslee, todo indica que ICE continúa gozando de un acceso ilimitado y sin orden judicial a los datos de los conductores de Washington.

De modo alarmante, a pesar de los mejores esfuerzos del gobernador, todo indica que ICE continúa gozando de un acceso ilimitado y sin orden judicial a los datos de los conductores de Washington. ¿Cómo es eso posible? La respuesta se encuentra tanto en la multiplicidad de puntos de acceso entrecruzados a través de los cuales estados como Washington permiten que la información sobre los conductores fluya hacia agencias exteriores, como en la dificultad de cortar esos puntos de acceso. A pesar de los esfuerzos tomados por los estados para restringir el acceso de ICE a los datos de las licencias de los conductores, ICE encuentra rutinariamente maneras para burlar la mayoría de los límites impuestos por los estados. Cuando se cierra un grifo, ICE sencillamente cambia de canal.

Cuando se cierra un grifo, ICE sencillamente cambia de canal.

Esta sección identifica los diferentes canales usados por ICE para acceder a los datos de conductores, describe el alcance y la frecuencia de las búsquedas de la agencia e ilustra cómo un mosaico de leyes federales y estatales (así como la disposición de ICE de evadir sigilosamente las pocas normas significativas que sí existen) han permitido que ICE entreteja los datos de los conductores en su red de vigilancia y arrastre.

A. ICE UTILIZA POR LO MENOS TRES CANALES DIFERENTES PARA TENER ACCESO A LOS DATOS DE LOS CONDUCTORES.

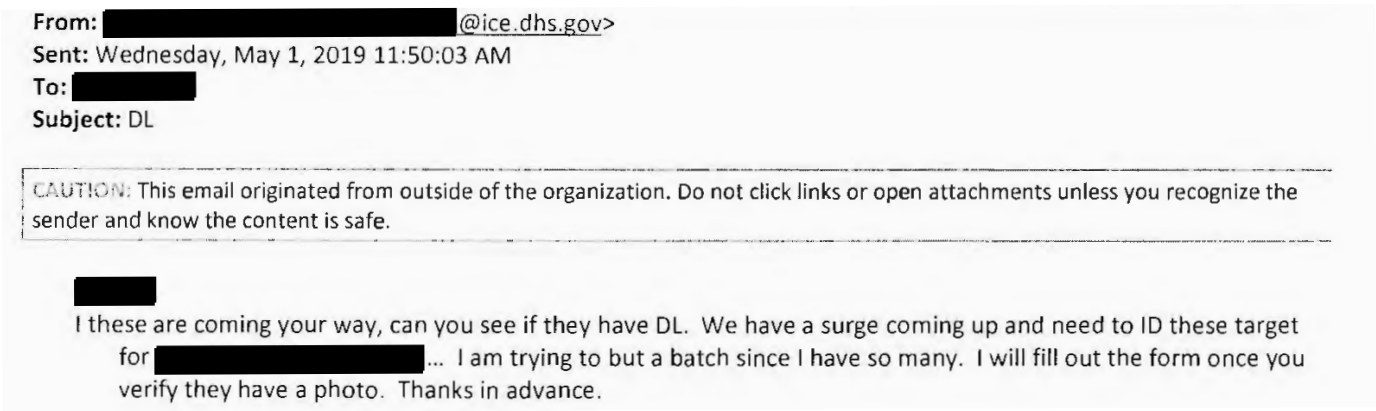
Los investigadores de ICE utilizan un extenso tejido de bases de datos, redes e iniciativas de compartición de datos para tener acceso a los registros de conductores de los estados. El 8 de junio de 2018, un agente de ICE que seguía un caso en Georgia escribió a un funcionario en el *Department of Driver Services* (Departamento de Servicios al Conductor). "¿Puede ayudarme", escribió el agente, "a encontrar una persona específica en GA?" El agente afirmó que tenía el "[número de] celular y los resultados CLEAR" de la persona", refiriéndose a registros sacados de una base de datos comercial, y quería saber si la persona contaba con una licencia de manejo en Georgia.[122] En un correo similar enviado al departamento dos semanas antes de eso, un agente de ICE preguntó si la persona tenía una licencia de manejo, pero solo después de que el agente fue "incapaz de verificar [esta información] en NLETS", otro sistema gubernamental que ICE usa para acceder a los datos de los conductores.[123]

Este conjunto de comunicaciones hace referencia a los tres principales canales que ICE utiliza para obtener información sobre las licencias de manejo estatales. En primer lugar, ICE obtiene acceso a la información de los conductores a través de **solicitudes directas** realizadas a los DMV. Los agentes de ICE pueden contactar a los funcionarios

de los DMV para solicitar registros y pueden, también, solicitar a los funcionarios que realicen búsquedas de reconocimiento facial. En segundo lugar, ICE obtiene acceso a la información de los conductores a través de **bases de datos gubernamentales**. Los agentes de ICE pueden buscar directamente en las bases de datos electrónicas de los conductores y vehículos registrados. Finalmente, ICE obtiene acceso a la información de los conductores a través de **agencias de datos**. Con frecuencia, los DMV venden datos de las licencias de manejo a empresas privadas que revenden el acceso a los agentes de ICE y a otros.

cooperar con la entrega de información acerca de posibles blancos de deportación que un agente de ICE respondió, "¡Vamos a tener que hacerte un agente honorario de ICE!"[125]

Las íntimas relaciones de trabajo entre agentes de ICE y empleados de los DMV permiten que los investigadores de ICE se dirijan directamente a los empleados estatales para pedir información sobre las licencias de manejo. Las solicitudes directas de ICE para información sobre las licencias de manejo llegan en dos formas principales: solicitudes para información asociadas con (1) el nombre de una persona,


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.

Un correo del 1 de mayo de 2019 enviado de un agente de ICE a un funcionario de licencias de Georgia. (Foto: Center on Privacy & Technology de documentos FOIA.)

1. Los agentes de ICE piden directamente a los funcionarios estatales que busquen los datos de los conductores y escaneen sus rostros, actividades a menudo realizadas en secreto.

Los agentes de ICE a menudo se dirigen directamente a los funcionarios de los DMV para solicitar ayuda en obtener información sobre las licencias de manejo. Esas solicitudes con frecuencia se realizan a través de relaciones de colaboración activa de larga duración con los funcionarios estatales de los DMV, quienes suelen estar deseosos de entregar información sobre los conductores a los funcionarios migratorios.[124] En Vermont, por ejemplo, un empleado del DMV se mostraba tan dispuesto a

su fecha de nacimiento u otra información biográfica; y (2) una fotografía de la licencia de manejo de la persona, consultada por medio del uso de tecnología de reconocimiento facial.

a. Solicitudes directas usando información biográfica

En casos en que los agentes de ICE tengan alguna información básica acerca de la persona en la mira, como un nombre o un número de teléfono, pueden enviar un correo a los empleados del DMV para que ayuden a obtener información adicional de los registros de licencia de esa persona. Un DMV estatal individual puede recibir

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

Una solicitud de búsqueda de reconocimiento facial enviada por un agente de ICE a un funcionario del departamento de licencias de Georgia. (Fotografía: Center on Privacy & Technology de documentos FOIA)

docenas de solicitudes directas de agentes de ICE que presentan el nombre de un sujeto u otra información biográfica.[126]

Aunque el número total de solicitudes directas de ICE se ha mantenido mayormente en secreto, la evidencia parece indicar que ICE hace cientos o miles cada año a los DMV en todo EE.UU. Previo a las redadas migratorias planeadas para Atlanta, por ejemplo, un agente de ICE envió un correo al Departamento de Servicios al Conductor de Georgia, en donde solicitaba toda una "tanda" de información sobre licencias de manejo, incluyendo fotografías, porque "viene una oleada" en camino y tenía a "tantas" personas en la mira.[127] Registros parecidos muestran que un agente de ICE envió una solicitud al DMV de Virginia en busca de información acerca de solicitudes de licencias de manejo de los residentes del estado.[128] Esas solicitudes también revelan que las búsquedas de ICE no se han limitado a las personas indocumentadas. En Arizona, un agente de ICE envió un correo al *Department of Transportation* (Departamento de Transporte) solicitando información sobre la licencia de manejo de una persona con estatus en el programa DACA.[129]

b. Solicitudes directas para búsquedas de reconocimiento facial

Cuando la única información fiable que posee ICE acerca de alguien es una fotografía, los investigadores pueden solicitar la ayuda de los funcionarios de los DMV estatales para usar tecnología de reconocimiento facial para buscar a ese individuo entre las fotos de las licencias de manejo en la base de datos del estado.[130]

Los registros muestran que desde el 2015, ICE ha solicitado escaneos de reconocimiento facial en por lo menos **14 estados**. Eso incluye las bases de datos de los DMV de 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] y Wisconsin.[144] (Hasta la publicación de este informe, Colorado,[145] Illinois,[146] Maryland,[147] Utah,[148] Vermont[149] y Washington[150] han prohibido que sus DMV cumplan con las solicitudes de reconocimiento facial de ICE para propósitos de control migratorio civil.) Además, tal como se comenta en el **Hallazgo 1**, ICE también tenía un contrato con el DMV de Rhode Island para poder ingresar a su base de datos de

reconocimiento facial.[151] Todo sumado, esto parece indicar que los agentes de ICE y los funcionarios de los DMV que actuaban a favor de ICE han utilizado tecnología de reconocimiento facial para escanear los rostros de por lo menos **83 millones** de conductores.[152] Esta cifra incluye alrededor de **1 de cada 3** adultos en EE.UU.[153]

Esas búsquedas fácilmente constituyen una red de arrastre. Cuando ICE, junto con los funcionarios de los DMV que actúan a su favor, usa el reconocimiento facial para buscar en la base de datos de las fotografías de las licencias de manejo de un estado, las imágenes de todos están siendo escaneadas por la agencia, no solo de la persona que está bajo investigación. En Wisconsin, un agente de ICE que realizaba una investigación de suplantación de identidad solicitó una comparación de reconocimiento facial con la base de datos de Wisconsin de **4.3 millones** de fotografías de licencias de manejo.[154] En Georgia, otro agente de ICE solicitaba de manera repetitiva comparaciones de las fotografías de un individuo con el conjunto de datos de Georgia de **7.3 millones** de fotografías de licencias de manejo.[155]

El uso de ICE del reconocimiento facial puede dar como resultado identificaciones erróneas y arrestos falsos. Según investigaciones revisadas por colegas y realizadas por los académicos Joy Buolamwini, Timnit Gebru y otros, los algoritmos de análisis facial a menudo tienen un pobre desempeño cuando analizan los rostros de las mujeres, los jóvenes y las personas de tez oscura.[156] Esos problemas de sesgo se extienden a los sistemas de comparación facial y pueden incluso empeorarse cuando los DMV de los estados usan sistemas anticuados de reconocimiento facial, como a veces sucede.[157]

Hay pocas normas que limitan el uso del reconocimiento facial por parte de las agencias de seguridad en general y casi ninguna norma que aborde el uso de esta tecnología por parte de ICE. Aunque las cortes todavía no han emitido un fallo con respecto a la constitucionalidad del reconocimiento facial en el contexto de los controles de seguridad, varios académicos han expresado preocupaciones acerca de su legalidad en varias disposiciones constitucionales, especialmente la Primera y la Cuarta Enmienda, y ni es claro si la práctica está legalmente autorizada en primer lugar. Desde por lo menos mayo de 2020, la política de ICE afirma prohibir el uso de la tecnología de reconocimiento facial por su división ERO para propósitos de control migratorio civil.[158] Sin embargo, en la práctica, no existe una línea nítida que separe la aplicación de las leyes migratorias de carácter civil de las operaciones de la *Homeland Security Investigations* (Oficina de Investigaciones de Seguridad Nacional, HSI, por sus siglas en inglés), un departamento de ICE que tiene como encargo investigar la actividad criminal. Cuando la HSI realiza investigaciones criminales, sus esfuerzos conducen de manera rutinaria a "arrestos colaterales" de personas que no eran blancos originales de la investigación.[159] Como consecuencia, aun si esos arrestos son parte de control migratorio civil, las investigaciones que condujeron a ellos podrían estar exentas de la prohibición manifiesta de ICE del uso de reconocimiento facial.

ICE ha tapado su uso de la tecnología de reconocimiento facial en las fotografías de las

licencias estatales con un grado de secretismo más parecido a lo que se esperaría de una agencia federal cuyo propósito principal es la vigilancia a gran escala, que de una agencia que afirma estar desempeñando tareas de seguridad. El FBI, una de las agencias de seguridad más poderosas del país, ha revelado la lista de cada DMV estatal de la que ha dependido para las búsquedas de reconocimiento facial.[160] También ha revelado los memorándums de acuerdo que sustentaban esos esfuerzos[161] y, durante años, ha publicado mensualmente estadísticas acerca del uso de su propio sistema de reconocimiento facial, el *Interstate Photo System* (Sistema Interestatal de Fotos, IPS, por sus siglas en inglés) del *Next Generation Identification* (Identificación de Próxima Generación, NGI, por sus siglas en inglés).[162] De manera similar, la CBP ha revelado el lugar donde se han desplegado cada uno de sus sistemas fronterizos de reconocimiento facial, y publica regularmente el número de búsquedas de reconocimiento facial que ha realizado.[163]

ICE ha tapado su uso del reconocimiento facial en las fotos de las licencias estatales con un grado anormal de secretismo.

En cambio, aunque ICE reconoce que utiliza tecnología de reconocimiento facial de manera rutinaria, nunca ha revelado oficialmente cuán seguido lo hace o en cuáles estados, insistiendo que comentarios públicos acerca de su uso de la tecnología amenazarían "sensibilidades de seguridad" sin especificar."[164] Hasta la publicación de este informe, ICE continua sin revelar esos detalles básicos. Esto no es para decir que el FBI o la CBP sean lo suficientemente transparentes, sino solamente para señalar que las prácticas de ICE ni siquiera llegan al nivel de los bajos estándares establecidos por sus agencias homólogas.

2. ICE busca directamente en las bases de datos de los DMV de los estados.

Además de contactar a los funcionarios de los DMV directamente para pedir información, ICE también consulta de manera frecuente las bases de datos de los DMV estatales para los registros de las licencias de manejo. Para hacer eso, la agencia depende de la Red Internacional de Seguridad Pública y Justicia, servicio más comúnmente conocido como NLETS.[165] NLETS, descrita como una "supercarretera de compartición de información" y empleada por las agencias de seguridad, ha permitido desde hace más de 20 años que ICE consulte electrónicamente y obtenga automáticamente información de las licencias de manejo recolectada por los DMV estatales participantes.[166] Hasta noviembre de 2020, divisiones de ICE que representan todos los 50 estados y el Distrito de Columbia han obtenido códigos llamados *Originating Agency Identification* (Identificador de la Agencia de Origen, ORI, por sus siglas en inglés) que autorizan el acceso al sistema NLETS.[167]

Según un memorándum interno de ICE recientemente divulgado, NLETS permite a los agentes de ICE consultar electrónicamente las bases de datos de licencias de manejo para propósitos de control migratorio en 34 estados.[168] A lo largo de esas 34 demarcaciones, ICE puede

usar NLETS para consultar la información personal de hasta 146 millones de conductores.[169] Este número es aún más alto cuando se incluyen las demarcaciones que permiten las consultas de ICE para fines no relacionados al control migratorio. Por medio de NLETS, agentes de ICE pueden consultar electrónicamente las bases de datos estatales de licencias de manejo para fines no relacionados al control migratorio en 39 estados y el distrito federal.[170] A lo largo de esas 40 demarcaciones, ICE puede usar NLETS para consultar la información personal de hasta **194 millones** de conductores, incluyendo aproximadamente **3 de cada 4** adultos.[171]

Registros públicos obtenidos por el *Center on Privacy & Technology* a través de solicitudes realizadas bajo la Ley de Libertad de Información revelan que ICE presenta decenas de miles de consultas de licencias de manejo y matriculaciones de vehículos cada mes por medio de NLETS. Los registros indican que ICE presentó **3,185** consultas en NLETS para licencias de manejo o matriculaciones vehiculares a lo largo de un periodo de **41 días** solo en **Wisconsin**.[172] Otros registros muestran que ICE presentó **223,814** consultas en NLETS para licencias de manejo entre 2015 y 2020 en **Texas**.[173] A lo largo del mismo periodo de cinco años, ICE presentó **83,400** consultas en NLETS de licencias de manejo en **Iowa**.[174] La evidencia parece indicar que esas consultas podrían abarcar un número significativo de personas. En **Washington** en 2019, ICE presentó **67,822** consultas en NLETS para licencias de manejo y obtuvo registros para **33,731** conductores en Washington.[175] Es el equivalente de alrededor una persona por cada dos consultas.

Este panorama parcial de cómo ICE ha usado NLETS para penetrar en los registros estatales de conductores solo ha emergido por medio de un proceso de atar cabos con archivos judiciales públicos y correos obtenidos por el *Center on Privacy and Technology* a través de solicitudes realizadas bajo la Ley de Libertad de Información, así como de la consulta de recursos publicadas por organizaciones de defensa de los derechos de los inmigrantes como *NILC* y *Just Futures Law*.[176] Las agencias estatales y federales han publicado muy pocos detalles acerca de cómo ICE usa NLETS para acceder a la información de las licencias de manejo de los DMV, eso debido a una combinación de secretismo de ICE y un pobre mantenimiento de información y archivos por parte de las agencias estatales.

Ninguna agencia puede divulgar detalles acerca de las búsquedas de ICE para los datos de los conductores de Maryland. Ninguna agencia se atribuye la responsabilidad para rastrear esos datos.

A nivel estatal, funcionarios gubernamentales han ayudado a preservar el secretismo de los registros de acceso de NLETS por medio de, efectivamente, enterrar sus cabezas en la arena. En Maryland, por ejemplo, ninguna agencia ha podido divulgar detalles acerca de las consultas de ICE en NLETS de los datos de los conductores de Maryland porque ninguna agencia se atribuye la responsabilidad para rastrear tales datos.

Cuando la legislatura estatal de Maryland solicitó información acerca del uso de ICE de NLETS para acceder a los registros de los conductores, el *Maryland Department of Transportation* (Departamento de Transporte de Maryland, MDOT, por sus siglas en inglés) afirmó en una declaración escrita en enero de 2021 que "no controla o monitorea el acceso" de los usuarios de NLETS.[177] En lugar de eso, MDOT sugirió que otros poderes del gobierno tenían esa información. Afirmó que el acceso de las agencias de seguridad a NLETS está "certificado por la Policía Estatal de Maryland para las agencias estatales y locales y por el Buró Federal de Investigaciones para las agencias federales" y que las consultas en NLETS "ocurren [. . .] por medio del Departamento de Seguridad Pública y Servicios Correccionales)".

Sin embargo, el *Department of Public Safety and Correctional Services* (Departamento de Seguridad Pública y Servicios Correccionales, DPSCS, por sus siglas en inglés) negó eso, afirmando que no era "el custodio oficial de" los registros relacionados con las consultas de ICE en NLETS sobre la información de los conductores de Maryland. Cuando el *Center on Privacy & Technology* envió una solicitud al departamento para los registros de NLETS, el departamento reenvió la solicitud a la Policía Estatal de Maryland.[178] En respuesta, la Policía Estatal de Maryland solo volvió a señalar al DPSCS. Una semana después de la objeción del DPSCS, la Policía Estatal de Maryland insistió que "no mantiene nada relacionado con" las consultas en NLETS.[179] Afirmó que las consultas en NLETS están registradas "en la central estatal de mensajes albergada por el DPSCS", el cual "debería poder conseguir los registros de ingreso".

Este juego de acusaciones es común. En Iowa, empleados en el Departamento de Transporte dijeron que "nosotros sencillamente ponemos esta información a la disposición" de la policía estatal y "cómo se usen los campos es asunto de" ellos.[180] En Idaho, funcionarios del DMV dijeron que la policía estatal supervisa la información de licencias de manejo y matriculaciones que se ponen a disposición a través de NLETS y que el DMV "no estaba involucrado".[181] Sin embargo, pocos departamentos estatales de policía han mantenido registros detallados de las solicitudes de ICE para obtener información personal de los conductores en NLETS. Como la policía estatal en Maryland, el Buró de Investigaciones de Colorado dice que no registra el número de consultas que recibe de ICE u otras agencias para información sobre las licencias de manejo.[182]

"Nosotros sencillamente ponemos a disposición esta información… cómo se usen los campos es asunto de [la policía estatal]".

Por su parte, ICE reconoce que "generalmente" obtiene información sobre las licencias de los conductores de los DMV de los estados a través del servicio NLETS,[183] pero los detalles completos acerca del uso del DHS de NLETS para acceder a la información de los DMV históricamente ha sido un secreto hermético. En el 2020, el *Homeland Security Committee* (Comité de Seguridad Nacional) de la Cámara de Representantes de EE.UU. lanzó una investigación insólita de los altos mandos del DHS por supuestamente haber mentido al Congreso al respecto.[184]

3. ICE consigue registros de los DMV en posesión de agencias privadas de datos.

Los agentes de ICE también utilizan registros de licencias de manejo vendidos por los DMV a las agencias privadas de datos. ICE reconoce que los registros obtenidos de esas fuentes a menudo están "incompletos, incorrectos o caducos" pero afirma que, con "el empleo de tiempo y esfuerzo adicionales", los agentes podrían usarlos para descubrir información como la dirección personal de un conductor.[185]

Con frecuencia, los DMV de los estados venden información sobre las licencias de manejo a las agencias de datos y otras entidades privadas, a menudo recaudando millones de dólares al hacerlo.[186] En Washington, por ejemplo, el Departamento de Licencias ganó más de $26 millones en 2017 por medio de la venta de registros de licencias de manejo y vehículos a múltiples agencias de datos, incluyendo LexisNexis.[187] Aunque LexisNexis es un conocido proveedor de investigaciones legales, también forma parte de una vasta empresa de servicios de información que junta enormes cantidades de datos y vende el acceso a éstos a las agencias gubernamentales.[188] Una de sus filiales, LexisNexis Risk Solutions, percibe más del 10% de sus ingresos anuales de la venta de servicios de "datos y analítica avanzada" a entidades gubernamentales y del sector salud.[189]

Desde marzo de 2021, ICE ha pagado $3.9 millones a LexisNexis Risk Solutions para tener acceso a información de las licencias de manejo y otros registros para ayudar en la "exploración profunda de personas de interés y vehículos".[190] Los términos del contrato de ICE con LexisNexis permanecen confidenciales, aunque LexisNexis ha reconocido en sus acuerdos de compra con los DMV que vende sus registros de licencias de manejo y matriculaciones de vehículos a clientes de seguridad nacional y otras agencias de seguridad.[191] Hasta la publicación de este informe, más de 11,000 agentes de ICE podrían realizar investigaciones por medio de consultas al servicio LexisNexis Risk Solutions.[192]

La evidencia indica que ICE ha comprado su acceso a la información de las licencias de manejo de los DMV a través de LexisNexis Risk Solutions. Los registros muestran que LexisNexis ha comprado información de las licencias de manejo directamente de los DMV en **12 estados** y el distrito federal: Arizona,[193] California,[194] el Distrito de Columbia,[195] Florida,[196] Illinois,[197] Minnesota,[198] Nebraska,[199] Nevada,[200] Carolina del Norte,[201] Oregón,[202] Carolina del Sur,[203] Tennessee[204] y Wisconsin.[205] En total, esto indica que ICE podría tener acceso a información de licencias de manejo compradas por LexisNexis pertenecientes a **88 millones** de conductores, incluyendo **1 de cada 3** adultos.[206]

ICE y LexisNexis han intentado mantener a oscuras al público acerca de los términos de su relación. Por ejemplo, ICE retuvo un resumen de su contrato de marzo de 2021 con LexisNexis Risk Solutions, afirmando que era "sensible el control de seguridad y no para la divulgación pública".[207] LexisNexis Risk Solutions ha sido más comunicativo acerca de sus acuerdos con el FBI, al emitir un boletín de prensa que anunciaba el contrato que otorgaba al FBI el acceso a su servicio *Accurint Virtual Crime Center* (Centro Virtual Contra el Crimen Accurint).[208] El FBI mismo reveló públicamente que usa LexisNexis Risk Services para tener acceso a información de domicilios, entre otros datos también.[209] Hasta la publicación de este informe, sin embargo, ICE y LexisNexis nunca han revelado esos detalles básicos de los servicios prestados bajo su contrato.

B. LAS LEYES FEDERALES Y ESTATALES HAN RESULTADO SER INSUFICIENTES CONTRA LAS BÚSQUEDAS—Y EVASIÓN—DE ICE.

Los DMV de los estados frecuentemente prometen fuertes protecciones estatales y federales a la privacidad personal de los conductores,[210] pero este informe ilustra que ICE ha podido obtener acceso de gran alcance a la información de los registros de los conductores a pesar de las protecciones legales. Eso se debe a que ICE aprovecha las debilidades en las leyes de privacidad federales y estatales, que a menudo siguen permitiendo a la agencia obtener información de los conductores a través de uno o más de sus tres principales canales de acceso.

1. La DPPA federal de 1994 no anticipó el uso de los datos de los conductores por las agencias federales de control migratorio.

La DPPA, una ley federal que reglamenta la compartición de la información de los registros de los conductores por parte de los DMV estatales, fue aprobada por el Congreso en 1994. Según el entonces senador Joe Biden, uno de los principales proponentes de DPPA en ese momento, la ley debía frustrar a los acosadores y hostigadores por medio de la protección de la "privacidad [de] direcciones y números de teléfono" proporcionados al DMV.[211] Pero ni el senador ni otros miembros del Congreso consideraron si la ley debiese proteger a los estadounidenses de las invasiones a la privacidad realizadas por las agencias federales de control migratorio. En esa época, los operativos de control migratorio eran comparativamente raros y el Congreso probablemente no anticipó los problemas que podrían surgir si eso cambiaba.[212] La DPPA expresamente permite a los DMV estatales compartir información con las agencias gubernamentales, así como con las agencias privadas de datos que la hacen disponible a las agencias gubernamentales.[213]

ICE ha operado dentro de esa laguna en la ley federal para poder acceder a la información de las licencias de manejo de los estadounidenses. Sin significativas protecciones federales a la privacidad que regulen cómo los DMV comparten los datos de los conductores con agencias gubernamentales y empresas privadas, ICE ha podido buscar información de las licencias de manejo de manera persistente, aún en estados que han permitido y animado a los inmigrantes a solicitar licencias de manejo.

2. La mayoría de las leyes estatales que protegen los datos de los conductores han resultado ser insuficientes. ICE ha evadido varias de las pocas leyes que ofrecen protecciones significativas.

En la ausencia de fuertes normas federales acerca del acceso de ICE a los datos de los conductores, muchos legisladores estatales y locales han emitido ordenes ejecutivas, políticas de agencia, estatutos y ordenanzas para resistir la expansión de las capacidades de vigilancia de ICE. Pero ICE ha evadido incluso las políticas más fuertes que los estados han aprobado para salvaguardar la información de sus conductores.

Oregón tiene una de las leyes de privacidad del conductor más fuertes para proteger la información de éstos en contra el acceso de ICE. En 2017, con el impulso de la gobernadora Kate Brown, la legislatura aprobó una ley que prohíbe la divulgación de las direcciones y otros datos por parte de las agencias gubernamentales para fines de control migratorio.[214] Al principio, la ley parecía funcionar: después de su promulgación, las solicitudes de ICE por información sobre los conductores de Oregón se cayeron drásticamente. Registros del DMV de

La gobernadora Kate Brown anuncia la firma de una orden ejecutiva para proteger a los inmigrantes en el estado el día 2 de febrero del 2017. (Fotografía: Gordon Friedman/Oregon Live)

Oregón obtenidos por el *Center on Privacy & Technology* muestran que el número de solicitudes directas de ICE para información de las direcciones de los conductores bajó de 35 solicitudes en 2015 y 40 solicitudes en 2016 a tres solicitudes en 2018 y cero solicitudes en 2019.[215] El grifo de las solicitudes directas al DMV para información se había cerrado. Solo en agosto de 2019, después de esa precipitosa caída en las solicitudes directas de ICE, aprobó Oregón H.B. 2015, la *Equal Access to Roads Act* (Ley de Acceso Igualitario a las Calles) para ampliar la elegibilidad de las licencias de manejo a personas sin documentación.[216]

Solo seis meses después, el DMV de Oregón firmó acuerdos para vender sus registros de licencias de manejo a las agencias de datos Thomson Reuters y LexisNexis Risk Solutions, otorgando a las empresas el permiso de divulgarlos a las "agencia[s] de gobierno para usarlos en llevar a cabo [sus] actividades gubernamentales".[217] Si el DMV de Oregón se dio cuenta de eso, o no, y sin importar que los contratos eran anteriores a esa ley, el DMV parecía estar permitiendo que la información sobre los conductores inmigrantes terminara en manos de ICE, a pesar de las fuertes leyes estatales cuya intención era prevenir precisamente eso.

A lo largo del país, las comunidades de inmigrantes han presionado a los legisladores para aprobar leyes que impidan este tipo de

abusos, y gracias a su organización y campañas, múltiples estados han intentado promulgar leyes que impidan a ICE el acceso sin orden judicial a la información de los conductores. Después de que los residentes de Maryland descubrieran los múltiples caminos de ICE para obtener acceso a su información de licencias de manejo, el grupo de derechos de los inmigrantes CASA encabezó una campaña para aprobar Ley de Privacidad de los Conductores de Maryland que prohíbe cualquier acceso a la información de las licencias de manejo de Maryland para medidas de control migratorio.[218] La ley fue aprobada en abril de 2021, y aunque el gobernador la vetó un mes después, la Asamblea General de Maryland anuló el veto en diciembre y la ley entrará en vigor este año [2022].[219] Leyes similares han sido aprobadas en otros estados. Cuando los residentes de California descubrieron que la agencia estaba usando un sistema estatal para ver la información de las licencias de manejo, el estado aprobó la AB 1747, que prohíbe el acceso de ICE al sistema estatal para emprender medidas de control migratorio civil.[220] Después de que los residentes de Utah se enteraran que ICE usaba tecnología de reconocimiento facial para escanear las fotos de sus licencias, Utah aprobó la S.B. 34 que prohíbe el uso de la tecnología de reconocimiento facial en bases de datos gubernamentales para propósitos de control migratorio civil.[221]

Pero estas leyes a menudo no logran bloquear todos los tres canales arriba descritos de acceso de ICE a la información de los conductores; o se quedan cortas en otros aspectos. Tal y como dijo la asambleísta Lorena González, "cada vez que creamos una nueva ley en California, ICE encuentra una manera de esquivar[la]".[222]

a. Puntuación para la privacidad de los conductores

El *Center on Privacy & Technology* ha realizado un análisis de las leyes y políticas de privacidad de los conductores en cada uno de los 16 estados que ofrecen a los migrantes indocumentados la posibilidad de solicitar una licencia de manejo o su equivalente; junto con el distrito federal, que tiene la misma política. Evaluamos la fuerza de las normas de cada demarcación sobre el acceso de ICE a la información de los conductores a través de sus tres principales canales de acceso, asignando a cada demarcación una puntuación según los siguientes criterios. Una demarcación recibió:

- una puntuación de **verde** cuando prohíbe la divulgación de los datos de los conductores a ICE sin orden judicial, el acceso a los datos de los conductores por parte de ICE sin orden judicial, o cuando tales datos no están disponibles para el acceso o la divulgación dentro del estado;
- una puntuación de **amarillo** cuando prohíbe el acceso por parte de ICE, o la divulgación de los datos de los conductores a ICE para medidas de control migratorio civil; y
- una puntuación de **rojo** cuando ninguna protección parecía aplicarse al acceso por parte ICE, o la divulgación a ICE de los datos de los conductores para medidas de control migratorio civil.

También asignamos puntuaciones a las demarcaciones según los mismos criterios, basándonos en si adoptaron protecciones contra las búsquedas por parte de ICE de reconocimiento facial sin orden judicial.

La puntuación que se presenta en la **Figura 3** muestra la aparición de un patrón claro. Nuestra revisión encontró que entre las 17 demarcaciones, seis no tienen restricciones significativas a los canales de solicitudes directas,[223] siete no tienen restricciones significativas a los canales de bases de datos gubernamentales,[224] y siete no tienen límites significativos a los canales de agencias de datos.[225] Cinco estados no tienen restricciones significativas a las búsquedas de reconocimiento facial.[226] Cuando las restricciones estatales a ciertos canales para los datos de los conductores sí existen, pueden lograr poco si las leyes permiten que los agentes de ICE tengan acceso a esa información por medio de otros canales.

Las leyes estatales para proteger la privacidad de los conductores a menudo no logran proteger contra todos los tres canales de acceso de ICE.

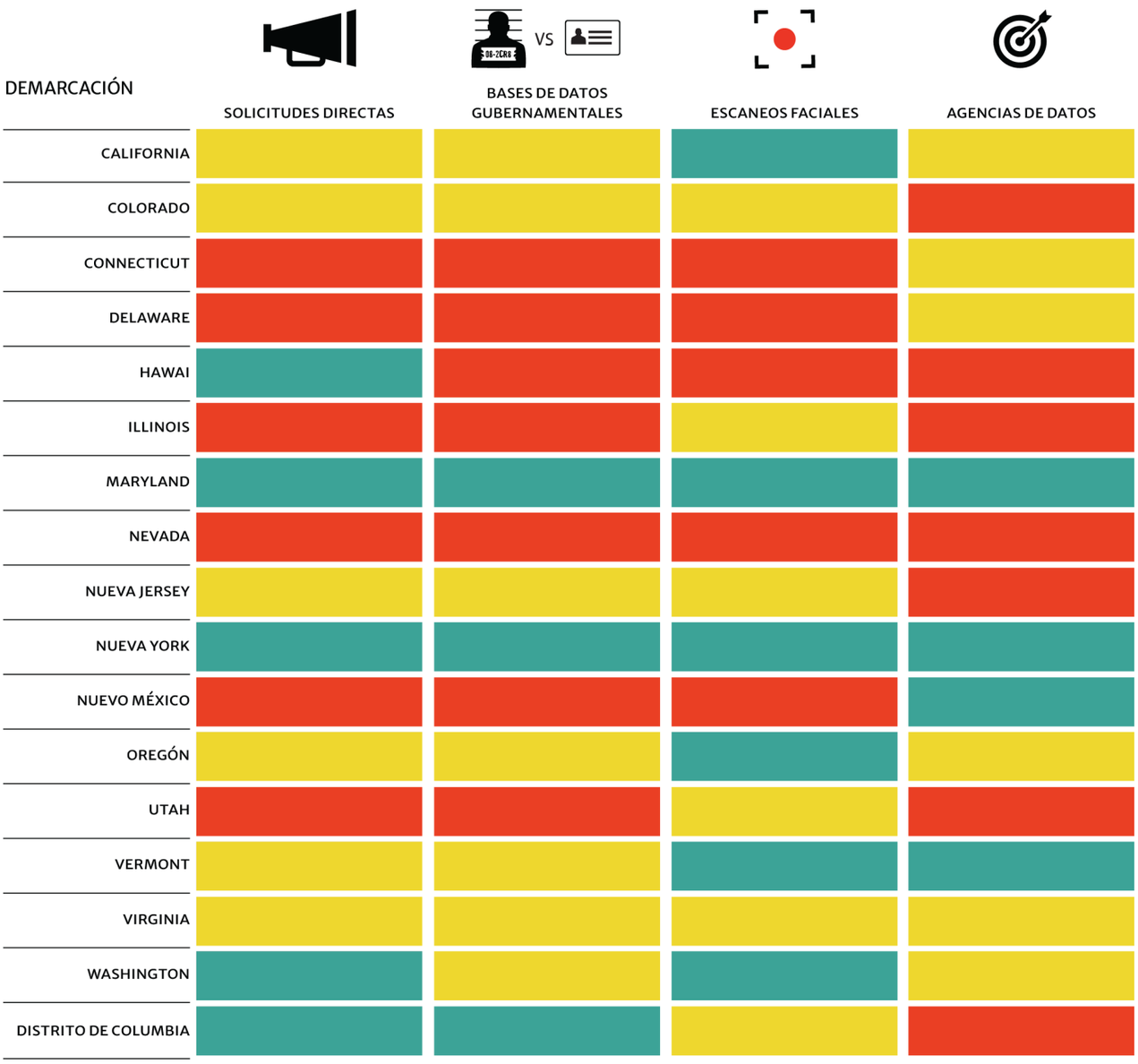
Varios estados han adoptado protecciones débiles que no requieren que ICE tenga una orden judicial para solicitar información personal de los conductores si la solicitud se basa en una investigación criminal. Nuestra revisión encontró que entre las diecisiete demarcaciones que otorgan elegibilidad a las personas indocumentadas para conseguir licencias de manejo, seis estados tienen restricciones débiles a los canales de solicitudes directas;[227] siete estados tienen restricciones débiles a los canales de bases de datos gubernamentales;[228] y seis estados tienen límites débiles a los canales de agencias de datos.[229] Cinco estados y el distrito federal tienen restricciones débiles a las búsquedas de reconocimiento facial.[230] Sin el requisito de una orden judicial, la condición de que exista una investigación criminal es poco más que una barrera de papel entre ICE y la información personal de un conductor.

Las leyes estatales de protección de la privacidad de los conductores típicamente contienen una o más debilidades significativas. Típicamente, las leyes débiles solo limitan la divulgación de la información de las licencias de manejo:

- por parte de la agencia de las licencias, sin una prohibición general a la divulgación de los datos subyacentes. Las protecciones de privacidad que solo aplican a la agencia de licencias permiten a las agencias federales de control migratorio valerse de otros empleados estatales para obtener acceso a los datos de los conductores y diseminarlos.
- a ciertos receptores, sin una prohibición general a las diseminaciones para propósitos de control migratorio. Las restricciones a la diseminación que solo aplican a agencias receptoras específicas permiten a las agencias federales de inmigración valerse de otros empleados federales para obtener acceso a los datos de los conductores y diseminarlos.
- cuando la información biográfica es solicitada directamente por un agente federal de inmigración, sin prohibiciones

Figura 3.

PUNTUACIÓN PARA LA PRIVACIDAD DE LOS CONDUCTORES



	ORDEN JUDICIAL REQUERIDA	INFORMACIÓN QUE NO SEA DE INMIGRACIÓN PERMITIDA	INFORMACIÓN DE INMIGRACIÓN PERMITIDA
SOLICITUDES DIRECTAS	Prohibida la diseminación a ICE sin una orden Judicial.	Se prohíbe la diseminación a ICE para propositos de controlar leyes migratorias civiles. (no se requiere una orden judicial para los no inmigrantes).	Se permite la diseminación a ICE para propósitos de controlar leyes migratorias civiles.
BASES DE DATOS GUBERNAMENTALES	El acceso por parte de ICE está prohibido son una orden judicial.	Se prohíbe el acceso de ICE para propósitos de controlar leyes migratorias civiles (no se requiere orden judicial para personas que no son inmigrantes).	Se permite el acceso por parte de ICE para propósitos de controlar leyes migratorias civiles.
ESCANEOS FACIALES	Se requiere orden judicial o la demarcación no utiliza tecnología de reconocimiento facial.	Se prohíbe el acceso directo, o la búsqueda por parte de un tercero en nombre del ICE, para fines de control de inmigración civil.	Se permite el acceso directo o las búsquedas en nombre de ICE para propósitos de controlar leyes migratorias civiles.

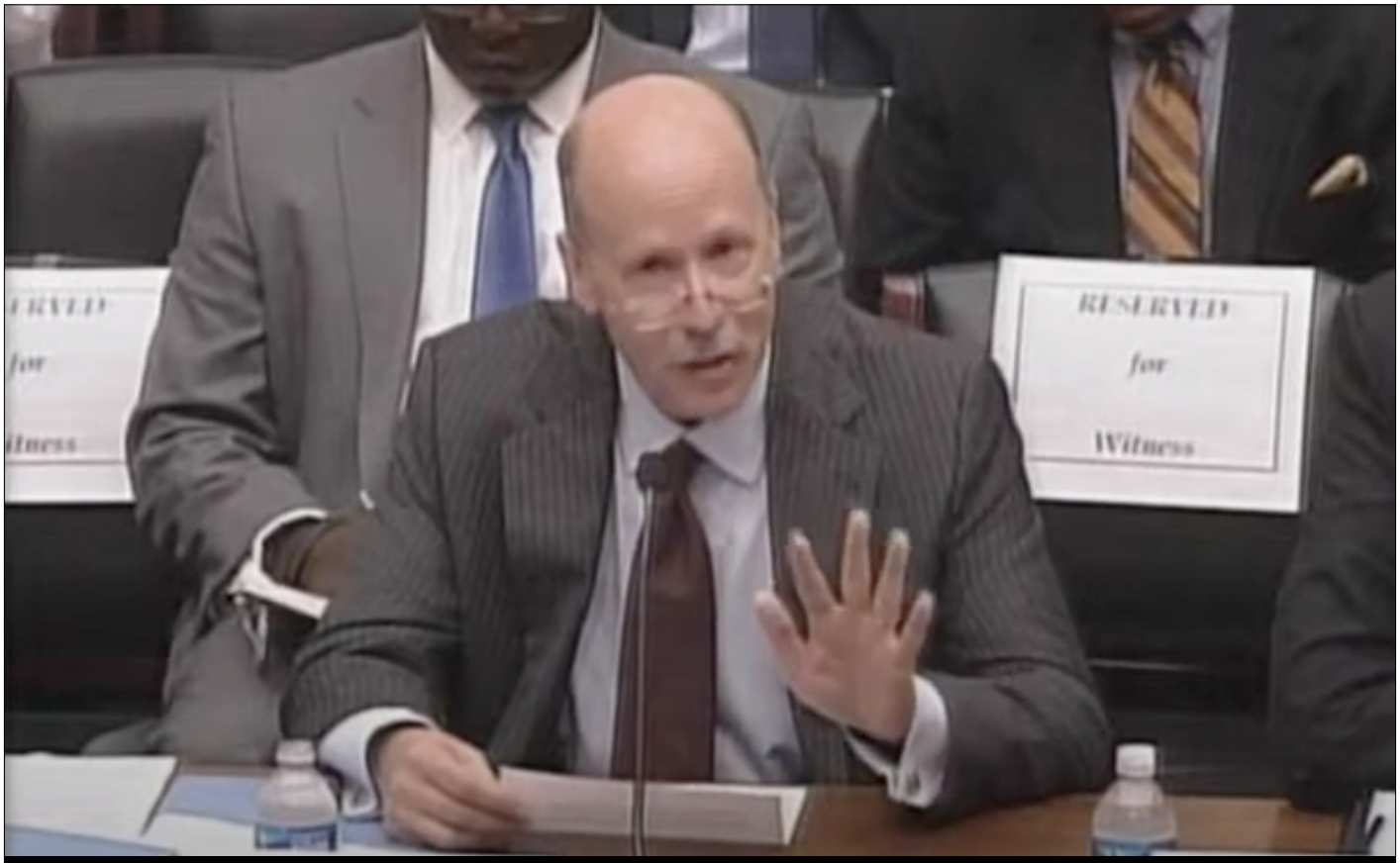
	SIN VENTAS A ICE	INFORMACIÓN QUE NO SEA DE INMIGRACIÓN PERMITIDA	INFORMACIÓN DE INMIGRACIÓN PERMITIDA
AGENCIAS DE DATOS	Está prohibida la reventa a ICE o la demarcación no vende a agencias de datoss.	Está prohibida la reventa a ICE para propósitos de controlar leyes migratorias civiles.	Se permite la reventa a ICE para propósitos de controlar leyes migratorias civiles.

al acceso indirecto o a la biométrica. Las protecciones de privacidad que solo aplican a las solicitudes directas de datos biográficos permiten a las agencias federales de inmigración obtener acceso a la información de licencias de manejo usando bases de datos electrónicas y búsquedas de reconocimiento facial.

- para propósitos de control migratorio civil, sin prohibiciones a la diseminación para investigar crímenes migratorios castigables. Las protecciones de privacidad que solo aplican a las solicitudes para propósitos de control migratorio civil permiten a las agencias federales de inmigración obtener acceso a la información de conductores para realizar actividades de control relacionadas con violaciones migratorias castigables, como los dos delitos federales al cruzar una frontera.
- a menos que sea solicitada por las agencias de seguridad. Las protecciones de privacidad que contienen excepciones demasiado amplias para las agencias de seguridad permiten a ICE valerse de agencias de seguridad locales, estatales y federales para obtener acceso a los datos de conductores y diseminarlos.

Con base en nuestra revisión, dos estados han promulgado protecciones de privacidad robustas para la información de las licencias de manejo. La Ley de Privacidad de los Conductores de Maryland bloquea la compartición de datos sin orden judicial con "cualquier agencia federal" que busca el acceso para "aplicar leyes migratorias federales".[231] La *Driver's License Access and Privacy Act "Green Light Law"* (Ley de Privacidad y Acceso a una Licencia Para Conducir, también conocida como la "Ley de Luz Verde") de Nueva York emparejó su ampliación de la elegibilidad para licencias de manejo con una prohibición categórica al DMV de divulgar o hacer accesible "de cualquier forma" los registros o información de las licencias de manejo a las agencias federales de control migratorio.[232] La aprobación de "Luz Verde" fue el resultado de una campaña plurianual realizada por una amplia coalición de múltiples sectores, encabezada por grupos de derechos de los migrantes y de trabajadores de todo el estado. Una consecuencia clave de la ley de Nueva York fue que la policía estatal empezó a cortar el acceso de ICE a información de las licencias de manejo a través NLETS. (La Policía Estatal de Nueva York prohibió a los códigos ORI de ICE, proporcionados por el FBI, de poder consultar la información de Nueva York de las licencias de manejo.[233]) Otra consecuencia clave fue que el DMV de Nueva York empezó a prohibir que los compradores de la información de las licencias de manejo del DMV la diseminara a ICE.[234] Con esas protecciones, el estado de Nueva York ha protegido de manera exitosa su información de las licencias de manejo de la vigilancia y extralimitación de ICE.

III. ICE APROVECHA LAS NECESIDADES BÁSICAS DE CALEFACCIÓN, ELECTRICIDAD Y AGUA DE LA GENTE AL RECOLECTAR EXPEDIENTES DE LOS SERVICIOS PÚBLICOS A TRAVÉS DE AGENCIAS DE DATOS POCO TRANSPARENTES Y SIN REGULACIÓN.



Stuart Pratt, entonces director ejecutivo de la Asociación de la Industria de Datos de Consumidores, testifica ante el subcomité de la Cámara de Representantes el 10 de septiembre de 2014 (Fotografía House Financial Services Committee)

En 2014, el *House Subcommittee on Financial Institutions and Consumer Credit* (Subcomité de la Casa de Representantes para Instituciones Financieras y Créditos al Consumo) llevó a cabo una audiencia para discutir un proyecto de ley cuya meta era extender el acceso a créditos para millones de estadounidenses. De acuerdo con el representante de Minnesota, Keith Ellison, en el país había al menos 50 millones de consumidores con historiales crediticios poco robustos para generar puntajes crediticios altos, mientras que otros 50 millones eran "invisibles para el crédito", lo que sugería que no tenían puntajes crediticios en absoluto.[235]

"La solución es simple", dijo Ellison al comité.[236] En vez de necesitar un crédito para construir, los consumidores pueden crear un expediente a través de algo que muchos ya pagan de manera cotidiana: sus recibos de servicios públicos. La *Credit Access and Inclusion Act* (Ley de inclusión y acceso al crédito) les daría luz verde a los

diferentes proveedores de gas, agua, electricidad y otros servicios para que notifiquen a los burós de crédito cada vez que un cliente paga—o no—un recibo mensual; y no solo cuando la cuenta sea enviada a cobranzas.[237]

La idea detrás de usar los pagos de servicios públicos para mostrar la capacidad crediticia no era totalmente nueva. Una importante agencia de información crediticia, Equifax, ya estaba recolectando los expedientes "completos" de pagos de servicios públicos de millones de clientes para emplearlos en informes crediticios especializados, los cuales se entregaban de manera específica a compañías de servicios públicos.[238] Pero la ley aún no era clara sobre si los datos completos de pagos de servicios podrían incluirse en los puntajes crediticios de los clientes; y Ellison quería autorizar la práctica. Él esperaba que la aprobación del Congreso fuera de gran utilidad para ayudar a que los estadounidenses con créditos bajos—o sin crédito alguno—se incorporaran al gran sistema financiero.[239]

Entre todos los testigos presentes en la audiencia, nadie habló tan vehementemente sobre el potencial del proyecto de ley para mejorar la vida de aquellos con menos privilegios como lo hizo Stuart Pratt. Pratt fue presidente y director ejecutivo de un grupo comercial llamado *Consumer Data Industry Association* (Asociación de la Industria de Datos de Consumidores, CDIA por sus siglas en inglés), cuyos miembros incluían a las tres grandes agencias de información crediticia del país: Equifax, Experian y TransUnion. "Al final", cuando habló de que los burós de crédito pueden incluir datos completos de pagos de servicios públicos en sus informes crediticios, Pratt insistió ante el comité que "los consumidores que son inmigrantes recién llegados, sin afiliaciones bancarias o sub-bancarizados, son los beneficiarios".[240]

"... los consumidores que son inmigrantes recién llegados, sin afiliaciones bancarias o sub-bancarizados, son los beneficiarios"

Solo un legislador expresó las inquietudes sobre si esta información valiosa podría terminar en las manos equivocadas. "Supongo que puedo preguntarle al panel," dijo el vicepresidente Sean Duffy, "¿qué medidas se están tomando para proteger millones de bits de información recolectada con respecto a los historiales crediticios e información personal de la gente?[241] Pratt, el representante de la industria, le aseguró que las compañías en CDIA contaban con equipos de seguridad y podrían monitorear si alguien obtenía acceso a los reportes crediticios de manera inesperada como, por ejemplo, alguien con una IP de Rusia.[242]

Pero Pratt olvidó mencionar que Equifax, uno de los miembros más grandes de esta asociación comercial, estaba creando compendios de información de los consumidores con lo recibido por las compañías de servicios públicos y entregándolos a una base de datos empleada por ICE.

Siete años después, en febrero de 2021, los representantes Raja Krishnamoorthi de Illinois y Jimmy Gómez de California exigieron respuestas por parte de Equifax y de la agencia de datos Thomson Reuters sobre estas prácticas, expresando su preocupación sobre que la compartición de datos de los clientes de servicios públicos a ICE representa "un abuso de la privacidad, mientras que el uso de esta

información por parte de ICE fue calificado como un "abuso de poder".[243]

A. ICE APROVECHA LAS NECESIDADES DE SERVICIOS COMO AGUA, ELECTRICIDAD, CALEFACCIÓN, TELÉFONO E INTERNET PARA DETECTAR BLANCOS DE DEPORTACIÓN.

El 2 de junio de 2020, un agente de ICE envió un correo electrónico a un funcionario del Departamento de Licencias de Georgia pidiendo ayuda. "¡Feliz martes!" escribió el agente. "Me encuentro atorado en uno de mis casos de inmigración."[244] El agente necesitaba ayuda para rastrear a una persona. Había obtenido los registros de servicios públicos de esta persona, los cuales revelaban que había "cambiado" de dirección "recientemente".[245] El agente llevó esa situación al Departamento de Licencias esperando que los registros de los conductores pudieran revelarle más información.

Tres meses antes, en los primeros días del confinamiento por COVID-19 en EE.UU., el jefe interino de ICE había anunciado que la agencia disminuiría temporalmente los arrestos, con la excepción de aquellos considerados como "misiones críticas" para "mantener la seguridad pública y nacional."[246]

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] named [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] show him recently departed from the [redacted] address in [redacted]

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

Un correo electrónico con fecha del 2 de junio de 2020 de un agente de deportaciones de ICE dirigido a un oficial del Departamento de Licencias de Georgia. (Fuente: Center on Privacy & Technology de los documentos de Freedom of Information)

Sin embargo, el agente que envió el correo electrónico al Departamento de Licencias de Georgia no estaba extrayendo expedientes para encontrar a alguien que encajaba con los nuevos criterios emitidos por ICE para el control migratorio. En cambio, el agente había intervenido una base de datos con millones de registros de clientes de servicios públicos como agua, electricidad, gas, teléfono, entre otros, con el fin de encontrar a alguien que simplemente había entrado al país con una visa y se había quedado más tiempo del permitido. Sin duda, se trataba de un caso de "estadía prolongada de una visita de placer."[247]

Desde hace varios años se ha sabido que ICE usaba bases de datos comerciales para obtener acceso a millones de nombres, direcciones y más información personal tomada de sus expedientes de contratos de servicios públicos.[248] Sin embargo, quedaron detalles sin saber, por ejemplo: ¿cómo es que datos de clientes de servicios públicos terminaron en bases de datos privadas al servicio de los agentes de inmigración? ¿exactamente cuáles fueron las compañías de servicios públicos que permitieron que ICE tuviera acceso a los datos de sus clientes?

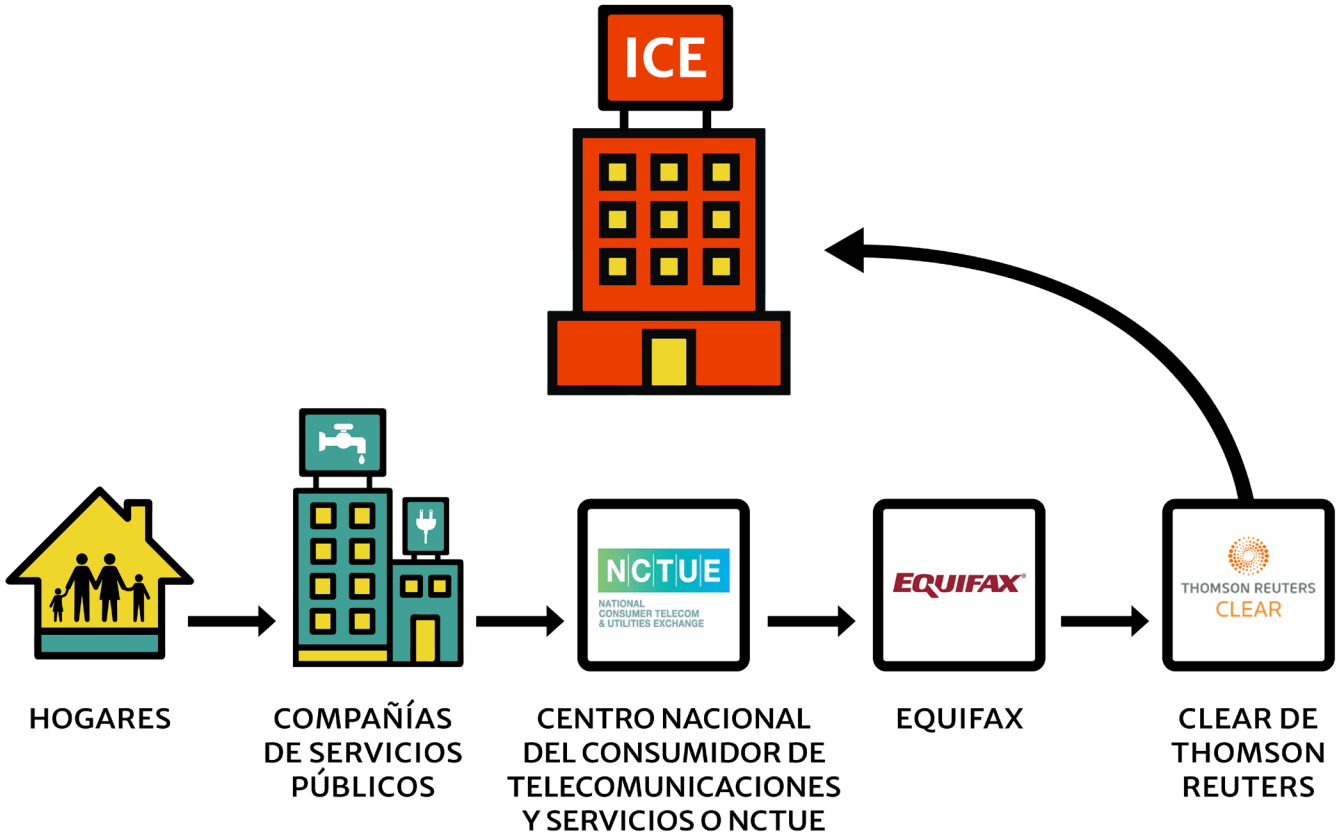
Al unir documentos públicos de marketing y de trámites ante el DOJ, el *Center on Privacy & Technology* pudo identificar la probable y añeja fuente de datos de servicios públicos de ICE: una pequeña agencia de informes crediticios conocida como el Centro Nacional del Consumidor de Telecomunicaciones y Servicios, (NCTUE por sus siglas en inglés). A través del acceso a datos de clientes provenientes de decenas de compañías de servicios públicos y de telecomunicación que eran miembros de la NCTUE, es probable que los agentes de ICE hayan revisado los expedientes de cerca de **218 millones** de clientes únicos, incluyendo **3 de cada 4** adultos en los Estados Unidos.[249]

Los investigadores de ICE desarrollaron la habilidad de examinar los registros de servicios de gas, agua, electricidad, teléfono, internet y otros servicios cuando, en 2010, la agencia firmó un contrato con Thomson Reuters para obtener acceso a una base de datos conocida como CLEAR.[250] CLEAR, diseñada para ser una "ventanilla única" para los investigadores que buscaban recopilar información sobre sus blancos, elimina las brechas en las cadenas de datos que los individuos van dejando día a día.[251] La base de datos extrae nombres y números de seguridad social de los informes crediticios; encuentra correspondencias entre las matrículas vehiculares de los registros del DMV y las fotografías tomadas en rutas de peaje y estacionamientos; y—para generar la información más actualizada sobre los domicilios de las personas—recopila direcciones enlistadas en sus cuentas de gas, agua, electricidad y otros servicios.

"En el caso de personas que no son fáciles de rastrear a través de medios convencionales . . . los registros de conexión de servicios públicos pueden ofrecer los únicos datos telefónicos y domiciliarios actuales disponibles."

En una carta de mercadotecnia y promoción enviada a posibles suscriptores, Thomson Reuters hace un especial énfasis en que los registros de los servicios públicos son extraordinariamente valiosos al momento de ofrecer una visión esclarecedora sobre las poblaciones que son

Figura 4. Posible trayecto de los datos de clientes de servicios públicos con destino a ICE



difíciles de rastrear a través de otros medios. "En el caso de personas que no son fáciles de rastrear a través de medios convencionales" (como informes crediticios), la carta dice que "los datos de localización obtenidos a partir de registros de conexión a los servicios públicos podrían ofrecer los únicos datos telefónicos y domiciliarios actuales disponibles."[252] Thomson Reuters se ha encargado de asegurar que su recopilación de registros de servicios públicos es extensa y actualizada; mientras que en la carta enviada a suscriptores potenciales se jacta de que "CLEAR ofrece los datos más detallados para la localización de clientes de servicios públicos en el mercado."[253]

En la carta, Thomson Reuters también revela que Equifax es el proveedor de los conjuntos de datos de servicios públicos de CLEAR.[254]

Equifax alberga una base de datos que contiene millones de expedientes de pagos de los clientes de servicios públicos que, a su vez, son suministrados por NCTUE. Este acuerdo empezó en 1993, cuando un grupo de ocho operadores de telecomunicaciones acudió al DOJ a revisar su plan para construir un "centro de intercambio de información crediticia,"[255] una base de datos central donde las compañías podrían compartir entre ellas datos de las cuentas y expedientes de pagos de sus clientes, (de no haberse hecho esa revisión, no se tendría certeza alguna sobre los resultados de un posible escrutinio antimonopolio)[256] El grupo seleccionó Equifax para construir y gestionar la base de datos[257] y, a cambio, Equifax negoció el derecho exclusivo para compilar y organizar los datos y entregárselos a compradores posteriores.[258]

La base de datos de clientes tiene un doble propósito. Cuando las compañías de telecomunicaciones inicialmente propusieron el centro de intercambio de datos al DOJ, argumentaron que su "propósito principal" era "proporcionar a los operadores advertencias por adelantado sobre clientes que representan un riesgo crediticio."[259] Por ejemplo, a un cliente potencial con un historial de adeudos se le podría pedir que hiciera un depósito mayor. Sin embargo, los operadores también planearon que esta reserva de registros fungiera como una herramienta de "localización de deudores"; es decir, una forma de rastrear clientes con adeudos.[260] Los clientes podían dar de baja los servicios o mudarse a otro lado, pero cada vez que se inscribieran con algún otro proveedor miembro de este grupo, el centro de intercambio de datos actualizaría su información con las direcciones nuevas e información de contacto proporcionada en sus solicitudes.

Para facilitar aún más el rastreo de clientes antiguos en sus nuevas direcciones, el grupo inicial de operadores de telecomunicaciones decidió invitar a proveedores de gas, agua y energía eléctrica para que aportaran sus propios registros de clientes. De acuerdo con otros trámites realizados por los operadores de telecomunicaciones ante el DOJ en 2002, "los servicios ofrecidos por estas compañías están vinculados a una localización física," lo que significa que "suelen tener información domiciliaria precisa."[261] Con la adición de 37 compañías de servicios públicos aportando información sobre sus clientes, el grupo se dio a conocer bajo el nombre de NCTUE.[262] La base de datos de NCTUE no solo se volvió útil para la evaluación crediticia, sino que se volvió una de las fuentes de información más confiables para saber los domicilios de la gente.

Cuando los agentes de ICE usaron CLEAR para obtener acceso a millones de nombres y direcciones a partir de los registros de servicios públicos, es posible que hayan visto datos que las compañías miembros de NCTUE entregaron a Equifax. Era poco probable que una recopilación tan exhaustiva de datos de los registros de las compañías de servicios públicos proviniera de cualquier otra fuente; pues se ha reportado que la base de datos de NCTUE es "por mucho, la base de datos más grande de información de registros de pagos de servicios públicos, televisión de paga y telecomunicaciones" del país.[263] Equifax también pregonó activamente la efectividad de la base de datos de NCTUE para capturar "aquel segmento esquivo del mercado; es decir, los expedientes con pocos o nulos resultados[264] que posiblemente no se encuentren en los datos de los encabezados de informes crediticios que Thomson Reuters recibe de otras agencias crediticias, como Experian y Transunion.

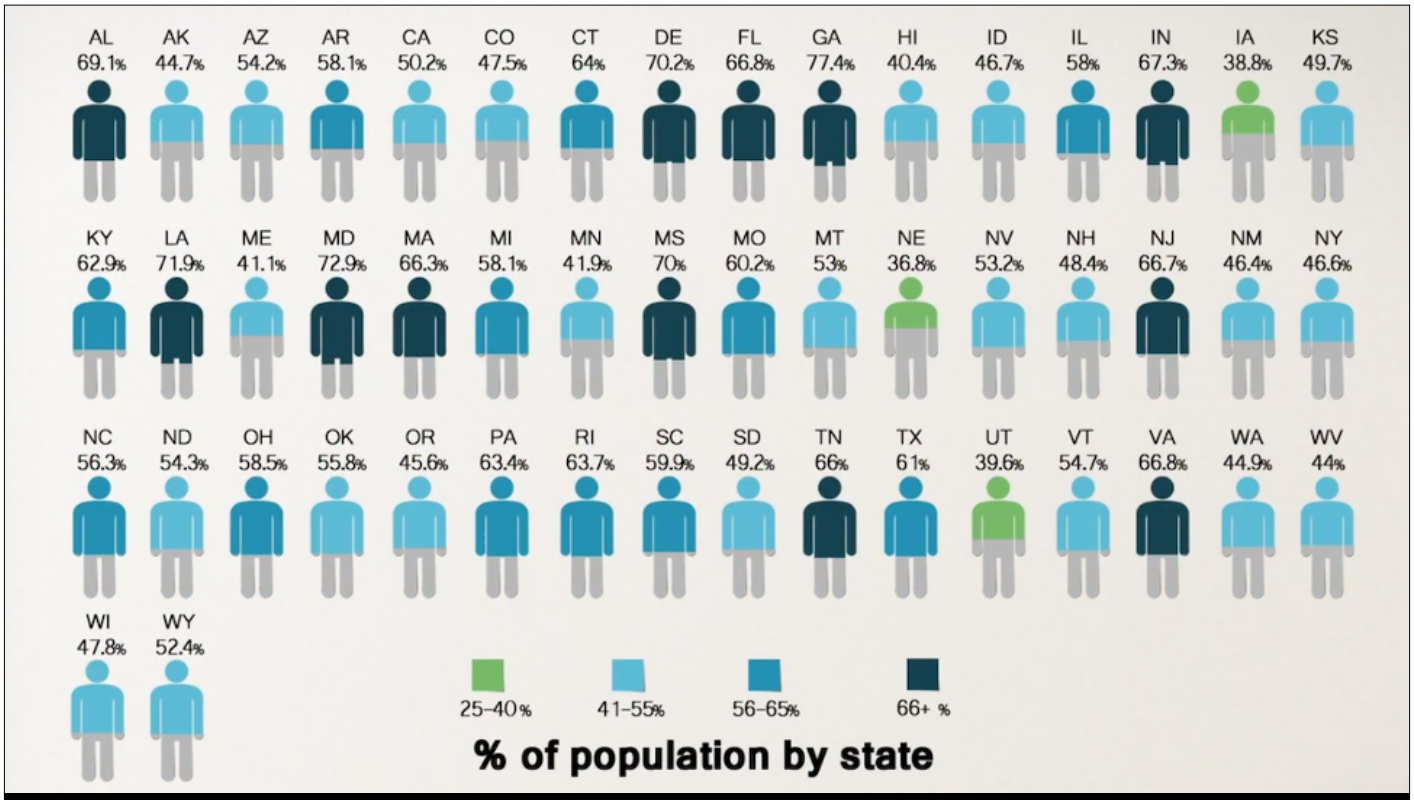
Aunque ninguna de las entidades involucradas en el suministro de registros de contratos de servicios públicos a Thomson Reuters ha confirmado el origen exacto de los mismos, los conjuntos de datos que Equifax gestiona para NCTUE, así como los registros de datos entregados a CLEAR son casi idénticos en cifras: CLEAR argumenta que cuenta con 400 millones de nombres y direcciones obtenidas de más de 80 proveedores de servicios;[265] mientras que Equifax ha revelado que la base de datos de NCTUE contiene más de 400 millones de registros de más 85 compañías.[266]

Equifax y NCTUE han mantenido en secreto la lista completa de compañías de servicios públicos cuyos registros han terminado en la base de datos de NCTUE y, por lo tanto, posiblemente en las manos de ICE. Sin embargo, la evidencia indica que la lista incluye a gigantes como

Verizon[267] y AT&T[268], así como a compañías regionales como Baltimore Gas & Electric[269] y Piedmont Natural Gas.[270] La evidencia también sugiere que incluso algunos proveedores de estos servicios gestionados por el gobierno, como Nevada Energy[271] y el Miami-Dade County Water and Sewer Department (Departamento de Aguas y Drenajes del Condado Miami-Dade)[272] han participado en el intercambio de datos. Otros proveedores de servicios que han sido parte de NCTUE se encuentran enlistados en el **Apéndice**.

El amplio acceso de ICE a los datos de servicios públicos afecta a millones de clientes de decenas de proveedores de servicios de todo Estados Unidos. La base de datos de servicios públicos CLEAR toma su información de proveedores regionales y nacionales de servicios telefónicos, de cable, satelitales, gas, electricidad y agua de todo el país, "enfocándose especialmente en las 50 compañías líderes."[273] Los conjuntos de datos encapsulan clientes de los 50 estados y el distrito federal, así como de Puerto Rico, Guam y las Islas Vírgenes, y se actualiza diariamente.[274]

A pesar de proporcionar información personal de millones de clientes de servicios públicos a una base de datos utilizada para el control migratorio, Equifax mantiene la narrativa de que sirve a los clientes menos privilegiados. En un video promocional publicado por Equifax, un director de Verizon proclama que el intercambio de datos de NCTUE "empodera de manera extraordinaria"[275] a clientes "multiculturales carentes de servicios y sub-bancarizados."[276] Un ejecutivo de Equifax también afirmó que el intercambio de información "presenta una oportunidad tremenda para individuos sub-bancarizados o invisibles al crédito."[277]



Cobertura de la NCTUE por estado (Fuente: Equifax)

Un empleado de Verizon declara que la NCTUE "empodera de manera extraordinaria" a clientes "multiculturales carentes de servicios y sub-bancarizados."

El acuerdo de ICE con Thomson Reuters para obtener acceso a la base de datos CLEAR terminó en febrero de 2021. Ese mismo mes, sin embargo, ICE pareció reemplazar su suscripción a CLEAR al adjudicar un contrato de $16.8 millones a Lexis Nexis Special Services, posiblemente para el acceso a una base de datos similar llamada Accurint.[278] Aunque no se sabe si este contrato le ofrece a ICE el acceso a los registros de servicios públicos de la base de datos de NCTUE, Lexis Nexis ha publicitado que sus conjuntos de datos incluyen registros de servicios públicos de 210 millones de consumidores—casi la misma cantidad que la base de datos de NCTUE dice tener—obtenidos de fuentes no especificadas.[279]

RECUADRO 2. DIVULGACIÓN TEMPRANA DE NUESTROS HALLAZGOS SOBRE NCTUE

El *Center on Privacy & Technology* normalmente publica los hallazgos de sus investigaciones en conjunto con los informes de investigación. Cuando develamos el trayecto de datos entre NCTUE y ICE, decidimos que la información era demasiado importante como para esperar la publicación de nuestro informe. Proporcionamos los documentos a Drew Harwell del Washington Post, que los publicó a manera de denuncia en una portada de febrero de 2021.[280] Ninguna de las compañías involucradas negó que los datos de los clientes de las compañías miembro de la NCTUE fueran entregados a ICE.

En octubre de 2021, la NCTUE instruyó a Equifax para que terminara con la venta de nombres, direcciones y otros datos biográficos tomados de los registros de clientes.[281] Este fue el resultado de las acciones del senador Ron Wyden de Oregón, quien, a raíz de la publicación de nuestros hallazgos en el Washington Post en febrero y de la defensa constante emprendida por *Just Futures Law* y *Mijente* en los meses consecuentes, presionó para que la venta de esta información cesara.[282]

De acuerdo con un comunicado emitido por Thomson Reuters a los clientes de sus bases de datos, incluyendo las de CLEAR, los datos de los encabezados de informes crediticios de servicios públicos ya no son proporcionados a agencias de seguridad, ni a entidades particulares, como investigadores privados.[283]

Sin embargo, a pesar de que la NCTUE aceptó terminar con la venta de datos de clientes de servicios públicos, es tan solo una de las numerosas fuentes posibles para obtener este tipo de información. Sin regulaciones contundentes para limitar la diseminación de datos de los servicios públicos, es tan solo cuestión de tiempo que las agencias de datos descubran nuevas vías para la acumulación de los mismos conjuntos de datos. Aunque ICE ha terminado su contrato de Thomson Reuters, su nuevo acuerdo con LexisNexis revela que muchas compañías diferentes pueden ofrecer servicios muy similares. Cuando ICE termina una relación con una agencia de datos, simplemente puede firmar nuevos contratos con otra.

B. LAS LEYES FEDERALES Y ESTATALES OFRECEN POCA PROTECCIÓN EN CONTRA DE BÚSQUEDAS DE DATOS DE SERVICIOS PÚBLICOS REALIZADAS POR ICE SIN UNA ORDEN JUDICIAL.

Durante una ceremonia de firma de leyes a finales de 2020, el gobernador Gavin Newsom orgullosamente declaró que los inmigrantes y refugiados hacían de California "un lugar mejor y más dinámico."[284] Entre las nuevas leyes aprobadas aquel día con la firma del gobernador, figuraba la ley del asambleísta de California, Todd Gloria, CA AB 2788, que prometía la protección de los datos—incluyendo información del uso de servicios—de los clientes de servicios públicos en contra de su exposición ante agencias federales de control migratorio.

La ley de Gloria respondía a un problema urgente. Los informes de transparencia de las compañías estatales de servicios públicos mostraban que las autoridades federales de control migratorio pedían de manera rutinaria información de los clientes de servicios públicos de California sin antes presentar una orden judicial.[285] Bajo la nueva ley, si ICE quisiera solicitar directamente información de los clientes de servicios públicos de California, necesitaría recurrir a un juez y obtener una orden judicial. Si ICE quisiera obtener acceso a la información de los clientes de servicios públicos de California a través de una agencia de datos, la ley detendría a la agencia en seco.[286]

La aprobación de la ley fue una "tremenda victoria," afirmó Gloria, "para la privacidad de todos los californianos, así como para salvaguardar a nuestras comunidades de inmigrantes y refugiados."[287]

El gobernador de California, Gavin Newsom, da el visto bueno al asambleísta Todd Gloria en una ceremonia de firma de un proyecto de ley en 2019. (Foto: AP Photo/Rich Pedroncelli)

Sin embargo, nuestros hallazgos con respecto a Equifax y NCTUE sugieren que la ley de California contaba con una gran puerta trasera. Aunque la legislación prohibía la venta de los datos de clientes, no protegía en contra de la simple diseminación de éstos. Como resultado, el límite puesto por California para la venta de datos de consumidores no serviría en contra de una compañía de servicios que compartiera la información de manera gratuita; por ejemplo, para llevar a cabo una verificación crediticia. Cuando las compañías de servicios públicos de California divulgan información de clientes a NCTUE para una evaluación crediticia y otros fines, es posible que éstas no se percaten de que NCTUE puede revender la información de sus clientes a terceros una vez que la evaluación haya terminado. De hecho, a pesar de la aprobación de esta ley, es posible que los datos de **1 en cada 2** californianos aún estén al alcance de ICE a través de Equifax y NCTUE.[288]

California no es el único estado cuyas leyes han permitido que los datos de los consumidores de servicios públicos lleguen a ICE. Los enormes vacíos en las leyes estatales de privacidad de servicios públicos, aunados a los propios vacíos en las leyes federales de privacidad han impedido que millones de estadounidenses tengan un nivel significativo de protección de su privacidad al momento de contratar servicios de agua o gas.

Dentro de este vacío en las regulaciones, las compañías han construido un mercado lucrativo para vender a ICE y a otras entidades

información de los clientes de servicios públicos, incluso cuando los legisladores han tratado de implementar fuertes regulaciones.

1. Las leyes federales de privacidad ofrecen una protección mínima o nula.

A finales de los años 1990, cuando recién empezaba a surgir un mercado para la venta de información personal y domiciliaria de los clientes de servicios públicos, los reguladores federales se resistían a reglamentar la compra y venta de esos datos. En 1997, la *Federal Trade Commission,* (Comisión Federal de Comercio, FTC por sus siglas en inglés) le dijo al Congreso que "los avances en la tecnología de computación" hacían posible que se buscara la información personal de los estadounidenses "a partir de fuentes como registros de servicios públicos, telefónicos o de viajes aéreos" de "una manera más sencilla y económica que antes".[289] Aunque resultaba muy fácil obtener esa información, muchos estadounidenses manifestaron vehementemente preferir un nivel alto de privacidad,[290] por lo que cumplir con esas preferencias parecía ser una de las prioridades de las compañías de servicios públicos.

La FTC simplemente recomendó que el Congreso le diera al *Individual Reference Services Group* (Grupo de Servicios de Referencias Individuales, IRSG por sus siglas en inglés), una asociación que representaba a las grandes agencias de datos como Equifax y LexisNexis, "una oportunidad" para autorregularse. El ISRG aceptó y prometió al FTC que sus compañías no venderían información de clientes de compañías telefónicas en los casos en los que los consumidores hubieran elegido permanecer fuera de la lista o de cualquier "información similar."[291]

No pasó mucho tiempo antes de que la autorregulación de la industria colapsara. En el año 2000, después de que la FTC adoptara medidas para proteger la privacidad de la información personal de los consumidores de los bancos y otras instituciones financieras, la ISRG se disolvió.[292] Ninguna entidad reguladora federal tomó su lugar para salvaguardar los datos de los clientes proporcionados a las compañías de servicios públicos. Asimismo, en los siguientes 20 años, el Congreso no aprobó una sola ley que protegiera la privacidad de los clientes de estos servicios.

Al no contar con legislaciones relevantes ni la autorregulación de la industria, la privacidad de los clientes de servicios públicos quedó a la deriva. Los reguladores federales ya habían interpretado las leyes existentes de privacidad como la *Fair Credit Reporting Act* (Ley de Informes Crediticios Justos) y la *Gramm-Leach-Bliley Act* como medios para proteger la información de los consumidores solo en ciertos casos, como cuando fuera utilizada por instituciones financieras (como bancos), o cuando se tratara de material relevante para informes crediticios de los consumidores.[293] Otras leyes de privacidad como la *Cable Privacy Act* (Ley de Privacidad de Servicio de Cable) o la *Electronic Communications Privacy Act* (Ley de Privacidad de Comunicaciones Electrónicas) no ofrecen interpretaciones que ofrezcan una protección importante en contra de la venta de información personal y domiciliaria de los consumidores. Por su parte, la protección de la privacidad de consumidores de servicios de gas, electricidad y agua quedó en manos de reguladores estatales.

2. Las leyes estatales de privacidad no protegen la información de las personas de manera adecuada.

La mayoría de los estados no cuentan con protecciones importantes de privacidad para los datos obtenidos de los clientes de compañías

de gas, agua, teléfono y cable. En el caso de las escasas leyes y políticas que sí existen, una revisión más detallada revela que la gran mayoría hace muy poco para proteger los datos domiciliarios de sus clientes en contra de las dos vías de divulgación a través de las que estos datos viajan: (1) divulgación a agencias de seguridad por parte de la compañía y (2) divulgación a terceros comerciales, que es el camino por el que los paquetes de información viajan a ICE, tal y como lo evidenció el acceso de ICE a los datos de Thomson Reuters y, probablemente, a LexisNexis hoy en día.

a. Puntuación de los niveles de privacidad estatales de las compañías de servicios públicos.

El *Center on Privacy & Technology* calificó las protecciones de 51 demarcaciones para datos domiciliarios de los clientes para los cinco servicios públicos en los dos caminos de divulgación que recorren hacia ICE. En el caso de la divulgación a las agencias de seguridad, cada jurisdicción recibió:

- una puntuación de **verde** cuando se requiere un mandato judicial que ordene la divulgación de la dirección de un cliente;
- una puntuación de **amarillo** cuando se requiere un citatorio judicial o más para obtener la dirección de un cliente, o cuando la regulación (pero no una ley) de la agencia prohíbe la divulgación de la dirección de un cliente; y
- un puntaje en **rojo** cuando se requiere un citatorio administrativo o menos para ordenar la divulgación del domicilio de un cliente

Para el caso de la divulgación de terceros comerciales, cada jurisdicción recibió:

- una puntuación de **verde** cuando prohibía que se difundiera el domicilio de un cliente a terceros o solamente permitía su diseminación para propósitos específicos de negocios y ordenaban su pronta eliminación
- una puntuación de **amarillo** cuando prohibía la diseminación del domicilio de un cliente a terceros o solamente permitía su diseminación para propósitos específicos de negocios sin ordenar su pronta eliminación; y
- una puntuación de **rojo** cuando estas protecciones no parecían aplicarse, o cuando la jurisdicción promovía la amplia diseminación del domicilio de una persona a terceros tras un previo aviso al cliente y con su respectivo consentimiento. Se incluyen fines de verificación crediticia.

Las leyes estatales diseñadas para establecer medidas para proteger la privacidad de la información personal de los clientes de compañías de servicios públicos suelen tener una o dos debilidades importantes. Las leyes estatales débiles normalmente solo limitan la divulgación de la información de los clientes:

- cuando la divulgación es ordenada por agencias de seguridad, pero no hay prohibición alguna sobre la divulgación voluntaria a otras entidades. Las protecciones de privacidad que solo aplican a los requerimientos obligatorios por parte de las agencias de seguridad permiten que las compañías de servicios divulguen de forma voluntaria información del cliente a agencias de datos o a terceros para cualquier otro propósito.

Figura 5. Puntuación de protecciones estatales de datos de servicios públicos frente al acceso de agencias de seguridad.

PUNTUACIÓN DE LOS NIVELES DE PRIVACIDAD ESTATALES DE LAS COMPAÑÍAS DE SERVICIOS PÚBLICOS

Figura 6. Puntuación de protecciones estatales de datos de servicios públicos frente al acceso de terceros comerciales.

PUNTUACIÓN DE LOS NIVELES DE PRIVACIDAD ESTATALES DE LAS COMPAÑÍAS DE SERVICIOS PÚBLICOS

- cuando la información se vende, pero no se cuenta con prohibiciones para la divulgación no remunerada. Las protecciones de privacidad que solo aplican a la venta de información del cliente permiten que las compañías divulguen información de sus clientes a autoridades federales de control migratorio, agencias de datos y terceros para cualquier otro propósito, incluyendo informes crediticios de los consumidores y la aplicación de medidas de control migratorio.
- cuando está relacionada con información de uso, pero no hay prohibiciones sobre la divulgación de nombres e información domiciliaria.
- a menos que se divulgue a agencias de informes crediticios de los consumidores, las protecciones de privacidad que contienen excepciones en los casos de informes de los créditos que han sido rebasados permiten que las agencias divulguen el nombre y la dirección de los clientes a terceros, incluyendo a agencias de control migratorio.

Tal y como lo muestra la **Figura 5**, la gran mayoría de los estados no han adoptado protecciones sólidas de privacidad que restrinjan la divulgación de datos de clientes de servicios públicos a agencias de seguridad. Solo tres estados, California, Connecticut y Michigan, solicitan que las agencias de seguridad obtengan al menos una autorización judicial para ordenar la divulgación de datos de clientes del servicio de gas. Para los clientes del servicio de electricidad hay cinco estados con medidas en vigor: California, Delaware, Michigan, Oklahoma y Wisconsin. En el caso de clientes de servicios de telecomunicación, solo California cuenta con medidas. No hay un solo estado que haya implementado restricciones importantes para la divulgación a agencias de seguridad de información de clientes de los servicios de agua y cable.

De igual manera, como lo indica la **Figura 6**, la abrumadora mayoría de estados tampoco ha implementado protecciones de privacidad importantes que restrinjan la divulgación a terceros comerciales de información de clientes de servicios públicos.

Sin embargo, hay un estado que sobresale. Nevada ha adoptado reglas severas que prohíben la divulgación a terceros de información de clientes de servicios de gas, agua, electricidad y telecomunicaciones. Estas reglas protegen a los consumidores tanto al limitar de manera estricta la divulgación con propósitos legales, como al prohibir la divulgación con propósitos comerciales. De manera crítica y a diferencia de otros estados, las reglas de Nevada no conceden excepciones para la divulgación de la información de un consumidor a pesar de que se cuente con el permiso de éste. En un mundo donde la mayoría de los reguladores no entienden el mercado existente para la reventa y divulgación de los datos de los consumidores, tampoco se puede esperar que estos últimos lo entiendan y sean capaces de dar su consentimiento informado.

IV. ICE ABUSÓ DE LA CONFIANZA DE MENORES SIN ACOMPAÑANTE Y DE SUS FAMILIARES CON EL FIN DE SEÑALAR A ESTOS ÚLTIMOS COMO BLANCOS DE DEPORTACIÓN.

Marisol carga a su hijo de siete años mientras conversa con los abogados de inmigración en el Proyecto Dreamers de Santa Fe Dreamers. (Fotografía: Gabriela Campos/The New Mexican)

En enero de 2017, un adolescente guatemalteco que huía de las agresiones de su tío cruzó el desierto de Sonora y se presentó sin compañía alguna en la frontera de Arizona. Tenía la esperanza de encontrarse con su hermano mayor, Gari, que vivía en Santa Fe, Nuevo México.[294]

El joven de 17 años fue recibido por agentes fronterizos y luego entregado a la custodia de la Oficina de Reasentamiento de Refugiados, ORR, la cual es gestionada por el Departamento de Salud y Servicios Humanos (HHS por sus siglas en inglés). Al llegar a las oficinas, funcionarios de la ORR le preguntaron al muchacho si tenía familiares cercanos que vivieran en Estados Unidos y que pudieran recibirlo. Con frecuencia, los menores sin acompañante que llegan a la frontera temen responder esa pregunta, especialmente si sus familiares son

indocumentados, pues entienden que compartir este tipo de información con funcionarios de gobierno pondría a sus familiares en riesgo. Sin embargo, los menores tampoco tienen muchas alternativas y terminan por arriesgarse en su desesperación por reunirse con sus familias.[295] El adolescente les dijo a los funcionarios que tenía un hermano en Estados Unidos y les proporcionó su número telefónico.

Cuando Gari recibió la llamada sobre la situación de su hermano, la preocupación lo abrumó, pero también le inquietaba pensar lo que implicaría presentarse y tomar al chico bajo su cuidado. Gari tenía su propia familia: una esposa, un hijo de siete años y una niña pequeña; y temía que al involucrarse en los exhaustivos procesos de solicitud y revisión de antecedentes se pusiera él mismo en riesgo de deportación.

Los funcionarios del HHS le aseguraron que ese no sería el caso y le dijeron que su participación en el proceso no afectaría su seguridad, pues solo se necesitaba que el menor tuviera un cuidador durante sus trámites de inmigración. Teniendo esto en cuenta, Gari decidió aceptar la tutela legal de su hermano, a quien no había visto en más de una década.

Sin embargo, unos meses después, sus miedos se volvieron realidad. Después de que el menor le proporcionara al gobierno el nombre de su hermano, y luego de que Gari mismo se presentara como tutor del joven, ICE fue tras él. En agosto de ese año, agentes de ICE llegaron al hogar de Gari para arrestarlo. Lo llevaron a una de las instalaciones de ICE en Chaparral, Nuevo México, y lo pusieron en proceso de deportación.[296] Antes de llevarse a Gari, los agentes de migración incluso llegaron a buscar a su esposa, Marisol.

A. ICE ESCUDRIÑO LOS REGISTROS DE ASISTENCIA SOCIAL INFANTIL PARA ENCONTRAR BLANCOS DE DEPORTACIÓN.

En los últimos 20 años, el número de menores sin acompañante que huían de la violencia y la pobreza al cruzar la frontera de Estados Unidos ha aumentado, por un orden de magnitud, de una cifra menor a 5,000 en 2003 a casi 50,000 en 2018.[297] Esos niños suelen recorrer grandes distancias y terrenos peligrosos en busca de asilo o algún otro tipo de protección en Estados Unidos, así como para reunirse con sus familias que se encuentran en el otro lado de la frontera.[298] Cuando finalmente llegan, están traumatizados y exhaustos.

Históricamente, cuando los menores sin acompañante llegan a la frontera, el extinto Servicio de Inmigración y Naturalización, INS, era la única agencia responsable de su cuidado y custodia. El INS tenía a los niños en condiciones tan atroces que terminó afrontando una demanda judicial colectiva, *Flores v. Reno,* la cual calificaba como deplorables las condiciones vividas dentro de sus instalaciones; como que los niños se encontraban en las mismas áreas que los adultos, eran sometidos a cacheos al desnudo, y no recibían algún tipo de educación o actividades recreativas. Todo esto sucedía mientras el INS se rehusaba a liberarlos y entregarlos a tutores responsables dispuestos a cuidarlos como era debido.[299]

La demanda terminó en un acuerdo resolutorio que estableció los estándares para el trato que deberían recibir los niños bajo la custodia del INS, incluyendo cubrir necesidades básicas como agua potable y comida, así como que se priorizara que el menor fuera asignado a un pariente o tutor con el fin de reducir su tiempo en detención.[300]

Con la Ley de Seguridad Nacional de 2002, la tarea de cuidar a menores sin acompañante que llegaran a los Estados Unidos se separó de las funciones de las autoridades federales de inmigración y se le adjudicó a la ORR, una agencia perteneciente al HHS y que era más apta para el cuidado de los niños.[301]

Hoy en día, bajo el marco establecido por dicha ley, los menores sin acompañante tienen que dejar de ser custodiados por agencias federales de migración como CBP o ICE, y pasar al cargo de la ORR tan pronto como sea posible. Cuando un menor sin acompañante llega a la frontera de Estados Unidos y es recibido por agentes fronterizos o por algún otro brazo del DHS, tiene que ser referido a la ORR para su cuidado en un plazo no mayor a 72 horas, mientras espera la revisión legal de su caso.[302] Por su parte, y a través del Acuerdo Flores y la *Trafficking Victims Protection Reauthorization Act* de 2008 (Ley de Reautorización de Protección de Víctimas de la Trata de Personas, TVPRA por sus siglas en inglés), la ORR tiene obligaciones vinculantes para encontrar el "ambiente menos restrictivo y más benéfico para el menor" y llevarlo ahí a la brevedad.[303] Esto implica que, cuando sea posible, la ORR deberá encontrar a familiares o tutores que puedan hacerse cargo del menor.[304]

Para encontrar posibles tutores, la ORR depende de la información que los mismos menores son capaces de proporcionar. Tras el ingreso del menor, miembros del personal le preguntan si tiene parientes o tutores dentro de los EE.UU. con quienes tengan intención de vivir. Si el menor es capaz de ofrecer esta información, la ORR contactará al tutor potencial para preguntarle si estaría dispuesto a hacerse cargo.[305]

Sin embargo, antes de poner al menor bajo la custodia de un guardián, la ORR tiene la responsabilidad de evaluar la aptitud de éste y, cuando sea pertinente, verificar que el adulto sí es familiar o tutor del menor. Aquellos que solicitan ejercer como tutores de un menor deben proporcionar a la ORR documentos personales detallados, como: información de contacto, comprobante de domicilio, información sobre personas con quienes se comparte vivienda, información financiera, información sobre su relación con el menor.[306] El tutor también está sujeto a una revisión de sus registros públicos, así como a la toma de sus huellas digitales para una verificación de antecedentes criminales.[307] Si bien compartir estos datos personales muchas veces es una decisión difícil, es algo que miles de personas han hecho, pues comprenden que es la única forma para que el menor que estiman pueda salir de un centro de detención. Al compartir esta información, estas personas deben confiar que la ORR no tiene un motivo ulterior más que el de velar por el bienestar del menor.

Agentes de ICE buscaron exhaustivamente entre los datos proporcionados por menores sin acompañante y sus tutores para armar "expedientes de candidatos de deportación" de dichos tutores.

Bajo la administración de Trump, ICE explotó esa confianza para encontrar blancos de deportación entre los familiares que aceptaron hacerse cargo de niños sin acompañante. En mayo de 2017, ICE inició con la *Human*

Smuggling Disruption Initiative (Iniciativa para acabar con el tráfico ilegal de personas), que aparentemente tenía la intención de acabar con el tráfico ilegal de personas y las organizaciones que lo ejercen. Esa iniciativa fue una "operación entre agencias con una duración de 90 a 120 días", enfocada a la "identificación, investigación y arresto de los facilitadores del tráfico ilegal de seres humanos, incluyendo, pero no limitado a, parientes y familiares de las víctimas."[308]

Durante esta operación, los agentes de ICE buscaron exhaustivamente entre años de archivos de la ORR con información proporcionada tanto por menores sin acompañante como por sus posibles tutores. Para recibir la información emitida por la ORR, la agencia se sirvió del NLETS, y posteriormente armó compilaciones denominadas como "expedientes de candidatos a deportación" de esos posibles tutores.[309] ICE tomó estos expedientes de candidatos y abrió casos a través del software conocido como *Investigative Case Management* (Gestión de Casos de Investigación, ICM por sus siglas en inglés) de la empresa Palantir; un sistema que ayuda a los agentes a gestionar investigaciones y a integrar una multitud de flujos de datos adicionales provenientes de fuentes dentro de las mismas agencias de seguridad.[310]

Al final, a pesar del propósito declarado de la iniciativa, ICE la utilizó casi exclusivamente para abordar a los posibles tutores de niños sin acompañante en vez de llevar a cabo operativos en contra del tráfico ilegal de personas. Más de 400 personas fueron arrestadas durante este programa, de las cuales a la mayoría nunca se les acusó de cometer crímenes por tráfico ilegal, sino por infracciones civiles migratorias.[311] ICE no solo se fue sobre los posibles tutores, también emprendió "arrestos colaterales" de personas que compartían residencia con los detenidos.[312]

Las acciones de ICE tuvieron efectos inmediatos en el bienestar de los menores y de sus posibles tutores. En una carta fechada en diciembre de 2017, dirigida a la *Office of Civil Rights and Civil Liberties* del DHS (Oficina de Derechos y Libertades Civiles), ocho organizaciones de derechos civiles documentaron los daños ya ocasionados sobre los menores y sus tutores. La carta hacía hincapié en el hecho de que los tutores temían cada vez más que el hacerse cargo de un menor condujera a su propio arresto o al de sus familiares, por lo que era más probable que evitaran presentarse y, por ende, provocaría que los niños permanecieran languideciendo durante largos periodos de detención. La estadía prolongada de los menores también conllevaba a una escasez importante de camas en los albergues gubernamentales, lo que generaba una acumulación de niños en las abarrotadas celdas de las estaciones de la patrulla fronteriza, que carecían del equipo básico para el cuidado de los infantes.[313]

"El aumento de las persecuciones sería reportado por los medios y tendría un efecto disuasorio importante."

La política de compartición de datos también tuvo un impacto devastador en los tutores y otros miembros de sus hogares. Las familias que ya se habían reunido con los menores a través de la ORR comenzaron a recibir visitas inesperadas por parte de ICE, y los tutores que se habían comprometido a hacerse cargo de algún niño eran premiados con interrogatorios y arrestos; separándolos no solo del menor bajo su cuidado,

sino también de sus propios hijos. De cara a los nuevos e inesperados desafíos legales, las familias han padecido inestabilidad financiera y de vivienda, mientras que los menores han experimentado consecuencias importantes en su salud mental.[314]

Los daños que ICE estaba causando a estos niños y a sus tutores en Estados Unidos no fueron un subproducto de una política de seguridad fronteriza mal desarrollada; fueron acciones deliberadas que formaban parte de estas medidas. Un memorándum filtrado en 2019 dirigido al senador Jeff Merkley (D-OR) muestra que señalar a posibles tutores para su deportación fue una acción elaborada con la intención de disuadir a futuros solicitantes de asilo, en donde se tenía plena consciencia del impacto negativo que tendría sobre los menores que ya se encontraban en custodia.[315] El memorándum, fechado en diciembre de 2017, detalla cómo un acuerdo formal de compartición de datos con la ORR promueve dicho objetivo.

A pesar de la creciente evidencia de los daños que causó esta política, ICE y la ORR decidieron formalizarla. En un memorándum de acuerdo fechado en abril de 2018, la ORR acordó proporcionar a ICE "el nombre, fecha de nacimiento, dirección, huellas digitales [. . .] y cualquier otro documento de identificación o información biográfica disponible sobre el posible tutor, así como de todos los otros adultos que habitaran en el mismo domicilio."[316] Esto no solo le dio a ICE el acceso a los datos históricos de la ORR, sino a la información que ingresaba continuamente sobre tutores potenciales y el resto de los miembros de su residencia.

Con la información proporcionada directamente desde la agencia legalmente obligada a velar por "el bienestar de los niños", ICE procedió a ubicar y arrestar a cientos de posibles tutores que habían aceptado hacerse cargo de menores que, de otra forma, habrían permanecido en detención. De acuerdo con su declaración ante el Congreso, Matthew Albence, el entonces director de ICE, la agencia arrestó a cerca de 330 tutores potenciales basándose en la información obtenida a través del programa de datos compartidos, antes de que este terminara.[317] Este número se suma a los casi 400 arrestos emprendidos durante la fase piloto del programa.

A medida que pasaban los meses, las consecuencias negativas de la política de datos compartidos entre ICE-ORR siguieron acumulándose. Cada vez menos tutores estaban dispuestos a dar la cara por los menores por

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.

Extracto de Policy Options to Respond to Border Surge of Illegal Immigration, (Código de formas para responder al surgimiento de la inmigración ilegal en la frontera), memorándum interno del DHS obtenido y difundido por el senador Jeff Merkley en enero de 2019. (Fotografía: Oficina de Sen. Merkley)

temor a ponerse en riesgo a ellos mismos o a alguno de sus familiares. Una encuesta de la *Women's Refugee Comission* (Comisión de Mujeres Refugiadas) y el Centro Nacional de Justicia para Inmigrantes (NIJC por sus siglas en inglés) aplicada a personas que trabajan con menores sin acompañante (defensores de infantes, abogados, técnicos en biometría) encontró que 75% de los encuestados sabían de posibles tutores que no se habían presentado por miedo al acuerdo de datos compartidos, mientras que dos tercios de los encuestados conocían muchos más casos.[318] Este temor no se limitaba a los tutores indocumentados, ya que la solicitud de tutela indaga sobre el resto de los miembros que habitan en el domicilio en el que el menor podría llegar a vivir. El hecho de que los tutores evitaran presentarse podría ser una respuesta a la necesidad de proteger al resto de los parientes con quienes comparten residencia.

Los menores sin acompañante permanecieron en las instalaciones de la ORR por un tiempo prolongado. Entre 2017 y 2019, se duplicó el tiempo promedio que los niños pasaban en detención.[319] Por otro lado, el número de menores detenidos también se disparó. Entre el verano de 2017 y el verano de 2018, el número de niños migrantes detenidos se multiplicó cinco veces; de 2,400 a 12,800.[320] Mientras tanto, la acumulación de casos siguió creciendo en las estaciones de la patrulla fronteriza, donde miles de menores apretujados en celdas esperaban que se abrieran espacios para ellos en los albergues de la ORR.[321]

A medida que la indignación pública creció y se volvió más evidente que la política de datos compartidos entre ICE y la ORR violaba el Acuerdo Judicial *Flores* y la TVPRA[322], los legisladores trataron de intervenir. La Ley de Partidas Presupuestarias Año Fiscal19 prohibió al DHS emplear fondos para "realizar detenciones, retirar o poner a consideración el inicio de procedimientos de expulsión o iniciar procedimientos de expulsión en contra de algún tutor, de un posible tutor, o de algún miembro que resida en la casa del tutor o del posible tutor de un menor inmigrante sin acompañante."[323] (El *Center on Privacy & Technology* se enorgullece de haberse asociado con el *Brennan Center for Justice*, el NIJC y con una coalición de decenas de organizaciones de la sociedad civil con el fin de presionar para que se efectuara esta disposición.)

Sin embargo, la cláusula en la ley de partidas presupuestarias no vetaba a las agencias a que compartieran datos con este fin, ni les cortaba la financiación en todas las instancias. No fue sino hasta marzo de 2021 que el Memorándum de Acuerdo fue clausurado oficialmente y reemplazado por otro que ya no comprometía a la ORR a compartir con ICE datos de los tutores, como huellas digitales o información biográfica.[324]

Desafortunadamente, esta no es la única historia de su tipo. El hecho de que el acuerdo de datos compartidos entre ICE y la ORR provocaba que los tutores potenciales no se presentaran para hacerse cargo de los menores sin acompañante, y que eso a su vez suscitara que los niños languidecieran en centros de detención fronterizos por largos periodos de tiempo, no debe verse como una atrocidad aislada. Al contrario, debe entenderse como parte de un patrón mucho más amplio en el que ICE se sirve de la vigilancia para señalar, cohesionar y explotar a uno de los sectores poblacionales más vulnerables de nuestro país.

B. LA VIGILANCIA DE ICE TIENE EFECTOS DISUASORIOS CLAROS Y MEDIBLES SOBRE LA CAPACIDAD DE LA GENTE PARA OBTENER ACCESO A SUS NECESIDADES BÁSICAS.

Teniendo su origen en la doctrina de la Primera Enmienda, la frase "efectos disuasorios" captura la idea de que algunas leyes o acciones gubernamentales evitan que la gente participe en actividades protegidas por la Constitución; en gran medida por miedo a ser perseguidos o por la incertidumbre de los procesos legales que se podrían iniciar.[325] Cuando de vigilancia se trata, esa sensación de incertidumbre—es decir, el no saber qué es lo que el vigilante sabe, cómo y desde dónde está observando, así como las consecuencias de esas vigilancia—es lo que la convierte en una acción particularmente efectiva para frenar y amedrentar a la gente.[326]

No obstante, tal y como los efectos disuasorios del acuerdo de datos compartidos entre ICE-ORR lo han dejado claro, la vigilancia por parte de las agencias migratorias evita que se lleven a cabo muchas más actividades que las protegidas por la Primera Enmienda. Además de inhibir la libertad de expresión o asociación, la vigilancia por parte de ICE—o incluso solo la posibilidad de ésta—también impide que la gente participe en un amplio rango de actividades fundamentales y necesarias para la salud y el bienestar.

1. La vigilancia provoca que los inmigrantes eviten interactuar con sistemas institucionales independientemente de su función.

La socióloga Sarah Brayne introdujo el concepto de "evasión del sistema" para describir cómo el temor de ser objeto de la vigilancia de agencias de seguridad afecta la disposición de los individuos para involucrarse en actividades esenciales.[327] A través de dos encuestas longitudinales y representativas a nivel nacional realizadas a jóvenes estadounidenses, Brayne encontró que quienes han estado en contacto con el sistema de justicia penal—desde haber sido detenidos brevemente en las calles hasta haber estado encarcelados—tienen menos probabilidades de interactuar con instituciones que manejan expedientes con datos personales (como bancos, hospitales, empleadores y escuelas) en comparación con aquellos que no lo han hecho. Al mismo tiempo, el contacto con el sistema de justicia penal no disminuyó la tasa con que la gente interactuó con instituciones que no manejan expedientes con datos personales, como organizaciones de voluntarios y grupos religiosos. Esto sugiere que la evasión de las personas está profundamente vinculada al registro de datos personales y, por consecuencia, a temores sobre cómo se podría utilizar esta información.

De manera similar, el sociólogo Asad L. Asad observó que los miedos de deportación estaban correlacionados con el temor de los inmigrantes de estar "en el sistema."[328] Analizando los resultados de 50 entrevistas hechas a profundidad a inmigrantes latinoamericanos en Dallas, Asad encontró que, para los participantes indocumentados, mantener su información privada fuera de instituciones que hacen expedientes personales era sinónimo de una sensación de seguridad. Algunos inmigrantes indocumentados incluso evitaban procesos en los que podrían legalizar su estatus migratorio, ya que su participación en ellos implicaría que se hicieran visibles a alguna institución que pudiera deportarlos. Por otro lado, en el caso de inmigrantes autorizados, como residentes permanentes o personas protegidas por el DACA, Asad observó que el "tener documentos" podía incluso aumentar el temor.

Los inmigrantes con estatus migratorio legal expresaron su preocupación por cometer algún paso en falso—algún error al llenar algún papel, una multa de tránsito sin pagar—que pudiera quedar registrado en sus expedientes y, por ende, poner su estatus migratorio en riesgo.

Estos temores pueden durar generaciones enteras. En una encuesta realizada a adultos hijos de inmigrantes, muchos de ellos ciudadanos estadounidenses, Desai et al encontraron que la evasión del sistema estaba relacionada al hecho de tener un padre o madre indocumentado.[329]

Estos estudios ofrecen una perspectiva a través de la cual podemos comenzar a entender todo aquello que ha sido documentado tanto en anécdotas como en la literatura académica: los temores sobre el intercambio de datos provocan que los inmigrantes evadan instituciones que mantienen registros y que, al mismo tiempo, son cruciales para su propio bienestar y el de sus familias. Ese miedo persiste incluso cuando se trata de involucrarse con instituciones que no están relacionadas con temas migratorios. El resto de esta sección demuestra cómo la

RECUADRO 3.
LOS DAÑOS DE LOS EFECTOS DISUASORIOS VAN MÁS ALLÁ DE LAS PERSONAS INDOCUMENTADAS.

Evadir instituciones que mantienen registros no solo provoca daños entre las personas, éstos también afectan a familias y comunidades enteras. Muchas familias de inmigrantes tienen estatus migratorios mixtos, lo que significa que diferentes miembros de los hogares tienen diferentes estatus legales y, por lo tanto, enfrentarán diferentes niveles de riesgo de deportación. Los impactos de la evasión del sistema por parte de padres indocumentados se extienden a sus hijos, de los cuales casi un 90% son ciudadanos estadounidenses.[330] El efecto de todo esto también afecta a la comunidad. Por ejemplo, si algunos miembros evitan buscar atención médica, los problemas de salud que bien podrían prevenirse se vuelven costosos y debilitan al resto de la comunidad.[331] Lo mismo sucede en las escuelas; la falta de seguridad alimentaria de un niño en particular puede alterar el ambiente de aprendizaje del resto de los estudiantes.[332]

vigilancia disuade la participación de las personas en tres contextos específicos: asistencia social infantil, atención médica y acceso a los sistemas de justicia.

2. La vigilancia disuade a la gente a aprovechar servicios que promueven el bienestar infantil.

Las investigaciones sugieren que los miedos en torno a la vigilancia de ICE provocan que las familias indocumentadas eviten aprovechar beneficios que promuevan tanto su bienestar como el de sus hijos. Con frecuencia, los niños de padres indocumentados son ciudadanos estadounidenses, lo que significa que califican para ser beneficiarios de programas como el de asistencia alimentaria. Sin embargo, la disposición de las familias para inscribirse en estos programas puede verse influenciada por miedo a la vigilancia de las agencias migratorias. A partir de los datos de una encuesta longitudinal representativa a nivel nacional sobre el consumo de alimentos de familias con infantes, un estudio encontró que la falta de seguridad alimentaria en hogares de origen mexicano sin ciudadanía aumentó casi 10 por ciento en las áreas metropolitanas donde la policía local estableció 287 (g) acuerdos para compartir datos y cooperar con las agencias migratorias.[333]

3. La vigilancia hace que la gente evite recibir atención médica.

El temor generado por los posibles acuerdos de datos compartidos entre hospitales o clínicas y las agencias gubernamentales también impide que inmigrantes y sus familias busquen atención médica. Una revisión de los estudios que indagaban sobre los obstáculos para la atención médica a inmigrantes indocumentados encontró que casi todas las investigaciones concluyeron que los inmigrantes no se sentían seguros de proporcionar documentos o usar los servicios de atención de médica o de asistencia pública, ya que esto podría suscitar que fueran reportados ante las autoridades de inmigración.[334]

Las clínicas en Denver reportaron que algunos pacientes descartaron el uso de Medicaid por temor a estar en un "sistema gubernamental."

Los proveedores de servicios de salud también cuentan con reportes anecdóticos sobre cómo el temor a las agencias migratorias puede afectar la disposición de los individuos para recibir atención médica. Con el fin de abordar los desafíos para el acceso a la atención médica, la *Mile High Health Alliance*, una alianza de múltiples interesados con base en Denver, realizó en 2017 una encuesta entre sus clínicas miembros y asociadas en torno al uso de servicios de salud por parte de inmigrantes y refugiados.[335] En la encuesta, muchas clínicas reportaron que los pacientes expresaron sus inquietudes al compartir información, lo que los llevó a descartar el uso de Medicaid y de otros beneficios a los que tenían derecho bajo el argumento de que temían estar en un "sistema gubernamental". Algunos pacientes incluso se negaron a contestar preguntas de sus propios médicos; como cuál era su país de origen. Un paciente, cuyo pequeño era indocumentado, usó el tiempo de la cita médica para hacer preguntas sobre las políticas santuario que restringían la compartición de datos y otras formas de cooperación con autoridades migratorias.

El efecto disuasorio de la vigilancia también ha sido demostrado en una escala mayor, y no

solo entre personas con estatus migratorios precarios. Una encuesta realizada en 2015 por ciudadanos latinos estadounidenses encontró que los participantes tenían menos probabilidades de agendar una cita con algún proveedor de atención médica si el tema migratorio era mencionado durante el proceso de asignación de citas.[336] Este efecto es aún más evidente en aquellos que han sido testigos cercanos de la aplicación de medidas migratorias. Los ciudadanos latinos estadounidenses que conocían a alguna persona indocumentada o que había sufrido la deportación tenían mayores niveles de escepticismo en torno a la seguridad del manejo de la información que compartían con proveedores de servicios de salud, y no descartaban que dicha información pudiera ser compartida a instancias externas al proveedor.

4. La vigilancia disuade a las personas de interactuar con el sistema de justicia y otras entidades gubernamentales.

Se ha demostrado que la compartición de datos entre agencias gubernamentales y agencias migratorias desalienta a los inmigrantes a interactuar con entidades gubernamentales, así como a participar en procesos judiciales. Una encuesta realizada por el *Urban Institute* mostró que las familias con migrantes tenían menos probabilidades de participar en una serie de actividades de rutina por miedo a verse en la necesidad de revelar su estatus migratorio, como solicitar licencias de manejo, hablar con la policía, reportar un crimen, usar el transporte público o hablar con trabajadores escolares, incluso cuando muchas de estas instituciones no están formalmente vinculadas con las autoridades federales.[337]

Las personas con familiares migrantes tenían menos probabilidades de conducir, solicitar licencia de manejo, hablar con la policía, visitar a un médico, reportar un crimen, usar transporte público o hablar con trabajadores escolares por miedo a tener que revelar su estatus migratorio.

Otros estudios han demostrado que el miedo a la compartición de datos juega un papel crucial en lo que respecta a disuadir a migrantes y a sus familias de interactuar con los sistemas burocráticos. Una encuesta realizada por *Latinx Immigrants* encontró que los encuestados reportaron que serían menos propensos a interactuar con los sistemas burocráticos y judiciales si supieran que las entidades comparten datos con ICE.[338] De manera específica, los hallazgos de esta encuesta describen la forma en que la política de datos compartidos de ICE paraliza la disposición de las personas para reportar un crimen a la policía, testificar en corte, o tener acceso a recursos para el cuidado infantil.

CONCLUSIÓN Y RECOMENDACIONES

Maribel Cortez el día de su testimonio en la Asamblea General de Maryland. (Foto: Erin Cox/The Washington Post por Getty Images)

El 27 de febrero de 2020, antes de que se cumpliera un mes del arresto y detención de su esposo por parte de agentes de ICE, Maribel Cortés visitó el recinto de la Asamblea General de Maryland. Iba acompañada por tres de sus hijos y por representantes del CASA, una organización a favor de los derechos de los migrantes que ha liderado los esfuerzos para proteger a los migrantes de Maryland del alcance de la vigilancia de ICE.

Maribel testificó ante comités tanto de la Cámara de Delegados como del Senado Estatal, en donde no solo contó su historia, sino que puso su grano de arena para la aprobación de una ley que proteja a familias como la suya. Asistida por una intérprete del CASA, Maribel habló en español:

"esto ha destruido a mi familia", dijo entre lágrimas.[339] "Durante toda su vida ellos siempre han tenido a su padre, y ahora esto es muy difícil para ellos", declaró a The Washington Post.[340]

La historia de Maribel alentó a los legisladores a actuar. Un año y un mes después, la Asamblea General de Maryland aprobó la Ley de Privacidad de los Conductores de Maryland, un proyecto de ley que terminaría con el acceso sin orden judicial a los datos de los habitantes de Maryland por parte de ICE.

De manera notable, lo que Maribel hizo aquel día en Annapolis, Maryland, ha sido replicado por otros inmigrantes a lo largo y ancho del país; en Albany, Nueva York; Denver, el Distrito; Honolulu; Montpelier, Vermont; Olympia, Washington; Richmond, Virginia; Sacramento, California; Salem, Nueva Hampshire; Santa Fe, Nuevo México; Springfield, Massachusetts; y Trenton, Nueva Jersey, hombro con hombro con organizaciones como *Immigrant Defense Project, Just Futures Law, the Legal Aid Justice Center, Make the Road New York, Mijente* y NILC.

Las recomendaciones presentadas a continuación no solo están inspiradas en la valentía de las comunidades que siguen luchando en contra de las deportaciones masivas, también se han elaborado bajo la guía de líderes del movimiento por los derechos de los migrantes, así como por otros expertos.

A. CONGRESO

1. El congreso debe reformar las leyes migratorias de los Estados Unidos para reducir de manera radical el número de personas que pueden estar sujetas a deportación.

La mejor y probablemente única forma de desmantelar las redes de arrastre de ICE es desmantelando las leyes en las que el poder ejecutivo se apoya para señalar a cientos de miles de blancos de deportación (principalmente gente de bajos recursos o de color) cada año. El Congreso podría reducir significativamente el número de personas sujetas a deportación al crear un camino a la ciudadanía para personas indocumentadas, así como al reducir de manera dramática los argumentos para la expulsión que se basan en la participación en actividades delictivas. Para construir un baluarte adicional, el Congreso debería promulgar un estatuto de limitación en las deportaciones. La mayoría de los crímenes y ofensas civiles no se pueden procesar después de cinco años de haber sucedido. Sin embargo, y de manera incongruente, una persona puede ser deportada de este país a través de un proceso en el que no se le garantiza legalmente un abogado; a pesar de vivir aquí, haber formado una familia y pagar impuestos durante décadas. En los últimos diez años, organizaciones de derechos de los migrantes han formulado una serie de marcos legislativos que ayudarán a que estas y muchas otras reformas importantes se logren.[341] Si bien estas propuestas no abordan el tema de la vigilancia per se, son la vía más directa para socavar las demandas de ICE por tener una gran autoridad en términos vigilancia.

2. El Congreso debería proteger la privacidad de las personas que confían sus datos al gobierno federal.

El gobierno federal gestiona una serie de programas que solicitan activamente que personas indocumentadas (muchas de las cuales han experimentado traumas o han sido coaccionadas) proporcionen una gran variedad de información de identificación personal y altamente sensible a las agencias federales.

Sin importar si anteriormente se han solicitado datos para ofrecer servicios o algún tipo de beneficio, el Congreso debe prohibir en lo

general que el gobierno use esta información para iniciar deportaciones. Esta política podría tomar como ejemplo las leyes federales que protegen la confidencialidad de los datos censales, las cuales son el referente para la protección de datos sensibles que el gobierno federal solicita de la población.[342] Estas leyes tienen una importancia crucial al prohibir el uso de los datos censales para propósitos que no tengan fines estadísticos. Además, en un sentido amplio, estipulan que "en ningún caso la información proporcionada [a la Oficina del Censo] podrá usarse en detrimento de un encuestado o de otra persona a quien se relaciona tal información", con una ligera excepción para violaciones de las propias reglas del censo.[343] El Congreso debe lograr que se establezcan estas protecciones a través de un estatuto comprehensivo. Hasta que esto se logre, el Congreso debería conseguir dichas protecciones a través de las leyes de partidas presupuestarias; restringiendo el uso de fondos, mientras que el DHS debería conseguirlas por medio de la creación de políticas departamentales.

Como mínimo, el Congreso debería modificar las leyes que rigen estos programas para que prohíban que las agencias migratorias utilicen los datos específicos generados en dichos programas. El Congreso debería modificar las leyes que se muestran a continuación del siguiente modo:

- TVPRA, 8 U.S.C. § 1232, que protege a menores sin acompañante;
- Los estatutos federales que crean visas de tipo T y U para víctimas de tráfico y otros crímenes, 8 U.S.C. § 1101(a)(15)(T) & (U);
- Las leyes federales de privacidad tributaria, 26 U.S.C. § 6103; y
- Disposiciones de privacidad de la *Higher Education Act* (Ley de Educación Superior) para datos relacionados a solicitudes de apoyo financiero federal, 20 U.S.C. § 1090(a)(3)(E).

El presidente Biden o el Secretario del DHS podrían también promulgar protecciones adicionales de privacidad para los solicitantes del DACA y de otras formas de estatus de protección temporal o acciones diferidas, ya sea a través de políticas departamentales o de una orden ejecutiva.

3. El Congreso debería frenar el uso de datos del DMV por parte de ICE.

El Congreso aprobó la DPPA antes de la moderna era de vigilancia y deportaciones masivas. La ley fue aprobada en 1994, tres años antes de que Estados Unidos empezara a expulsar a 100,000 personas al año, nueve años antes de la creación de ICE, y 15 años antes de que ICE comenzara a deportar anualmente a aproximadamente el 0.1% de la población estadounidense.[344]

ICE no ha dudado en utilizar las amplias excepciones en la DPPA en lo que respecta al acceso de las agencias gubernamentales para escanear sin orden judicial los rostros de un número sorprendente de estadounidenses, así como para buscar información a través de los datos postales de la mayoría de los residentes de Estados Unidos. El Congreso debería actualizar la DPPA para prohibir o requerir un mandato judicial para el uso por parte de las agencias de seguridad de los datos de los DMV con fines migratorios.

Reps. Raja Krishnamoorthy (D.-Ill.) y Jimmy Gomez (D.-Cal.) presionaron a Thomson Reuters y Equifax para que revelaran más información de la venta de información de clientes de servicios públicos a ICE. (Fotografías: Tom Williams/Pool via Getty Images (L, R))

4. El Congreso debería llevar a cabo una supervisión feroz de la vigilancia emprendida por ICE.

Aunque ciertos miembros del Congreso han empezado a presionar a ICE por medio de cartas de supervisión, ninguno de los comités o subcomités presuntamente encargados de supervisar a ICE han llevado a cabo una audiencia dedicada a este tema en particular. Por su parte, la Oficina de Responsabilidad Gubernamental, GAO, tampoco ha realizado investigación alguna sobre el vasto arsenal de vigilancia de ICE.

Todo esto debe cambiar, y puede suceder rápidamente. Los presidentes de los comités y subcomités no necesitan una votación mayoritaria o supermayoritaria para exigir que ICE responda tanto por los abusos cometidos por su vigilancia, como por el gran secretismo que les rodea. Los posibles temas para tratar en una audiencia o en reportes de la GAO incluyen:

- si existen bases legales para las prácticas de vigilancia de ICE, dada la ausencia de una autorización explícita en estatutos o regulaciones;
- cómo ICE esquiva las leyes estatales que protegen los datos de conductores y otros residentes;
- si las redes de vigilancia y arrastre de ICE, así como el intercambio de datos, violan la Cuarta Enmienda y otras disposiciones constitucionales;
- cómo la cooperación entre las agencias de datos y ICE está por encima del

escrutinio público y ayuda a esta última a eludir protecciones reglamentarias y constitucionales de privacidad;

- cómo ICE usa actualmente información biométrica, incluyendo el reconocimiento facial, huellas digitales y ADN, y cómo planea usar esta información en el futuro;
- las ramificaciones prácticas y éticas del uso que ICE hace de registros telefónicos y de servicios de gas, electricidad, agua e internet para señalar blancos de deportación; y
- las prácticas de vigilancia de ICE a expensas de los contribuyentes.

El amplio rango de inquietudes que la vigilancia de ICE provoca debería suscitar que varios comités o subcomités del Congreso se involucraran en este tema a través de una audiencia, o al solicitar una investigación por parte de la GAO.

El Congreso también debería solicitar una declaración pública detallada sobre los programas de vigilancia de ICE como parte del proceso anual de asignación de presupuestos.

B. DHS & ICE

1. ICE debería terminar con todos los programas de redes de vigilancia y arrastre.

Los agentes de ICE han obtenido o realizado búsquedas de reconocimiento facial en los rostros de al menos 1 de cada 3 adultos. Han contratado una compañía que rastrea los movimientos vehiculares de los residentes de las 50 ciudades más grandes de los Estados Unidos, las cuales concentran la mayoría de la población del país. De igual modo, han contratado a otras compañías que les entregan los registros de los servicios públicos de la mayoría de la población de EE.UU.

Llevadas en total secretismo, incluso para los miembros de alto rango del Congreso encargados de supervisar a ICE, estas acciones minan incluso las nociones más fundamentales del equilibrio del poder, corroen la confianza pública y se pasan por alto la Cuarta Enmienda.

Todos los programas de vigilancia de ICE deberían estar sujetos a un escrutinio feroz. Sin embargo, ICE debería terminar inmediatamente con todos los programas de las redes de vigilancia y arrastre—tanto los que están dirigidos por ICE como los que funcionan a través de las agencias de datos—que recolectan datos de manera indiscriminada de tantas personas en EE.UU. como sea posible. Los programas que deberían ser categorizados como este tipo especialmente problemático de vigilancia y arrastre incluyen, por lo menos (1) la práctica del escaneo de las fotografías en la licencia de manejo para la aplicación de medidas de control migratorio; (2) la recolección de grandes volúmenes de información postal y otros registros del DMV y de compañías de servicios públicos y (3) la recolección de grandes volúmenes de fotografías de matrículas que capturan los trayectos de los conductores en las áreas metropolitanas más importantes de Estados Unidos; (4) la compra a corporaciones o agencias de grandes conjuntos datos de cualquier información antes mencionada.

2. ICE debería dejar de usar el reconocimiento facial para la aplicación de medidas de control migratorio.

En mayo de 2020, ICE emitió una *Privacy Impact Assessment* (Evaluación del Impacto de la Privacidad), en donde afirmaba que las "Operaciones de Expulsión y Cumplimiento de la Ley (ERO) no usarán, y la HSI tampoco apoyará que las ERO utilicen [sistemas de reconocimiento facial] solo para fomentar el

cumplimiento de la ley migratoria."[345]. Parecería que esta declaración seguiría permitiendo a ICE utilizar el reconocimiento facial para señalar sin restricciones a casi cuatro de cada diez personas indocumentadas que hubieran entrado al país sin inspección alguna, o a cualquier otro inmigrante que estuviera presuntamente involucrado en cualquier delito por mínimo que fuera.[346] Estas ofensas justificarían el escaneo facial de millones de estadounidenses sin distinción alguna, fueran nativos o nacidos en el extranjero, con documentos o indocumentados.

En 2021, se encontró que los algoritmos de reconocimiento facial estaban plagados con sesgos raciales y de género establecidos por el mismo gobierno.[347] De hecho, habían sido utilizados de formas que abiertamente violaban los principios básicos de privacidad y de un proceso justo.[348] Además, habían derivado en una serie de acusaciones y arrestos de un gran número de personas sin tener bases legales, muchas de las cuales eran gente de color.[349] ICE no debería emplear esta herramienta para ningún tipo de medida de control migratorio.

3. ICE debería dejar de aprovechar la necesidad de la gente por servicios como agua, calefacción, electricidad, teléfono o internet para buscar blancos de deportación.

Actualmente hay investigaciones basadas en una gran cantidad de evidencia revisada entre homólogos que muestra que los inmigrantes evitan usar servicios esenciales, como la atención médica; no solo por miedo a que los arresten dentro de las mismas instalaciones, sino porque temen que sus datos lleguen a manos del gobierno federal y se mantengan almacenados en los sistemas del Estado.[350]

Las personas necesitan calefacción, agua y electricidad para sobrevivir. De igual manera, requieren internet y líneas telefónicas para sostener sus medios de vida y conectarse con sus comunidades. Sin embargo, ahora sabemos con certeza que las direcciones e información de casi 200 millones de adultos ha llegado a ICE después de que éstos contrataran servicios de agua, gas, electricidad, teléfono o internet.[351] El DHS debería emitir de manera inmediata una clara prohibición en contra del uso de estos datos para la aplicación de medidas de control migratorio.

4. ICE debería informar a los miembros del Congreso y funcionarios clave del Estado sobre los programas de vigilancia y los fondos invertidos.

Los presidentes de los comités clave del Congreso se han enterado de los extensos programas de vigilancia de ICE a través de los periódicos. Lo mismo ha sucedido con los legisladores, que son los responsables de autorizar y votar por la financiación de muchas de las bases de datos estatales utilizadas por ICE. Los rostros de uno de cada tres adultos han sido escaneados por ICE—o por encargo de ICE—sin su conocimiento.[352]

Esto no solo no es aceptable, tampoco es compatible con los principios básicos de un gobierno democrático. ICE debería, como mínimo, emitir informes regulares a los miembros y personal de los comités y subcomités clave de supervisión del Congreso, incluyendo:

- Comité de Seguridad Nacional y Asuntos Gubernamentales del Senado;
- Comité de Asuntos Judiciales del Senado, incluyendo la Subcomisión de Migración, Ciudadanía y Seguridad Fronteriza y la Subcomisión de Privacidad, Tecnología y Leyes;
- Comité de Seguridad Nacional de la Cámara de Representantes;

- Comité de Asuntos Judiciales de la Cámara de Representantes, incluyendo la Subcomisión de Migración y Ciudadanía; y
- Comité de Supervisión y Reformas de la Cámara de Representantes.

(Para una referencia precisa, los nombres oficiales en inglés de estos comités es, en el mismo orden: 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; y the House Committee on Oversight & Reform.) ICE también debería emitir un informe a los gobernadores y legisladores clave de los estados en los que realiza sus prácticas de vigilancia. ICE suele notificar al estado y a los funcionarios locales antes de emprender acciones para señalar a cientos de personas como blancos de las medidas de control migratorio. Si, por ejemplo, ICE se involucra en programas de redes de vigilancia que atraparán a millones de conductores con licencias del estado, entonces debería notificar a los funcionarios estatales sobre estas acciones.

5. El inspector general del DHS debería emitir reportes regulares de las actividades de vigilancia de ICE.

Informar solamente a los legisladores no es suficiente. A menudo, el poder ejecutivo tiene una impresión muy diferente de lo que se reporta en comparación a lo que sabe su audiencia. En 2013, después de que la prensa publicara las órdenes judiciales que revelaban que la Agencia de Seguridad Nacional estaba recabando de manera significativa todos los registros de llamadas domésticas de los estadounidenses, Obama aseguró al público que "cada miembro del Congreso ha recibido un informe sobre este programa".[353] El proponente de la de la Ley USA PATRIOT en la Cámara de Representantes, el Rep. Jim Sensenbrenner (R-Wisconsin) respondió inmediatamente que, de hecho, "la mayoría" de los miembros del Congreso—él incluido—se habían quedado a oscuras con respecto a este tema.[354]

Para evitar que estos errores se repitan, el inspector general del DHS no solo debería informar a los miembros del Congreso, gobernadores y legisladores estatales, también debería ofrecer un reporte de carácter público. Como mínimo, estos informes tendrían que identificar:

- los tipos de tecnologías que ICE está empleando (ej. reconocimiento facial, lector automático de matrículas vehiculares, etc.);
- los estados y condados en los que ICE aplica estas herramientas;
- las bases de datos gubernamentales y estatales a las que ICE tiene acceso, los tipos de datos que hay en dichas bases, y los números de búsquedas realizadas;
- el número aproximado de personas cuyos datos han sido recolectados, o a quién pertenecen los datos en las bases de datos revisadas;
- el número de personas que fueron arrestadas, encarceladas o deportadas a partir de la información recabada o revisada; y
- si ICE ha informado a funcionarios locales, estatales y federales sobre los operativos llevados a cabo.

El gobierno federal ya publica informes anuales detallados sobre dónde, cuándo y por cuánto tiempo se intervienen las líneas telefónicas; la naturaleza de los crímenes investigados; y los resultados de dichas investigaciones. Esto

se lleva a cabo independientemente de la severidad de la ofensa.[355]

C. LEGISLADORES ESTATALES & LOCALES[356]

1. Los legisladores estatales y locales deben proteger a las personas que les confían sus datos.

Cuando personas indocumentadas aplican para una licencia de manejo, inscriben a sus hijos (o a ellos mismos) en la escuela, se registran para recibir la vacuna contra la COVID-19, o dependen de programas estatales o locales de asistencia alimentaria, lo hacen bajo la promesa explícita o implícita de que las autoridades estatales o locales no permitirán que sus datos sean divulgados, en masa, con las autoridades de control migratorio.

Los gobiernos estatales y locales deben ofrecer protecciones comprehensivas para cualquier información—no solo datos de conductores vehiculares—de residentes indocumentados que sea solicitada y mantenida por el estado en cuestión. Lo que es más, las demarcaciones que ya han promulgado estas políticas deberían tomar medidas para fortalecer estas protecciones lo más posible. De manera específica, los legisladores deberían:

- **Adoptar una política de minimización de datos.** Autoridades de inmigración, agencias de datos y otros partidos no pueden explotar datos que no existen. Las burocracias estatales y locales deberían adoptar una política de minimización de datos en donde: solo se recaben los datos necesarios para la administración de servicios; los datos se almacenen durante el menor tiempo posible; se diseñen sistemas digitales de expedientes en donde la minimización de datos sea un aspecto prioritario de su configuración.
- **Enfocarse en los datos, no en quien los custodia.** Diferentes agencias pueden tener acceso a los mismos grupos de datos, incluidos los registros de conductores vehiculares. El *Sanctuary Values Act* de D.C. (Ley de los Valores Santuario) evita este problema al restringir la difusión de información de identificación personal y otros datos por parte del "Distrito de Columbia", en vez de nombrar a agencias o subagencias específicas.[357]
- **Enfocarse en el *propósito* del intercambio de datos, no en el receptor.** Nombrar a ICE es, al mismo tiempo, sub- y super-inclusivo. Otras agencias federales (ej. CBP) normalmente se involucran en medidas de control migratorio, y ciertos componentes del trabajo de ICE están separados de temas relacionados al control en sí.[358] Por lo tanto, las demarcaciones deben proteger en contra del intercambio de datos cuyo *propósito* sea el control migratorio, no solo en contra del intercambio de datos con ICE, la entidad. Un ejemplo de esto es la Ley de Privacidad de los Conductores de Maryland aprobada en 2021, la cual bloquea el intercambio de datos sin orden judicial previa con "cualquier agencia federal" que busque obtener acceso con el propósito de "hacer cumplir la ley federal de inmigración".[359]
- **Proteger en contra de todas las formas de compartición de datos,** incluyendo (1) compartir información en respuesta a una solicitud directa, (2) acceso a las bases de datos para funcionarios de agencias de control migratorio, y (3) la venta o compartición de información a agencias de datos, quienes, a su vez, los entregan al servicio de inmigración. Con frecuencia, abordar los dos primeros modos de compartición de datos es un proceso sencillo.

El tercero, sin embargo, normalmente requiere de un uso meticuloso del lenguaje. La Ley Luz Verde de Nueva York sirve de modelo en ese sentido, pues contiene una disposición en donde se establece que cualquier entidad que reciba datos de conductores tiene que certificar que no revelará la información a las agencias de control migratorio.[360]

- **No hacer distinciones entre la aplicación "civil" y "criminal" de leyes migratorias para fines de protección de la privacidad y restricciones en la compartición de datos,** ya que la ley federal criminaliza tanto el ingreso ilegal como el reingreso ilegal.[361] Por ejemplo, la ley de Hawái que permite que personas indocumentadas soliciten una licencia de conducir establece una prohibición simple en contra de la compartición de datos de los solicitantes, sin ningún tipo de excepción para ningún tipo de medida de control migratorio.[362]
- **Asegurarse que el reconocimiento facial esté claramente incluido en estas restricciones.** Las fotografías del DMV a veces quedan excluidas en las categorías de datos protegidos de las leyes estatales de privacidad.[363]
- **Eliminar las excepciones generales para que las "autoridades de control migratorio" tengan acceso a datos locales o estatales.** Entre 2017 y 2019, los legisladores de California aprobaron tres leyes diferentes para prevenir que las agencias estatales compartieran libremente datos de conductores con autoridades de inmigración.[364] Desafortunadamente, no modificaron una ley separada que dictamina que "las agencias de control migratorio . . . tendrán acceso a" los registros del DMV de California. El DMV suele valerse de esta disposición para defender su aparente intercambio de datos de conductores con ICE.[365]
- **Los legisladores estatales y locales deberían configurar las bases de datos gubernamentales de manera que puedan rastrear los accesos de ICE y revisar regularmente dichas bases para identificar las rutas, frecuencia y naturaleza de éstos.**

Cualquier administrador de una base de datos debe tener la capacidad de contestar las siguientes dos preguntas: ¿tiene ICE acceso a esta base de datos? Si ese es el caso, ¿cómo y por qué la ha utilizado ICE? En la tercera década del siglo XXI, los gobiernos locales y estatales no tienen excusas para que una base de datos con datos sensibles no cuente con un sistema que registre cuidadosamente los tiempos y frecuencia de la actividad, y además garantice el acceso solo de personas autorizadas.

Resulta inusual e inaceptable que las actuales bases de datos del gobierno no cuenten con mecanismos de auditoría. Si a los legisladores se les dice que el monitoreo no es posible, entonces deben redoblar la presión.

Las autoridades estatales y locales deberían revisar con regularidad estas bases de datos para determinar si ICE está ingresando a ellas, cómo y con qué frecuencia. Si las autoridades no llevan a cabo estas inspecciones por su cuenta, los legisladores deberían enviar cartas de supervisión

RECUADRO 4.
PROHIBICIONES FEDERALES EN LAS LEYES SANTUARIO ESTATALES Y LOCALES.

No hay ley federal que limite o prohíba a un estado o a una localidad de establecer restricciones en la recolección, retención y difusión del nombre y el domicilio de alguno de sus residentes. Una ley federal, la 8 U.S.C 1373, pretende prohibir que un estado o localidad establezca límites en la compartición de datos relacionados a "la ciudadanía o el estatus migratorio" de alguno de sus residentes.[366] Sin embargo, la constitucionalidad de esa ley aún está pendiente,[367] y por sus propios términos no se extiende a restricciones en la recolección, retención o compartición del nombre y la dirección de algún residente.

a las agencias estatales exigiendo un monitoreo y audiencias de supervisión para obligar a que los funcionarios de estas agencias actúen.

Los legisladores que presionan para que esas auditorías se lleven a cabo deberían saber que es inusual e inaceptable que una base de datos moderna omita estas acciones de monitoreo, y si se les niega la posibilidad de hacerlo, deberían presionar aún más. En Maryland, por ejemplo, a los legisladores se les dijo inicialmente que el sistema estatal de reconocimiento facial, el *Maryland Image Repository System*, no era capaz de rastrear a los usuarios según la agencia de procedencia de sus datos. Sin embargo, en una visita subsecuente, los legisladores se enteraron de que el *Department of Public Safety and Correctional Services* (Departamento de Seguridad Pública y Servicios Correccionales, DPSCS por sus siglas en inglés) si tenía la capacidad de rastrear esos datos.[368]

2. Los legisladores estatales y locales deberían bloquear la difusión, venta o reventa de los datos de las compañías de servicios públicos para su uso en el control migratorio.

Los servicios públicos de gas, agua y electricidad están ampliamente regulados a nivel estatal y local por estatutos, ordenanzas y comisiones de supervisión de los servicios públicos. Asimismo, los gobiernos estatales y locales con frecuencia tienen protecciones de datos del servicio telefónico y de internet que complementan a la ley federal.[369] Las autoridades estatales y locales

deberían prohibir la difusión, venta o reventa de esos datos cuyos fines estén relacionados al control migratorio.

Algunos estados tienen buenos estándares de privacidad que aplican a un servicio en particular (ej. gas o electricidad). No obstante, no existe un estado o territorio que haya promulgado protecciones de privacidad comprehensivas y significativas para todos los servicios públicos. Al promulgar este tipo de protecciones, las autoridades estatales y locales deberían:

- **Restringir la difusión a agencias de datos, no solo al gobierno.** ICE suele obtener acceso a registros de servicios públicos a través de las agencias de datos, en vez de solicitarlas directamente a las compañías. Las leyes deben proteger contra la difusión de estos datos a terceros, como lo son estas compañías, y no solamente al gobierno.
- **Evitar excepciones generales para información y evaluaciones crediticias.** Los datos divulgados a una agencia crediticia para propósitos relacionados a los créditos pueden ser fácilmente redivulgados a las autoridades de inmigración. De hecho, la entidad que creó las bases de datos a la que Equifax ingresó en un principio para después entregar la información de servicios públicos a Thomson Reuters, y subsecuentemente a ICE, es una agencia de información crediticia. [370] Desafortunadamente, las leyes estatales de privacidad que rigen a los servicios públicos están plagadas de lagunas que permiten estas triangulaciones.[371]
- **Crear protecciones contra *todas* las formas de divulgación.** El trayecto de los datos de registro de servicios públicos hacia ICE parece mostrar que las compañías de servicios compartieron voluntariamente (en vez de vender) sus datos con NCTUE, que luego divulgó los datos a Equifax, quien posteriormente se los entregó a Thomson Reuters, quien a su vez se los otorgó a ICE. Por lo tanto, se quedará corta cualquier ley que solo prohíba la venta de esos datos en vez de *cualquier otra forma de divulgación* o que, en su defecto, no aborde la reventa o redivulgación de los datos.
- **Asegurarse de proteger las direcciones de los clientes.** Muchas leyes de privacidad de los servicios públicos se enfocan en los usos de sus datos. Desafortunadamente, algunas de estas leyes no son lo suficientemente claras con respecto a sí las direcciones de los clientes están protegidas.[372]

Las leyes de privacidad de Connecticut sobre las compañías de gas ofrecen un modelo inusual con respecto a cómo debería ser un estatuto ideal. Las leyes prohíben que se compartan datos a terceros y, al mismo tiempo, limitan estrechamente la compartición que sí ocurre. Además, no contienen excepciones generales para la información crediticia y protegen en contra de todas las formas de compartición de información, no solo contra la venta.[373]

Desde que Biden asumió la presidencia a inicios de 2021, el enfoque de la vigilancia de ICE no ha cambiado mucho. Los contratos de la agencia para lectores automáticos de matrículas vehiculares, bases de datos de registros públicos, tecnología de reconocimiento facial, rastreo de geolocalización y sistemas para la visualización y análisis de datos no solo siguen en vigor, sino que se han renovado y, en algunos casos, extendido. Las políticas y acuerdos gubernamentales que permiten el acceso descontrolado a las bases de datos del estado siguen vigentes. En vez de desmantelar aquello que se ha heredado, Biden y el Congreso han mantenido el estado de vigilancia a los migrantes.

Antes de las elecciones, la campaña de Biden prometió "prioridades sensatas en asuntos de seguridad", y escribió que "nadie debería tener reticencia de buscar atención médica; ir a la escuela, al trabajo o a los espacios de culto religioso por miedo a las acciones de control migratorio."[374] Casi un año después, Biden ha tomado algunas medidas para reducir las deportaciones, al tiempo que el número de arrestos de migrantes están en el nivel más bajo de los últimos 10 años.[375] No obstante, la administración aún no ha echado mano del gran poder del ejecutivo para reducir las actividades de vigilancia a gran escala emprendidas cotidianamente por ICE, lo que plantea riesgos inmediatos a la seguridad y al bienestar de las comunidades de migrantes en todo el país.

Independientemente de si esta administración en particular se sirve de la vigilancia para emprender cuatro o 400,000 deportaciones este año, la existencia del aparato de vigilancia de ICE representa en sí un problema serio. Así como se carecen de estatutos o regulaciones que autoricen explícitamente al gobierno federal a utilizar la vigilancia masiva para llevar a cabo deportaciones, tampoco hay estatutos o regulaciones que obliguen al gobierno federal a utilizar la información recabada de dicha vigilancia solo para fines de deportación. La vigilancia de ICE debería preocuparle a usted; quizá no porque le importe lo que le pueda suceder a las comunidades de inmigrantes, a la confianza pública en las instituciones gubernamentales, a los derechos de privacidad o al balance de poder político en nuestra democracia, sino porque le importa lo que le pueda suceder a usted o a las personas que ama si alguien decide buscarles entre las redes de arrastre de Estados Unidos.

APÉNDICE

APÉNDICE A: METODOLOGÍA DETALLADA DE ANÁLISIS DE ADQUISICIONES Y CONTRATACIONES.

A. FUENTES DE DATOS

Inspeccionamos todos los contratos de ICE desde enero de 2008 a septiembre de 2021: 40,715 contratos únicos de ICE con un total de 108,873 transacciones.[376] Descargamos información de contratos de ICE de USAspending, que es la "fuente oficial de datos de gastos" del gobierno federal.[377] En casos en donde ICE dio por terminado un contrato de vigilancia durante nuestro período de revisión sin haber gastado más dinero, decidimos excluirlo.

Hay algunas limitaciones en torno a la fiabilidad de estos grupos de datos.[378] Por ejemplo, no tenemos acceso a los pagos reales de ICE.[379] En cambio, nos valimos de datos de USAspending que rastrean las promesas de gasto de fondos de ICE, conocidas como obligaciones.[380] Para un contrato cerrado, la obligación total debería ser igual al total que ICE gastó en el mundo real; sin embargo, cualquiera de los contratos vigentes que revisamos podrían cambiar en valor. Además, ICE envía los datos de sus gastos en adjudicaciones a las bases de datos del *Federal Procurement Data System* (Sistema Federal de Información de Adquisiciones), las cuales se comparten en USAspending. También cabe señalar que los errores de la agencia pueden derivar en errores en los valores reportados.[381] Nuestros datos están actualizados hasta septiembre de 2021.[382]

B. METODOLOGÍA

1. Resumen

Para identificar y analizar los gastos de ICE en tecnología de vigilancia, revisamos las transacciones de las adjudicaciones otorgadas por ICE enlistadas en USAspending, la fuente oficial de información de los gastos federales. Identificamos las operaciones de gastos que podrían haberse destinado en tecnologías de vigilancia y los catalogamos en seis funciones: geolocalización, biométrica, análisis de datos, agencias de datos, bases de datos gubernamentales y telecomunicaciones.[383]

2. Identificación de adjudicaciones de vigilancia.

Establecimos dos enfoques para identificar las adjudicaciones de vigilancia. Al usar el primer enfoque iniciamos una lista de herramientas de vigilancia conocidas e identificamos las adjudicaciones de ICE para esas herramientas. Con el segundo enfoque, empezamos con una serie de adjudicaciones de ICE y revisamos aquellas que sospechamos que eran para herramientas de vigilancia.

Para nuestro primer enfoque armamos una lista de los proveedores de vigilancia conocidos de ICE. Revisamos las *Privacy Impact Assessments* (Evaluaciones del Impacto de Privacidad, PIA por sus siglas en inglés) de ICE y el DHS, así como el *System of Record Notices* (Sistema de Avisos de Registros, SORN por sus siglas

en inglés), los cuales son unos de los pocos documentos sobre las iniciativas del DHS que dicho departamento muestra al público. Descargamos las PIA y los SORN de los archivos de los sitios web de DHS/ICE y leímos los documentos buscando menciones sobre las tecnologías cubiertas en nuestras categorías. Casi ninguna de las PIA o de los SORN estaban relacionados a un contrato en particular, sino que daban información general de las iniciativas existentes de ICE, proyectos y programas (ej., LeadTrac, RAVEN, VISA, etc). Posteriormente recabamos los nombres de los proveedores de vigilancia conocidos de ICE a partir de los informes publicados por organizaciones como NILC, *Mijente, TechInquiry* y *Top10VPN*.[384] Finalmente, realizamos búsquedas de palabras clave en los motores de búsqueda para identificar nombres de otros programas y tecnologías de vigilancia de ICE.

Para nuestro segundo enfoque, leímos miles de adjudicaciones y señalamos aquellas que sospechamos estaban vinculadas con funciones de vigilancia.[385] Señalamos adjudicaciones para software que contenían palabras clave relacionadas con la vigilancia (ej. biométricos), así como adjudicaciones marcadas dentro de una categoría posiblemente relacionada a la vigilancia (ej. que tenían un código de producto para "recuperación de información") o tenían otros campos distintivos. Posteriormente, realizamos búsquedas en línea de palabras clave de posibles contratos de vigilancia según su número de adjudicación de contrato, las compañías contratantes y el producto o servicio proporcionado. Esas búsquedas arrojaron sitios web de compañías, así como coberturas de medios e información adicional que nos ayudó a crear una lista de proveedores y sus productos de vigilancia.

En el caso de los proveedores que identificamos como proveedores de vigilancia, buscamos otras adjudicaciones que tuvieran con ICE usando su clave identificadora única, conocida como número DUNS. Luego revisamos cada una de las adjudicaciones de ICE a la compañía y añadimos las que coincidían con nuestras categorías de funciones. Si había casos en donde el proveedor vendía predominantemente tecnología que caía dentro del criterio de una de nuestras funciones, decidimos incluir todas las adjudicaciones de ICE en nuestra lista. Además, dado que ICE puede hacer más de una transacción para cualquier adjudicación, siempre que aparecía una operación de gastos asociada a una adjudicación posiblemente vinculada a la vigilancia, incluíamos la adjudicación completa en nuestra lista final.

3. Clasificación de las adjudicaciones.

Muchas de las adjudicaciones de ICE estaban vinculadas a las tecnologías que ofrecían múltiples funciones de vigilancia. Por ejemplo, ICE utiliza algunas tecnologías que abarcan diferentes categorías; como los simuladores de torres de telefonía celular, que interceptan las comunicaciones (interceptación de telecomunicaciones) para rastrear gente (geolocalización)[386] Para decidirnos dentro de qué función la catalogaríamos, recurrimos al producto etiquetado en el contrato o a la categoría de servicio. Las adjudicaciones de contratos eran códigos asignados tanto por el *North American Industry Classification System* (Sistema Norteamericano de Clasificación de la Industria, NAICS por sus siglas en inglés), que es un estándar federal para clasificar negocios,[387] como por el *Product Service Code* (código de servicio de producto, PSC por sus siglas en inglés), que es un estándar del Sistema Federal de Información de Adquisiciones, FPDS, para describir los productos y servicios.[388] Cuando

analizamos los contratos que entraban en alguna de nuestras clasificaciones de funciones, notamos patrones en los métodos de asignación de los códigos NAICS y PSC. Por ejemplo, el FPDS asignó el PSC "subscripción web" para muchos contratos de ICE que nosotros clasificamos como agencias de datos. Como resultado, cuando encontramos códigos PSC de "suscripción web", lo veíamos como un indicio de que la adjudicación podría clasificarse bajo la función de agencias de datos.

4. Análisis automatizado de contratos.

La revisión manual que hicimos de las transacciones de ICE arrojó un conjunto inicial de datos de las transacciones de vigilancia de ICE, pero el enfoque resultó intensivo en términos de tiempo. Para encontrar y evaluar aquellos contratos que podríamos haber pasado por alto en nuestra primera fase de revisión, nos apoyamos en un modelo diseñado para identificar contratos con una alta probabilidad de estar vinculados a actividades de vigilancia. Luego, revisamos manualmente cada contrato señalado digitalmente. El modelo complementó nuestra revisión manual y señaló a los proveedores, productos y servicios que no identificamos en nuestra primera fase por diferentes razones como, por ejemplo, ortografía irregular en la descripción de la adjudicación. Emplear este modelo a manera de apoyo en nuestro proceso no solo nos permitió analizar un número significativamente mayor de contratos, también pudimos identificar más casos de gastos vinculados a la vigilancia por parte de ICE.

5. Estandarización de los nombres de los proveedores.

- **Eliminación de los duplicados.**
  Con frecuencia, ICE carece de estándares para registrar los nombres de los destinatarios. Por ejemplo, puede registrar a un contratista como la Ciudad de Filadelfia como "filadelfia ciudad de", "filadelfia, ciudad de", o simplemente "Filadelfia". Para estandarizar los nombres de los destinatarios, usamos algoritmos de colisión de claves de Open Refine para detectar correspondencias poco claras y fusionar nombres.[389] Posteriormente, decidimos complementar las fusiones automatizadas por medio de correcciones manuales.

- **Enlistado de los proveedores según su empresa matriz.**
  Atribuir un contrato a un proveedor no siempre es un proceso simple. Algunas compañías disfrazan sus contratos con ICE al proporcionar sus servicios a través de empresas fantasmas o subordinadas. Las compañías también cambian sus nombres, adquieren o se fusionan con compañías más pequeñas. Para desenmarañar esta red, recurrimos a los destinatarios de las adjudicaciones a partir de los nombres actuales (hasta octubre de 2021) de sus empresas matrices. Para vincular a los proveedores con sus empresas matrices usamos un mapeo de proveedores desarrollado por TechInquiry.[390]

6. Cálculo de los gastos totales.

Nuestro reporte rastrea la cantidad acumulada que ICE gastó a lo largo de 12 años. Dado que las adjudicaciones no suelen registrar gastos acumulados en el contrato, decidimos recalcular los valores totales acumulados de todas las adjudicaciones de vigilancia. Para calcular la suma acumulada de los valores anuales de la adjudicación, sumamos las transacciones anuales de la misma; es decir, las "obligaciones de acción federal" en una suma acumulada.

7. Limitaciones.

a. Conteo inferior al número de contratos reales.

A riesgo de pecar de precavidos, es posible que hayamos hecho un conteo inferior del número real de contratos de vigilancia de ICE. Incluso tras una investigación significativa, no pudimos determinar si algunos contratos tenían fines de vigilancia que entraran en nuestras categorías. Por ejemplo, excluimos una compra de "escáneres"[391] realizada por ICE, ya que el proveedor vende tanto escáneres de imágenes como escáneres de huellas digitales.

b. Conteo superior al número de contratos reales.

También es posible que hayamos hecho un conteo mayor al número real de las adjudicaciones de vigilancia como consecuencia de las turbias prácticas informativas de ICE. La agencia rara vez muestra suficiente información que ofrezca detalles sobre lo que se está comprando, así como de la manera en cómo sus agentes usan estas herramientas. Por ejemplo, ICE describió una compra realizada como "necesaria para operaciones de vigilancia electrónica."[392] Esta adjudicación no solo es ambigua, sino que el vendedor tiene muchos tipos de tecnologías de vigilancia, incluyendo aquellas de las que nuestro reporte no está siguiendo la pista.[393]

c. Contratistas externos.

Nuestra revisión no desenmaraña los proveedores que vienen de contratistas externos. Por ejemplo, enlistamos un contrato de HART que adquiere los Amazon Web Services a nombre del contratista externo al que se le adjudicó inicialmente el contrato.[394]

APÉNDICE B:
LISTA DE CONTRATOS DE VIGILANCIA DE ICE Y ESTIMACIONES DE GASTOS.

Para ver la hoja de datos y cálculos, haga clic aquí por favor.

APÉNDICE C:
TEMPLETES DE SOLICITUDES DE EXPEDIENTES.

A. TEMPLETE DE SOLICITUDES PARA LOS DMV ESTATALES.

1. Solicitud para los registros de los DMV estatales en búsquedas directas y NLETS.

[Fecha]
[Dirección de la agencia]

Re.: Solicitud de expedientes

Funcionario de Expedientes Abiertos:

El *Center on Privacy & Technology*, un centro de estudio con base en la Facultad de Leyes de la Universidad de Georgetown está llevando a cabo una encuesta de departamentos vehiculares relacionada a las prácticas de compartición de información con otras agencias.

En virtud de [Ley Estatal de Solicitud de Expedientes y cita], solicitamos los siguientes expedientes.

Expedientes solicitados

Favor de proporcionar copias de los siguientes expedientes relacionados con la compartición de datos desde 2015:

1. Solicitudes emitidas por el Servicio de Inmigración y Control de Aduanas de los Estados Unidos sobre datos de conductores, incluyendo solicitudes para obtener los datos domiciliarios de los conductores.

2. Acuerdos o memorándums de entendimiento firmados por ICE o por el Departamento de Seguridad Nacional de los Estados Unidos relacionados al acceso a información de conductores, incluyendo acceso a los datos domiciliarios de éstos.

3. Documentos de políticas, incluyendo guías, manuales o memorándums que contengan procedimientos para usar NLETS para compartir información de los conductores, incluyendo sus datos domiciliarios.

La presente solicitud proviene de una organización sin fines de lucro cuya misión es la de avanzar en el campo de las políticas de privacidad y tecnología, así como entrenar en este ámbito a estudiantes de leyes de todo el condado. Dado nuestro estatus sin fines de lucro y el hecho de que esta solicitud es acerca de un asunto de interés público, solicitamos una exención de pago. En caso de que dicha exención sea denegada, favor de informarnos por adelantado si el costo excederá los $50.

De acuerdo con la [Ley Estatal de Solicitud de Expedientes], un custodio de los expedientes públicos deberá responder a la solicitud [dentro de X días hábiles a partir de la fecha recepción del documento/periodo especificado por la ley]. Favor de enviar los documentos de respuesta a [nombre y información de contacto] o a:

[dirección de correo postal]

Si tienen alguna pregunta o no pueden responder a esta solicitud dentro del periodo reglamentario, o si esta solicitud ha llegado a la dirección equivocada, favor de contactarme en la dirección [información de contacto]. Gracias por la pronta atención a este asunto.

Sinceramente,
[nombre]

2. Templete de solicitud para los expedientes de los DMV estatales para información sobre el acceso a la base de datos y a las búsquedas de reconocimiento facial.

[Fecha]
[Dirección de la agencia]

Re.: Solicitud de Expedientes

Funcionario de Expedientes Abiertos:

El *Center on Privacy & Technology*, un centro de estudio con base en la Facultad de Leyes de la Universidad de Georgetown, está llevando a cabo una encuesta sobre la compartición de información entre las agencias estatales y las agencias de datos.

En virtud de [Ley Estatal de Solicitud de Expedientes y cita], solicitamos los siguientes expedientes.

Expedientes solicitados

Favor de proporcionar copias de los siguientes expedientes relacionados al reconocimiento facial desde 2015:

1. Solicitudes emitidas por el Departamento de Seguridad Nacional de los Estados Unidos, incluyendo sus componentes, como el Servicio de Inmigración y Control de Aduanas y la Oficina de Aduanas y Protección Fronteriza, para llevar a cabo búsquedas de reconocimiento facial o accesos internos que hayan registrado búsquedas de reconocimiento facial por parte del DHS, así como cualquier otro material enviado al DHS en respuesta de estas solicitudes y/o búsquedas.

2. Acuerdos o memorándums de entendimiento firmados con el Departamento de Seguridad Nacional de los Estados Unidos), incluyendo sus componentes, como el Servicio de Inmigración y Control de Aduanas y la Oficina de Aduanas y Protección Fronteriza que permitieran a la agencia realizar o solicitar búsquedas de reconocimiento facial.

Favor de proporcionar copias de los siguientes expedientes relacionados con la compartición de datos con agencias de datos desde 2015:

3. Documentos de contrataciones, incluyendo órdenes de compras, facturas, acuerdos de licencias, acuerdos de confidencialidad, o cualquier otra adquisición, servicios o acuerdos de mantenimiento con Giant Oak, IHS Markit (anteriormente d/b/a RL Polk), Thomson Reuters (incluyendo su subsidiaria, West Publishing Corporation) y RELX (incluyendo su subsidiaria, LexisNexis).

4. Materiales de mercadotecnia que anuncien productos o servicios ofrecidos por Giant Oak, IHS Markit (anteriormente d/b/a RL Polk), Thomson Reuters (incluyendo su subsidiaria, West Publishing Corporation) y RELX (incluyendo su subsidiaria, LexisNexis).

La presente solicitud proviene de una organización sin fines de lucro cuya misión es la de avanzar en el campo de las políticas de privacidad y tecnología, así como entrenar en este ámbito a estudiantes de leyes de todo el condado. Dado nuestro estatus sin fines de lucro y el hecho de que esta solicitud es acerca de un asunto de interés público, solicitamos una exención de pago. En caso de que dicha exención sea denegada, favor de informarnos por adelantado si el costo excederá los $50.

De acuerdo con la [Ley Estatal de Solicitud de Expedientes], un custodio de los expedientes públicos deberá responder a la solicitud [dentro de X días hábiles a partir de la fecha de recepción del documento/ periodo especificado por la ley]. Favor de enviar los documentos de respuesta a [nombre y información de contacto] o a:

[dirección de correo postal]

Si tienen alguna pregunta o no pueden responder a esta solicitud dentro del periodo reglamentario, o si esta solicitud ha llegado a la dirección equivocada, favor de contactarme en en la dirección [información de contacto]. Gracias por la pronta atención a este asunto.

Sinceramente,
[nombre]

B. TEMPLETE DE SOLICITUDES A PROVEEDORES DE SERVICIOS PÚBLICOS.

[Fecha]
[Dirección de la agencia]

Re.: Solicitud de Expedientes

Funcionario de Expedientes Abiertos:

El *Center on Privacy & Technology*, un centro de estudio con base en la Facultad de Leyes de la Universidad de Georgetown, está llevando a cabo una encuesta sobre las compañías de servicios públicos y la venta o transferencia de información sobre sus clientes a agencias de información crediticia.

En virtud de [Ley Estatal de Solicitud de Expedientes y cita], solicitamos los siguientes expedientes.

Expedientes solicitados

Favor de proporcionar copias de los siguientes expedientes desde 2015:

1. Documentos de contratación, incluyendo órdenes de compra, facturas, acuerdos de licencias, acuerdos de confidenciales, u otra correspondencia, adquisición, servicio o acuerdos de mantenimiento con Equifax, Experian, y Transunion.

2. Documentos de políticas, incluyendo guías, manuales u otros memorándums que contengan procedimientos para realizar verificaciones crediticias o una verificación de identidad de algún cliente potencial o existente.

La presente solicitud proviene de una organización sin fines de lucro cuya misión es la de avanzar en el campo de las políticas de privacidad y tecnología, así como entrenar en este ámbito a estudiantes de leyes de todo el condado. Dado nuestro estatus sin fines de lucro y el hecho de que esta solicitud es acerca de un asunto de interés público, solicitamos una exención de pago. En caso de que dicha exención sea denegada, favor de informarnos por adelantado si el costo excederá los $50.

De acuerdo con la [Ley Estatal de Solicitud de Expedientes], un custodio de los expedientes públicos deberá responder a la solicitud [dentro de X días hábiles a partir de la fecha de recepción del documento/ periodo especificado por la ley]. Favor de enviar los documentos de respuesta a [nombre y información de contacto] o a:

[dirección de correo postal]

Si tienen alguna pregunta o no pueden responder a esta solicitud dentro del periodo reglamentario, o si esta solicitud ha llegado a la dirección equivocada, favor de contactarme en la dirección [información de contacto]. Gracias por la pronta atención a este asunto.

Sinceramente,
[nombre]

APÉNDICE D: PROVEEDORES DE SERVICIOS PÚBLICOS QUE PROBABLEMENTE HAYAN PARTICIPADO EN NCTUE.

1. AT&T[395]
2. DIRECTV[396]
3. Verizon[397]
4. Sprint[398]
5. Citizens Communications Inc. (now Frontier)[399]
6. Broadwing Communications Inc.[400]
7. Dish Network[401]
8. American Electric Power[402]
9. Baltimore Gas & Electric[403]
10. Southern Company[404]
11. Georgia Power[405]
12. PSNC Energy (now North Carolina Gas)[406]
13. Scana Energy[407]
14. Piedmont Natural Gas[408]
15. Citizens Energy[409]
16. Nevada Energy[410]
17. Consumers Energy Company[411]
18. Miami-Dade County Water and Sewer Department[412]

Las evidencias también indican que los siguientes proveedores de servicios públicos no han sido o ya no son miembros de NCTUE:

1. Duke Energy[413]
2. Minnesota Energy Resource Corporation[414]

NOTA DE TRADUCCIÓN

El objetivo del presente reporte es dar a conocer a la audiencia el origen, funcionamiento, e impacto de las redes de arrastre americanas, así como las medidas que podrían implementarse para frenarlas. Debido a su naturaleza informativa, y dado que no se sabe con certeza qué grupos, asociaciones o personas (especializadas o no en el campo de las leyes y defensa de los derechos humanos) puedan valerse de este reporte para avanzar en sus propias actividades, el criterio de traducción prevalente ha sido el de explicitar conceptos y traducir en su mayoría—de manera informal—nombres de agencias, comités, leyes, estatutos, etc. para así asegurar el mayor entendimiento por parte de la audiencia, sin importar su formación, procedencia o contexto. Aunque la extensión y complejidad del tema no facilita el uso del lenguaje inclusivo, la presente traducción reconoce la necesidad de éste y aspira a que en un futuro el idioma siga evolucionando para que su uso sea aceptado y comprendido en todo tipo de documentos, independientemente de su contenido o formalidad.

En cuanto a los criterios de traducción. El cuerpo del texto menciona los nombres de las agencias en ambos idiomas, con el inglés en cursiva y español entre paréntesis solo la primera vez que se mencionan. Después de esta primera mención, estos nombres aparecen en español a lo largo de todo el cuerpo del texto. Han permanecido en español, sin necesidad de nombrar su título en inglés, aquellas agencias, leyes o entidades cuyos nombres cuentan con una traducción oficial o su nombre traducido informalmente ya es de dominio público. Los nombres que no son posibles de traducir permanecen en cursivas. Por otro lado, en las notas al pie, los nombres de todas las agencias, leyes y entidades sí han permanecido en inglés, ya que aparecen adjuntas a hipervínculos o documentos adjuntos que funcionan como pruebas argumentativas.

En el caso particular de consultas, solicitudes, memorándums de acuerdos, testimonios o cartas de respuestas que aparecen al pie del texto, las referencias han sido parcialmente traducidas para su comprensión, pero no en su totalidad para que no se desvinculen como pruebas. En el caso de contratos, acuerdos, audiencias, artículos o libros sin traducción oficial, las referencias permanecen en inglés.

AGRADECIMIENTOS

Este reporte no habría sido posible sin la poderosa búsqueda y defensa de nuestros amigos y aliados cuyo objetivo es exponer las redes de vigilancia y arrastre de ICE. Estamos profundamente agradecidos por el trabajo de organizaciones como 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 y muchas más.

El profesor David Vladeck, director del cuerpo docente de este centro, nos brindó una guía invaluable y una lectura concienzuda de este reporte. También agradecemos a los revisores externos, incluyendo a Heidi Altman, Tanya Broder, Joan Friedland, McKenzie Funk, Anil Kalhan, Sarah Kim Pak, Julie Mao, Jack Poulson, Vasudha Talla así como a varios más que permanecerán en el anonimato por darnos sus valiosas aportaciones durante todo el proceso de redacción. Los revisores no están necesariamente de acuerdo con los temas abordados en este reporte.

Asimismo, este reporte no sería posible sin todo el equipo del Centro, quienes ayudaron de muchas maneras: Katie Evans, Clare Garvie, Cynthia Khoo, Laura Moy, Korica Simon, Jameson Spivack, y Serena Zets. También agradecemos a los asistentes de investigación del centro, pasantes y compañeros de verano, incluyendo a Daniel Barabander y Romina Montellano Morales; Ashley Burke, Augusto Cividini, Dana Holmstrand, Jeremy Penn, Jesús Rodríguez y Natalie Tverdynin; a nuestro corrector, Joy Metcalf; a nuestra firma de diseño y desarrollo web, Rootid, así como a nuestra casa de traducción, Sirena Peligro.

El Center on Privacy & Technology de Georgetown Law (Centro de Privacidad y Tecnología de Georgetown) cuenta con el apoyo de la Ford Foundation (Fundación Ford), la Kresge Foundation (Fundación Kresge), la Open Society Foundations (las Fundaciones Open Society), la MacArthur Foundation (Fundación MacArthur), Luminate, el Media Democracy Fund (el Fondo para la Democracia de los Medios), la Seldin/Haring-Smith Foundation (la Fundación Seldin/Haring-Smith), y Georgetown University Law Center (la Facultad de Leyes de la Universidad de Georgetown).

NOTAS FINALES

1. 148 Cong. Rec. S8046 (edición diaria 3 de septiembre, 2002) (comentarios del Sen. Robert Byrd). Esta introducción incorpora elementos de Álvaro Bedoya, Watching Immigrants, Harv. Nat'l Sec. J. (disponible 2022). El Profesor Bedoya no ha revisado o aprobado este informe.

2. 147 Cong. Rec. S11059 (edición diaria 25 de octubre, 2001) (Sen. Feingold como el único "no" en la votación final de 98-1).

3. Ver John Tierney, THREATS AND RESPONSES: THE SENATE; Byrd, at 85, Fills the Forum With Romans and Wrath, New York Times (20 de noviembre, 2002) (que describe al Sen. Byrd y su oposición "virtualmente solitaria" al proyecto de ley); Pork or Progress? Sen. Byrd Leaves Legacy, CBS News & Associated Press, 28 de junio, 2010 (sobre el legado de partidas presupuestarias conseguidas por el Sen. Byrd para Virginia del Oeste).

4. Id. Ver también Temporary Relocation of the Coast Guard National Maritime Center (NMC), 72 Fed. Reg. 58,865 (17 de octubre, 2007) (mudanza de Arlington, Va. a Kearneysville, W.Va.); Permanent Relocation of the Coast Guard National Maritime Center (NMC), 73 Fed. Reg. 12,747 (10 de marzo, 2008) (mudanza a Martinsburg, W.Va.).

5. Ver, en lo general, 148 Cong. Rec. S11358-113560 (edición diaria 19 de noviembre, 2002) (comentarios del Sen. Byrd en oposición a la Homeland Security Act del 2002).

6. Id at S11359.

7. Id.

8. 148 Cong. Rec. S8045 (edición diaria 3 de septiembre, 2002).

9. Ver 148 Cong. Rec. S11359 (edición diaria 19 de noviembre, 2002) ("cámara masiva de secretos"). Ver también 148 Cong. Rec. S8047-8048 (edición diaria 3 de septiembre, 2002) (con respecto a las excepciones a la Federal Advisory Committee Act y la Freedom of Information Act, la falta de independencia del inspector general del DHS, y describiendo a los funcionarios de privacidad y derechos civiles del DHS como "consejeros sin ningún poder real de investigación o ejecución").

10. 148 Cong. Rec. S11359 (edición diaria 19 de noviembre, 2002).

11. El que la vigilancia y las redes de arrastre fueran consecuencias previsibles de la Homeland Security Act no significa que la HSA debería leerse como una autorización de las prácticas de vigilancia descritas en este informe. Ver, en lo general, Anil Kalhan, Immigration Surveillance, 74 Md. L. Rev. 1 (2014).

12. 148 Cong. Rec. S8046 (edición diaria 3 de septiembre, 2002).

13. 148 Cong. Rec. S11360 (edición diaria 19 de noviembre, 2002).

14. Id. at S11462.

15. Ver Tierney, supra nota 3.

16. Personal Information, State and Local Agencies, Restrictions on Access: Hearing on H.B. 23 Before the Md. H. of Delegates Judiciary Committee (27 de enero, 2021) (declaración de Alex Vazquez de 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 (al minuto 46:33, "muerte segura").

17. Erin Cox, Gov. Hogan opposed to ending ICE's warrantless access to driver's license database, Washington Post (27 de febrero, 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. Ver id.

19. Ver Drew Harwell, ICE has run facial recognition searches on millions of Maryland drivers, Washington Post (26 de febrero, 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 (26 de febrero, 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. El término licencia "estándar" se usa en Maryland para diferenciar esos documentos de identidad de las licencias que cumplen con los requisitos de la ley federal REAL ID, que requieren una verificación del estatus migratorio. El depósito de reconocimiento facial, la Maryland Image Recognition System, o MIRS, incluye todas las fotografías de los conductores sin reparar en el tipo de licencia. 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 millones de conductores con licencia en 2018).

20. Ver Cox, supra nota 17.

21. Ver Carta de Kevin Combs, Md. Dep't of Public Safety and Corr. Servs. a Sen. Susan C. Lee et al., 21 de noviembre, 2019 (explicando, en respuesta a una consulta de los legisladores con respecto al número de tales búsquedas, que Maryland no tiene acceso a los resultados de búsqueda de los usuarios y, en lugar de eso, se ofrece dar a conocer el número de "sesiones [que] fueron guardadas" por los usuarios de ICE en 2018 y 2019).

22. Ver, en lo general, infra Hallazgo 2.

23. Ver Vasudha Talla, Documents Reveal ICE Using Driver Location Data from Local Police Departments, ACLU NorCal (13 de marzo, 2019), https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data ("Vigilant saca su información de las licencias de manejo de 'las 5 áreas metropolitanas más pobladas' en el país, correspondientes a casi 60 por ciento de la población de EE.UU.").

24. Ver, en lo general, infra Hallazgo 3.

25. Ver, en lo general, infra Hallazgo 4.

26. Ver, i.e., U.S. Immigration and Customs Enforcement, ICE announces results of latest operations targeting criminal aliens (1 de septiembre, 2020), https://www.ici.eov/news/releases/ice-announces-results-latest-operations-targeting-criminal-aliens ("[a]l enfocar nuestros esfuerzos en los perpetradores de crímenes contra la gente, podemos retirar esas amenazas de nuestras comunidades e impedir que ocurran futuras víctimas. A través de nuestros esfuerzos de control enfocados, estamos deshaciéndonos de la amenaza generada por esos criminales, muchos de los cuales son delincuentes reincidentes."

27. Como adulto joven, Robert Byrd organizó una facción del Ku Klux Klan. Como senador joven, se hizo un nombre oponiéndose a las leyes de los derechos civiles. Como senador mayor, sin embargo, estaba profundamente avergonzado de eso y se convirtió en un acérrimo defensor de la Voting Rights Act y otras leyes clave de los derechos civiles. Esta gracia, desafortunadamente, nunca se extendió a personas como el señor Hernández. De hecho, el senador Byrd habló acaloradamente en contra de los esfuerzos de otorgar a los indocumentados un camino a la ciudadanía. En sus comentarios en la cámara del Senado durante un debate sobre la inmigración, advirtió que "cualquiera" de esos "extranjeros indocumentados, no verificados… podría ser un terrorista potencial". No obstante, independientemente de su historia o sus motivaciones, la advertencia del senador Byrd ha resultado ser aterradoramente acertada. 109 Cong. Rec. S2794 (edición diaria 4 de abril, 2006) (declaración del Sen. Robert Byrd).

28. Ver, en lo general, 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 (26 de febrero, 2021), https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data.

30. Ver Drew Harwell, Utility giants agree to no longer allow sensitive records to be shared with ICE, Washington Post (8 de diciembre, 2021), https://www.washingtonpost.com/technology/2021/12/08/utility-data-government-tracking/; Carta de Ron Wyden, U.S. Senator a Hon. Rohit Chopra, Director, Consumer Financial Protection Bureau 1 (8 de diciembre, 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; @JustFuturesLaw, Twitter (8 de diciembre, 2021), https://twitter.com/JustFuturesLaw/status/1468590605668425729?s=20.

31. Ver Carta de Ron Wyden, U.S. Senator a Hon. Rohit Chopra, Director, Consumer Financial Protection Bureau 2 (8 de diciembre, 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 (28 de noviembre, 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 (12 de marzo, 2021), https://www.dhs.gov/news/2021/03/12/hhs-and-dhs-joint-statement-termination-2018-agreement.

35. Aunque el gobernador de Maryland, Larry Hogan, vetó ambos proyectos de ley en mayo de 2021, la Asamblea General de Maryland anuló el veto en diciembre de ese año. Clara Garcia, Maryland General Assembly Overrides Hogan's Vetoes of Immigration Bills, NBC Washington (8 de diciembre, 2021), https://www.nbcwashington.com/news/local/maryland-general-assembly-overrides-hogans-vetoes-of-immigration-bills/2904771/.

36. Por ejemplo, el Criminal Alien Program (CAP) manda a funcionarios de ICE a las cárceles para entrevistar a personas detenidas para determinar si pueden ser deportables. Los funcionarios de CAP no distinguen entre personas detenidas de manera preventiva y los que han sido condenados por un crimen. De hecho, un número significativo de personas removidas bajo CAP no tenían condenas criminales. Ver Guillermo Cantor, Mark Noferi & Daniel E. Martinez, Enforcement Overdrive: A Comprehensive Assessment of ICE's Criminal Alien Program, American Immigration Council 2 (1 de noviembre, 2015), https://www.americanimmigrationcouncil.org/sites/default/files/research/enforcement_overdrive_a_comprehensive_assessment_of_ices_criminal_alien_program_final.pdf ("De más de medio millón de remociones bajo CAP que tuvieron lugar entre el año fiscal 2010 y el año fiscal 2013, ICE clasificó la cantidad mayor (27.4 por ciento) como "no totalmente criminales"—i.e., ICE no registró ninguna condena criminal.").

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.ici.eov/doclib/foia/secure_communities/securecommunitiesstrategicplan09.pdf (A través del despliegue y uso de sistemas de identificación basados en la biometría, todas las personas acusadas de un crimen y llevadas bajo custodia serán automáticamente verificadas en cuanto a su estatus migratorio, así como a sus antecedentes criminales.)

38. Este informe distingue entre datos del law enforcement (del ámbito de seguridad) y non-law enforcement (externas al ámbito de seguridad), pero debido a la creciente interoperabilidad de las bases de datos y redes en todos los niveles y poderes del gobierno, como asunto práctico podría tener más sentido empezar a pensar en todos los datos como información potencial para el ámbito de seguridad.

39. Ver, en lo general, 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) ("Las cárceles y los centros de detención hacinados motivaron a los legisladores a proponer medidas para deportar a los alien felons (extranjeros criminales) para liberar camas . . . Las penas mínimas obligatorias alimentaron el hacinamiento; pero el Congreso definió el problema como una falta de camas . . . legisladores y funcionarios declararon ante el Congreso que podrían 'casi resolver el hacinamiento de nuestras cárceles si el gobierno federal hace lo que tiene que hacer para tomar a estos criminales y deportarlos.'"); Immigration Reform and Control Act del 1986, Pub. L. No. 99-603, § 701,100 Stat. 3445 (requiriendo al Fiscal General "en el caso de un alien que es condenado por un crimen, el cual lo hace sujeto a la deportación . . . [a] iniciar cualquier deportación, procediendo tan diligentemente como sea posible a partir de la fecha de la condena."); William A. Kandel, Cong. Rsch. Serv., R44627, Interior Immigration Enforcement: Criminal Alien Programs 23 (2016) (se discute cómo el INS ejecutó su mandato en el Congreso al establecer el Institutional Removal Program (IRP) y el Alien Criminal Apprehension Program (ACAP) para las deportaciones dirigidas a los inmigrantes criminales).

41. En el 1988, el Congreso creó una categoría de crímenes conocidos como aggravated felonies (crímenes agravados). Al momento de su creación, incluían sólo crímenes como homicidio o tráfico de armas de fuego y drogas, pero la definición de aggravated felony se vió ampliada considerablemente por el Congreso entre1990 y 1996 con la aprobación de una serie de medidas; de manera más notable la Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA), para incluir otros motivos para la deportación, con una aplicación retroactiva. Kandel, supra nota 40 al 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). Ver también Cong. Rsch. Serv., RL32480, Immigration Consequences of Criminal Activity 3-5 (2009).

42. Ver 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 (30 de julio, 2021) ("Antes de mediados de los años 1990 el número anual de deportaciones no había excedido 50,000 durante décadas, pero con la aprobación de la ley de 1996 este umbral fue traspasado, y para principios del siglo las deportaciones estaban a un nivel de poco menos de 200,000 por año.").

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

44. Ver Marc R. Rosenblum & William A. Kandel, Cong. Rsch. Serv., R42057, Interior Immigration Enforcement: Programs Targeting Criminal Aliens 11-17 (2012); id. al 16 ("Más de la mitad (32 of 57) de los acuerdos §287(g) identificados en diciembre del 2012 son acuerdos de operación en las cárceles."); The 287(g) Program: An Overview, American Immigration Council (8 de julio, 2012), https://www.americanimmigrationcouncil.org/research/287g-program-immigration ("Para junio de 2020, había 76 MOAs modelo active jail enforcement en 21 estados y 65 MOAs modelo warrant service officer en nueve estados.").

45. U.S. Immigration and Customs Enforcement, Secure Communities: A Comprehensive Plan to Identify and Remove Criminal Aliens 1-2 (2009), https://www.ici.eov/doclib/foia/secure_communities/securecommunitiesstrategicplan09.pdf (A través del despliegue y uso de sistemas de identificación basados en la biometría, todas las personas acusadas de un crimen y retenidas bajo custodia serán automáticamente verificadas en cuanto a su estatus migratorio, así como en sus antecedentes criminales.)

46. Julia Preston, States Resisting Program Central to Obama's Immigration Strategy, New York Times (5 de mayo, 2011), https://www.nytimes.com/2011/05/06/us/06immigration.html ("Las objeciones de los estados están fomentando una confrontación con el Department of Homeland Security, cuya secretaria, Janet Napolitano, ha dicho que Secure Communities es obligatorio y será extendido a todas las demarcaciones del país para el 2013.").

47. U.S. Immigration and Customs Enforcement, Secure Communities (9 de febrero, 2021), https://www.ici.eov/secure-communities ("ICE finalizó la implementación total de Secure Communities en todas las 3,181 demarcaciones en los 50 estados, el Distrito de Columbia y cinco territorios estadounidenses el 22 de enero, 2013.").

48. Ver Carta de Jeh Charles Johnson, Secretary, U.S. Department of Homeland Security a Thomas S. Winkowski, Acting Director, U.S. Immigration and Customs Enforcement et al. 2–3 (20 de noviembre, 2014), https://www.dhs.gov/sites/default/files/publications/14_1120_memo_secure_communities.pdf ("Por consiguiente, ordeno a U.S. Immigration and Customs Enforcement (ICE) descontinuar Secure Communities. ICE debería poner en su lugar un programa que continuará dependiendo de los datos biométricos basados en huellas digitales entregados durante los arrestos por las agencias de seguridad estatales y locales al Federal Bureau of Investigation para la verificación de antecedentes criminales . . . Este nuevo programa debería referirse como el 'Priority Enforcement Program' o 'PEP.'").

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

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

51. En el año fiscal 2011, el número de remociones bajo S-Comm fue 79,726. TRAC, Removals under the Secure Communities Program (2019), https://trac.syr.edu/phptools/immigration/secure/. (En total, ICE ERO removió a 396,906 individuos durante el año fiscal 2011.) U.S. Immigration and Customs Enforcement, FY 2011:

ICE announces year-end removal numbers, highlights focus on key priorities (17 de octubre, 2011), https://www.ici.eov/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. Estas cifras también podrían reflejar el hecho de que las estadísticas de remociones empezaran a incluir deportaciones en la frontera. Ver Bethania Palma & David Mikkelson, Were More People Deported Under the Obama Administration Than Any Other?, Snopes (20 de octubre, 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 (9 de abril, 2019), https://www.dhs.gov/immigration-statistics/yearbook/2017/table39.

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

56. Ver National Immigration Law Center, NLETS: Questions and Answers 13 (noviembre 2020), https://www.nilc.org/wp-content/uploads/2020/11/NLETS-Q-and-A.pdf ("El NCIC es una base de datos del FBI que contiene, según el FBI, un centro de información electrónico de datos de crímenes al que pueden acceder virtualmente casi todas las agencias de justicia criminal en la nación, 24 horas al día, 365 días al año.' A pesar de la clasificación del NCIC por el FBI como una base de datos criminal, también incluye registros de inmigración civil, como registros de órdenes previas de remoción/deportación.

57. En Chae Chan Ping v. United States, la Suprema Corte estableció el principio de deferencia a los poderes ejecutivo y legislativo en asuntos de control migratorio, formando la base de la doctrina de los plenos poderes. Ver, en lo general, 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. Ver 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) ("Los funcionarios de deportación de la Office of Detention and Removal Operations siempre han detenido a los aliens fugitivos de manera ad hoc, pero no se establecieron equipos exclusivos para esta actividad."). Dos esfuerzos para cambiar eso a finales de los 1990 no tuvieron éxito. Id. ("El plan contempló la creación de abscondee removal teams y la ley de partidas presupuestarias de 1996 otorgó financiamiento para estos nuevos puestos… los puestos fueron absorbidos como parte de las operaciones día-a-día de detención y deportación del INS… [otra] iniciativa contempló la creación de Fugitive Operations Teams … pero ningún equipo fue establecido para este fin en ningún momento."); 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 (septiembre 2005) ("Como esfuerzo para reducir el número de extranjeros ilegales residiendo en Estados Unidos que habían violado los términos de cierto tipo de visas, ICE estableció la [Compliance Enforcement Unit (CEU)] en junio del 2003"); Visa Overstays: Can They Be Eliminated?: Hearing Before the House Committee on Homeland Security, 111th Cong. 11 (2010) (declaración de John T. Morton, Assistant Secretary, U.S. Immigration and Customs Enforcement, Department of Homeland Security) (CEU fue "el primer programa nacional dedicado al control de violadores de visas no inmigrantes.").

59. Memorándum de Michael R. Bromwich, Inspector General, Department of Justice, a Doris Meissner, Commissioner, Immigration and Naturalization Service (4 de septiembre, 1997), https://oig.justici.eov/sites/default/files/legacy/reports/INS/e9708/i9708p1.htm ("Históricamente, el asunto de permanecer más tiempo de lo permitido en las visas no ha sido una consideración principal en la formulación y ejecución de la política migratoria.").

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 (marzo 1996), https://oig.justici.eov/reports/INS/e9603/index.htm ("Los Aliens no detenidos que no cumplen con una solicitud de rendición rara vez son perseguidos activamente . . . Ha sido una política nacional que los investigadores [de INS] no trabajen casos de abscondees, excepto si un abscondee les llama la atención como parte de una investigación más amplia."). Esto no parecía molestar a los funcionarios migratorios en ese entonces. En 1994, cuando la directora del INS, Doris Meissner, fue entrevistada al respecto por el Times, dijo que "[no]sotros no tenemos éxito cuando se trata de la remoción, en líneas generales." Deborah Sontag, Porous Deportation System Gives Criminals Little to Fear, New York Times (13 de septiembre, 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 (febrero 2003), https://oig.justici.eov/reports/INS/e0304/final.pdf ("El INS define absconders como aliens con órdenes finales de remoción sin ejecutar y cuyos paraderos son desconocidos. La mayoría de los absconders son aliens no detenidos.")

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

63. Alien Registration Act, Pub. L. No. 76-670,54 Stat. 670 (1940). Ver U.S. Gov't Accountability Office, GAO-03-188, Homeland Security: INS Cannot Locate Many Aliens Because It Lacks Reliable Address Information (resumen de los cambios a la ley de 1940-2002, todos los cuales mantuvieron algún tipo de requisito de actualizar direcciones). Los requisitos para actualizar direcciones siguen en vigor hasta hoy. U.S. Citizenship and Immigration Services, Change of Address, https://egov.uscis.gov/coa/displayCOAForm.do ("Excepto para los que tienen excepciones, todos los aliens en EE.UU. son obligados a reportar cualquier cambio de dirección o dirección nueva.").

64. Ver U.S. Gov't Accountability Office, GAO-03-188, supra nota 63, al 12-13 (pobre cumplimiento y aplicación de los requisitos de reportar direcciones); Memorándum de

Michael R. Bromwich a Doris Meissner, supra nota 59, al 1 ("Sin embargo, los datos del [Non-Immigrant Información System] son inadecuados para permitir al INS identificar, localizar y arrestar los individuos que han permanecido más tiempo de lo permitido en sus visas.").

65. U.S. Department of Justice, Office of the Inspector General, Rep. No. I-96-03, supra nota 60, al 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) ("El resultado fue una redada atroz, dirigida por el gobierno y enfocada de manera aplastante a individuos musulmanes y árabes.").

68. Memorándum de Larry Dean Thompson, Deputy Attorney General, Department of Justice, al Commissioner, Immigration and Naturalization Service et al. (25 de enero, 2002), https://www.shusterman.com/pdf/absconderapprehensioninitiative.pdf; U.S. Department of Homeland Security, Office of the Inspector General, OIG-07-34, supra nota 58, al 1.

69. Kevin Lapp, supra nota 67, al 583–85.

70. Memorándum de Larry Dean Thompson, supra nota 68.

71. U.S. Gov't Accountability Office, GAO-03-188, supra nota 63, al 13 ("De los aproximadamente 314,000 aliens con órdenes finales de remoción todavía prófugos en Estados Unidos, INS identificó 5,046 que eran de países en los que ha habido la presencia o actividad terrorista de Al Qaeda. Para localizar y detener a esos aliens, el INS, en conjunto con el FBI, el Foreign Terrorist Tracking Task Force, y los fiscales de EE.UU., usaron los datos de direcciones del INS y los complementaron con la información de direcciones en las bases de datos de fuentes públicas. Según un alto funcionario del INS, hasta el 24 de junio del 2002, 4,334, u 86 por ciento, de los 5,046 alien absconders no habían sido detenidos, mientras que 712, o 14 por ciento, habían sido detenidos.").

72. Id. al 12–16 (El ejemplo AAI "ilustra una limitación intrínseca de un requisito de reportar direcciones que depende del autoinforme, ya que la confiabilidad y completitud de la información de direcciones depende del grado en que los aliens cumplen con el requisito de reportar… La falta de publicidad, la no aplicación de los castigos por no realizar la notificación de cambio de dirección, y los inadecuados procedimientos y controles de procesamiento explican, en parte, por qué la información de las direcciones de los aliens del INS no es fiable."); id. al 25 (recomendando "comprar información de direcciones de fuentes comercialmente disponibles").

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. al 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 (septiembre 2005); Industry Day, National Security Investigations Division, Department of Homeland Security 9 (31 de octubre, 2017), https://www.brennancenter.org/sites/default/files/Industry%20Day%20Presentation_0.pdf (haciendo referencia a la modificación del nombre del CEU a CTCEU).

76. Esta cifra no incluye el costo de los programas pagados por otras agencias y usados por ICE.

77. Mobilcomm, Vigilant Solutions (visitada por última vez el 13 de enero, 2022), https://www.mobilcomm.com/vigilant-solutions/.

78. Ver Carta de U.S. Immigration and Customs Enforcement a Vasudha Talla 75 (13 de julio, 2017), https://www.documentcloud.org/documents/5767094-ALPR-documents-from-ICE-FOIA.html.

79. Id.

80. Id. al 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. *Ver también* Vasudha Talla, *Documents Reveal ICE Using Driver Location Data from Local Police Departments,* ACLU NorCal (13 de marzo, 2019), https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data.

81. Ver Carta de U.S. Immigration and Customs Enforcement a Vasudha Talla 83 (13 de julio, 2017), https://www.documentcloud.org/documents/5767094-ALPR-documents-from-ICE-FOIA.html.

82. Charles Levinson, Through apps, not warrants, 'Locate X' allows federal law enforcement to track phones, Protocol (5 de marzo, 2020), https://www.protocol.com/government-buying-location-data ("En septiembre de 2018, funcionarios de ICE firmaron un contrato de un año por $1.1 millones con Babel Street. El acuerdo incluyó Locate X, según un exempleado de Babel Street. En agosto pasado, ICE firmó un nuevo acuerdo de cinco años con un valor de hasta $6.5 millones con Babel Street por 'servicios de suscripción de datos,' según registros."); USAspending, Contract Summary: THUNDERCAT TECHNOLOGY, LLC, https://www.usaspending.gov/award/CONT_AWD_70CMSD18FR0000226_7012_HSHQDC13D00002_7001.

83. Russell Brandom, Exclusive: ICE is about to start tracking license plates across the US, Verge (26 de enero, 2018), https://www.theverge.com/2018/1/26/16932350/ice-immigration-customs-license-plate-recognition-contract-vigilant-solutions.

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 (18 de enero, 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 (Consultada el 26 de noviembre, 2021); Thomson Reuters, CLEAR for know your vendor, https://legal.thomsonreuters.com/en/products/clear-investigation-software/know-your-vendor (visitada por última vez el 26 de noviembre, 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 (2 de abril, 2021), https://theintercept.com/2021/04/02/ice-database-surveillance-lexisnexis.

89. En total, 16 estados y el Distrito de Columbia han promulgado leyes que permiten a los inmigrantes no autorizados obtener licencias de manejo: California, Colorado, Connecticut, Delaware, Hawái, Illinois, Maryland, Nevada, Nueva Jersey, Nuevo México, Nueva York, Oregón, Utah, Vermont, Virginia y Washington. National Conference of State Legislatures, States Offering Driver's Licenses to Immigrants (9 de agosto, 2021), https://www.ncsl.org/research/immigration/states-offering-driver-s-licenses-to-immigrants.aspx. De estas 17 demarcaciones, 5 de ellas permiten a ICE consultar electrónicamente la información de las licencias de manejo para propósitos de control migratorio: Colorado, Delaware, Nuevo México, Utah y Washington. Ver infra Hallazgo 2.

90. Aunque las intervenciones telefónicas de ICE son regidas por el Título III de la Wiretap Act, que exige una orden judicial para interceptar "comunicaciones alámbricas, orales o electrónicas", la lista de delitos predicados hace más fácil que ICE obtenga esta información. Ver, i.e., 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 (24 de mayo, 2019), https://privacyinternational.org/news-analysis/2995/ice-paying-millions-surveillance-company-spy-peoples-communications.

91. Privacy International, supra nota 90; Chantal da Silva, ICE Just Launched a $2.4m Contract with a Secretive Data Surveillance Company that Tracks You in Real Time, Newsweek (7 de junio, 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 (11 de mayo, 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 (visitada por última vez el 27 de noviembre, 2021); Chantal Da Silva, ICE Just Launched a $2.4m Contract With a Secretive Data Surveillance Company That Tracks You in Real Time, Newsweek (7 de junio, 2018), https://www.newsweek.com/ice-just-signed-24m-contract-secretive-data-surveillance-company-can-track-you-962493.

93. Ver U.S. Department of Homeland Security, DHS/ICE/PIA-045, Privacy Impact Assessment for ICE Investigative Case Management 7 (16 de junio, 2016), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf ("TLS contiene información de telecomunicaciones ingresada inicialmente en el software Pen-Link de ICE, que sirve como una herramienta investigativa in situ que permite a HSI realizar análisis locales de un solo caso o a través de múltiples casos. Pen-Link contiene un módulo construido a la medida para ICE que estandariza los registros de telecomunicaciones de un gran número de formatos usados por los proveedores de servicios y se usa para exportar e importar archivos de datos en un formato específico usado por TLS. TLS vincula los datos relacionados por medio del uso de identificadores clave para esta información de telecomunicaciones, como los números telefónicos. Esta información permite a los agentes de HSI discernir relaciones que podrían ayudar a identificar las partes de las redes criminales bajo investigación, promoviendo investigaciones adicionales y contribuyendo a la interrupción o al desmantelamiento de las organizaciones criminales.").

94. Ver OIG-07-34, An Assessment of United States Immigration and Customs Enforcement's Fugitive Operations Teams (Marzo 2007), https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/OIG_07-34_Mar07.pdf at 25, 27 (FOSC "apoyará a la Office of Detention and Removal Operations a procesar los datos recibidos a través de los acuerdos negociados de compartición de información de varias maneras."). Id. ("Bajo esos acuerdos, ICE proporciona datos sobre aliens fugitivos del Deportable Alien Control System a esas agencias. Las agencias luego reconcilian los datos proporcionados con la información contenida en sus respectivas bases de datos, y cualquier correspondencia que se encuentre es compartida con ICE.").

95. Memorándum de Acuerdo entre 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 (13 de abril, 2018), https://www.texasmonthly.com/wp-content/uploads/2018/06/Read-the-Memo-of-Agreement.pdf; *Ver* 8 U.S.C § 1232(c)(2)(A) (2012) ("Sujeto a la sección 279(b)(2) del título 6, un *alien* menor de edad sin acompañamiento bajo la custodia de la *Secretary of Health and Human Services* será puesto sin demora en el ambiente menos restrictivo que sea en beneficio del niño.").

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 (11 de febrero, 2020).

99. Ver, i.e, 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. al 1130.

102. Nina Shapiro, Washington state regularly gives drivers' info to immigration authorities; Inslee orders temporary halt, Seattle Times (11 de enero, 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 (23 de febrero, 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 nota 102 ("de 20 a 30 veces al mes, una agencia estatal ha estado dando información personal de los residentes a los funcionarios federales de control migratorio; información usada para arrestar y deportar a las personas según las políticas del presidente.").

107. H.B. 1444, 1993 Reg. Sess. (Wa. 1993) (autoriza la emisión de una licencia con base en la residencia en el estado, entre otros requisitos, sin tomar en consideración el estatus migratorio).

108. Washington Governor Jay Inslee, Inslee statement on Licensing policy changes to protect personal information of immigrants and refugees (15 de enero, 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 (15 de enero, 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 (17 de mayo, 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, 28 de abril, 2017, WADMV_002329 (28 usuarios de ICE con acceso a DAPS).

112. Washington State Department of Licensing, Solicitud de Acceso de parte de Agencias ICE ERO (Dec. 3, 2013), WADMV_002666 ("El acceso es necesario [sic] para verificar y confirmar las identidades de los individuos que han recibido órdenes de remoción de Estados Unidos, incluyendo [sic] los que han vuelto a entrar en Estados Unidos ilegalmente después de ser deportados, así como individuos [sic] con condenas criminales [sic] que representan una amenaza para la sociedad. Con la información proporcionada tras el acceso tanto a los conductores como a los vehículos, sería más fácil realizar vigilancia [sic] y detener a estos individuos.").

113. Registro de auditoría de DAPS en su formato original para todas las búsquedas de matrículas vehiculares realizadas por los usuarios de U.S. Immigration and Customs Enforcement en el Pacific County entre el 1 de enero de 2016 y el 1 de enero de 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 (7 de julio, 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 . . . TERMINADO - SIN OPCIÓN de firmar un nuevo contrato . . . US Dept. of Homeland Security, Immigration & Customs Enforcement/DRO Yakima . . . TERMINADO - SIN OPCIÓN de firmar un nuevo contrato . . . US Dept. of Homeland Security, Immigration & Customs Enforcement, Homeland Security Investigations . . . TERMINADO - SIN OPCIÓN de firmar un nuevo contrato").

116. Frank Bajak, Washington DOL denies giving ICE access to facial recognition searches, KING-TV (8 de julio, 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, Correo de Jeff Oehlerich, Investigador 3 a Agente de Patrulla Fronteriza (30 de marzo, 2017), WADMV_001963-WADMV_001964 ("En el pasado, hemos sido muy liberales en aceptar la justificación de 'investigación criminal' de los solicitantes [sic] y no exigíamos descripciones más específicas. Esto cambió hace alrededor de un mes, como resultado de una orden ejecutiva del gobernador. Ahora exigimos el título o citación estatutaria del delito bajo investigación antes de proporcionar una fotografía. Esto según instrucciones de nuestro equipo ejecutivo de liderazgo. La formulación que autoriza una fotografía para verificar identidades cuando un policía pueda solicitar una identificación fue agregada para permitir a los policías tener un acceso directo a las fotos en sus patrullas y demandar a los infractores cuando detengan a uno que no tenga identificación. El sistema WSP ACCESS sí tiene un formato específico de consultas donde pueden conseguir una foto cuando solicitan la verificación de un conductor. El método actual de hacer la consulta depende del programa de interfaz que usa la agencia, entonces no sé cuáles limitaciones o requisitos puedan tener cada departamento. Recomiendo que se contacte a una de las agencias en su área local para saber si ellos [sic] pueden ayudar.").

118. Washington State Police, Respuesta a Harrison Rudolph (4 de enero, 2021), WANLETS_000007 ("Número de consultas: 2015—398710, 2016—393666, 2017 - 539638, 2018 - 997069, 2019 - 1129711, 2020 - 680847").

119. Washington Department of Licensing, Respuesta a Harrison Rudolph (5 de febrero, 2021), WADMV_3269-WADMV_3274; Washington Department of Licensing, Respuesta a Harrison Rudolph (5 de febrero, 2021), WADMV_003275-WADMV_003281.

120. Washington Department of Licensing, Solicitudes mediante NLETS y acceso a WSP de las agencias federales de inmigración. FY 2019, WADMV_002876-

WADMV_002883 (En el año fiscal 2019, 67,822 ICE-DOL consultas (33,731 conductores), pero 1,395,531 consultas de DHS en total).

121. Id. (17,940 solicitudes de imágenes/30,801 conductores=58%).

122. Georgia DDS, ICE HSI Correo a Georgia DDS (8 de junio, 2018), GADMV_000198 ("¿Puedes ayudarme a buscar una persona en Georgia? No tenemos identificadores específicos excepto un número de celular y los resultados CLEAR. Estoy intentando determinar si hay "dl" [licencia de manejo] sobre el posible sujeto").

123. Georgia DDS, DHS Correo a Georgia DDS (24 de mayo, 2019), GADMV_000436 ("Favor de avisar si [tachado] tiene una DL [licencia de manejo] o identificación estatal de Georgia válida. No logro verificarlo en NLETS.").

124. Ver National Immigration Law Center, How U.S. Immigration & Customs Enforcement and State Motor Vehicles Share Information 3 (Mayo 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 (15 de enero, 2020), https://www.nilc.org/2020/01/15/migrant-justice-settles-discrimination-lawsuit-with-vermont-dmv/.

126. Ver, i.e., Oregon DMV, Hoja de cálculo de solicitudes de información de conductores por parte de ICE (7 de agosto, 2020), ORDMV_000040-ORDMV_000048 (2015: 35 direcciones consultadas; 2016: 40 direcciones consultadas; 2017: 27 direcciones consultadas; 2018: 3 direcciones consultadas; 2019: 0 direcciones consultadas; 2020: 0 direcciones consultadas).

127. Georgia DDS, ICE Correo a Georgia DDS (1 de mayo, 2019), GADMV_000467 ("Viene una oleada en camino y necesito identificar esos blancos [sic] para [tachado] . . . Estoy intentando hacerlo, pero [sic] un grupo ya que tengo tantos. Rellenaré el formulario una vez que verifiques si tienen una foto. Gracias por anticipado.").

128. Ver Virginia DMV, Carta a Harrison Rudolph (17 de agosto, 2020), VADMV_000300.

129. Ver Arizona Department of Transportation, OIG/Professional Standards Unit Narrative (29 de marzo, 2017), AZDMV_000071.

130. Ver U.S. Department of Homeland Security, DHS/ICE/PIA-054, Privacy Impact Assessment for the ICE Use of Facial Recognition Services 2 (13 de mayo, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf ("De manera rutinaria, el HSI encuentra imágenes digitales de víctimas potenciales o individuos sospechosos de cometer delitos pero no puede conectar esas imágenes a información identificable a través de los medios y métodos investigativos en existencia. Por lo tanto, el HSI entrega esas imágenes a las agencias gubernamentales y a vendedores comerciales para compararlas con sus galerías de imágenes digitales a través de los procesos de reconocimiento facial.").

131. Lista de agencias que solicitaron datos del estado de Alaska, 101210.

132. Registros Spillman Flex para solicitudes recibidas del U.S. Department of Homeland Security, incluyendo sus componentes U.S. Immigration and Customs Enforcement, y 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 (16 de marzo, 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 (12 de julio, 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 (18 de febrero, 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. Correo de ICE a Illinois Secretary of State Police (1 de abril, 2020), ILDMV_000139.

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

138. Michigan DMV, MIDMV_000041 ("El día 05/22/2019 consulté el sujeto en COLD, Images y File Net, hablé con un agente de ICE que solicitó reconocimiento [sic] facial y certificaciones de orden. Resultados MSP FR sin otras correspondencias. Recibí las certificaciones el 05/29/2019 [sic].").

139. Ohio Attorney General, Facial-Recognition Inquires: A Special Report 2 (Agosto 2019), https://www.ohioattorneygeneral.gov/FacialRecognitionInquiriesReport ("Agencias federales que han usado la base de datos de reconocimiento facial de Ohio incluyen la U.S. Border Patrol; U.S. Department of State Bureau of Diplomatic Security; U.S. Immigration and Customs Enforcement; el FBI; Federal Reserve Bank of Cleveland; Drug Enforcement Administration; el U.S. Marshals Service; y el Bureau of Alcohol, Tobacco, Firearms and Explosives; y otras.").

140. Driving Pennsylvania Forward, Secure Our Data: Protecting the Privacy of Pennsylvania Residents and Drivers 17 (Septiembre 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, Registros de Consulta, 108850-108911.

142. Vermont Department of Motor Vehicles, Solicitudes para investigaciones de reconocimiento facial, 103714, 103739, 103761, 103763, 104241.

143. Washington State Department of Licensing, ICE-HSI Solicitudes de búsquedas de reconocimiento facial, 100140-100143, 100147-100151, 100285-100288, 100289-100292, 100293-100296.

144. Wisconsin Department of Transportation, Solicitud de ICE para reconocimiento facial a DOT DMV Fraud Unit (18 de julio, 2018), WIDMV_000038.

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

146. S.B. 0225, 102d Gen. Assemb. (Il. 2021), disponible en https://www.ilga.gov/legislation/BillStatus.asp?DocNum=225&GAID=16&DocTypeID=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), disponible en https://le.utah.gov/~2021/bills/static/SB0034.html.

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

150. S.B. 5497, 2019 Reg. Sess. (Wa. 2019), disponible en 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. A través de estos 14 estados, hay un total de aproximadamente 82,822,300 conductores. 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. A través de estos 14 estados, aproximadamente 81,632,770 conductores son adultos. Id. En EE.UU., hay un total de aproximadamente 257,536,091 adultos. U.S. Census Bureau, QuickFacts, https://www.census.gov/quickfacts/fact/table/US/POP010210#POP010210.

154. Wisconsin DOT, WISC correo a WI DOT; Solicitud de reconocimiento facial (16 de marzo, 2017), WIDMV_001017 ("En nombre del Department of Homeland Security, Homeland Security Investigations, quisiera solicitar una tentativa de FR [reconocimiento facial] con las fotos anexas. El individuo en la imagen estaba recibiendo documentos de identidad falsos y la oficina de HSI en Milwaukee está intentando determinar su verdadera identidad. Esto es parte de una investigación de fraude en curso que ellos están manejando.").

155. Georgia DDS, Correo a Georgia DDS (2 de marzo, 2018), GADMV_000157 ("¿Puedes intentar con éstas, amigo? También puedo entrar en Facebook e intentar encontrar una mejor… ¿Puedes intentar otra vez con estas fotos en FR [reconocimiento facial] cuando se presente la ocasión?").

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. Ver 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 (12 de diciembre, 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. (6 de febrero, 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 (18 de septiembre, 2019), https://www.sltrib.com/news/politics/2019/09/18/utah-lawmakers-scrutinize/ ("los funcionarios admitieron que el sistema de Utah es anticuado; propenso a cometer errores, especialmente con mujeres y personas de color; requiere que los analistas reciban más capacitación y no tiene estándares legales para su operación").

158. Ver U.S. Department of Homeland Security, DHS/CBP/PIA-054, Privacy Impact Assessment for the ICE Use of Facial Recognition Services 9 (13 de mayo, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf ("HSI sólo entregará fotos de rastreos para que se utilicen en el desarrollo de investigaciones criminales en curso… HSI no apoyará a la ERO en el uso [del reconocimiento facial] únicamente para el desarrollo de medidas de control migratorio civil.").

159. Joan Friedland, How ICE Blurs the Line between Enforcement of Civil Immigration Violations and Enforcement of Criminal Laws, National Immigration Law Center (27 de agosto, 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 (Mayo 2016), https://www.gao.gov/assets/gao-16-267.pdf ("Hasta diciembre del 2015, el FBI tiene acuerdos con 7 estados para buscar en NGI-IPS, y está trabajando con más estados para lograr el acceso. Además del NGI-IPS, el FBI tiene una unidad interna llamada Facial Analysis, Comparison and Evaluation (FACE) Services que ofrece capacidades de reconocimiento facial, entre otras cosas, para apoyar las investigaciones del FBI en curso. FACE Services no sólo tiene acceso al NGI-IPS, sino también puede buscar o solicitar una búsqueda en bases de datos en posesión de los Departamentos de Estado y Defensa y 16 estados, que usan sus propios sistemas de reconocimiento facial.").

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

162. Federal Bureau of Investigation, July 2021 Next Generation Identification (NGI) System Fact Sheet (Julio 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 (Febrero 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 (14 de noviembre, 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 (7 de julio, 2019), https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html.

165. El sistema se llamaba anteriormente el National Law Enforcement Telecommunication System.

166. U.S. ICE, Replacement/Upgrade of Message Switching System (23 de septiembre, 2006), https://drivi.eoogle.com/file/d/11M_G3wOwB7x0-U_LAVd5M0kw-XJcWGuj/view?usp=sharing ("El contrato remplazará y actualizará su patentado sistema OpenFox Message Switching System instalado en el año 2000 en la actividad de campo [LESC] de ICE en Williston, VT. El sistema se comunica mediante una interfaz con sistemas nacionales como el National Law Enforcement Telecommunications System (NLETS) y el National Crime Information Center (NCIC) y otros protocolos especializados propios a la comunidad de seguridad".); Bonnie Locke, Five Commonly Asked Questions About NLETS, NLETS Blog (27 de mayo, 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. 167 Ver Wisconsin DOT, Consultas WI NLETS (2020), WINLETS_000010-WINLETS_000102.

168. Los que no comparten su información de DMV con NLETS (7 estados): "Nevada, Hawái, Oklahoma, Illinois, Carolina del Sur, Connecticut, Vermont, Guam, y las Islas Vírgenes." Los que han cortado el uso de ICE por otras razones (7 estados): Alaska (orden judicial) California (permitido para controles no migratorios) Nueva York (por medio del código ORI) Nueva Jersey (permitido para controles no migratorios) Dakota del Norte (no es claro por qué) Dakota del Sur (no es claro por qué) Oregón (permitido para controles no migratorios)); Ver también H.B. 2163, Va. Gen. Assemb., 2021 Sess. (Va. 2021), https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+HB2163 (Ley de Virginia que limita la divulgación de información del DMV para propósitos de control migratorio civil); 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. A través de estos 35 estados, hay un total de aproximadamente 150,697,928 conductores. 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. Ver Documento 71-1, presentado el 17 de junio, 2020, en 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 (Los que no comparten su información de DMV con NLETS (7 estados): "Nevada, Hawái, Oklahoma, Illinois, Carolina del Sur, Connecticut, Vermont, Guam, y las Islas Vírgenes." Los que han cortado el uso de ICE por otras razones (7 estados): Alaska (orden judicial) California (permitido para controles no migratorios) Nueva York (por medio del código ORI) Nueva Jersey (permitido para controles no migratorios) Dakota del Norte (no es claro por qué) Dakota del Sur (no es claro por qué) Oregón (permitido para controles no migratorios)); Ver también H.B. 2163, Va. Gen. Assemb., 2021 Sess. (Va. 2021), https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+HB2163 (Ley de Virginia que limita la divulgación de información del DMV para propósitos de control migratorio civil); 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. A través de estas 40 demarcaciones, hay un total de aproximadamente 193,643,467 conductores, de los cuales aproximadamente 191,079,036 son adultos. 191M/257M = 74%. Ver 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 (número total de adultos).

172. Ver Wisconsin DOT, Consultas WI NLETS (2020), WINLETS_000010-WINLETS_000102.

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

174. Iowa Department of Public Safety, Correo a Harrison Rudolph (18 de noviembre, 2020), IANLETS_000003 (La tabulación de las cifras de estas consultas específicas desde el 2015 llega a un total de aproximadamente 83,400.).

175. Washington Department of Licensing, Solicitudes mediante NLETS y acceso a WSP de las agencias federales de inmigración - FY2019, WADMV_002876-WADMV_002883 (En el año fiscal 2019, 67,822 consultas ICE-DOL (33,731 conductores)).

176. Ver, i.e., National Immigration Law Center, NLETS: Questions and Answers (Noviembre 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 (Marzo 2020), https://justfutureslaw.org/wp-content/uploads/2020/04/2020-3-5-State-DMV-Data-Sharing-Just-Futures-Law.pdf.

177. Carta de Christine E. Nizer, William P. Doyle, Ricky D. Smith & Pilar Helm al 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

(28 de enero, 2021), https://drivi.eoogle.com/file/d/1siYx-yDkwggUQB3APZzqYmfKkg7BQHnF/view?usp=sharing.

178. Maryland DPSCS, Carta a Harrison Rudolph, 21 de enero, 2021 ("Escribo para informarle que el *Department of Public Safety and Correctional Services* (DPSCS) no es el custodio oficial para los datos que busca. Para facilitar el procesamiento de su petición, he remitido su consulta a: *Maryland Department of State Police*").

179. Maryland State Police, Carta a Harrison Rudolph, 27 de enero, 2021 ("Al revisar su solicitud, se determinó que el MSP no mantiene nada relacionado con las consultas. Todos los registros de las consultas que se originan dentro y fuera del estado están registrados en la central estatal de mensajes albergada por el DPSCS. Ellos deberían poder conseguir los registros").

180. Iowa Department of Transportation, Carta a Harrison Rudolph (24 de agosto, 2020), IADMV_000081 ("El Iowa Department of Transportation es la única fuente de información de conductores y vehículos a la que el DPS tiene acceso y usa para cumplir su obligación con NLETS. El DPS tiene una conexión directa con el Iowa Department of Transportation donde tienen acceso a un servicio web (DPSService) para obtener información de los conductores. El DPS envía una solicitud para un cliente específico, y con base en el tipo de solicitud, se genera una respuesta usando el Global Justice XML Data model (GJXDM) que luego es devuelta al DPS. Las respuestas son dinámicas y varían según el tipo de cliente y solicitud. Qué campos se usan y cómo es asunto del DPS; nosotros sencillamente ponemos esta información a la disposición del DPS a través del DPSService.").

181. Idaho Transportation Department, Carta a Harrison Rudolph (25 de agosto, 2020), IDDMV_000009-IDDMV_000011 ("El ITD no posee ningún documento tal. El ITD está obligado por la REGLA administrativa estatal 39.02.41.200 (anexa abajo) a enviar la información de vehículos y conductores al Idaho Law Enforcement Telecommunication Systems (ILETS) para proporcionar la información de vehículos y conductores a las agencias de seguridad. La policía estatal de Idaho supervisa a ILETS y cómo interactúa con NLET; ITD no está involucrado en este proceso.").

182. Colorado Bureau of Investigation, Correo de Kristina Gavit a Harrison Rudolph (13 de noviembre, 2020), CONLETS_000019-CONLETS_000020.

183. Documento 43-1, presentado el 24 de abril, 2020, en Lewis-McCoy, et al. v. Wolf, et al., Case 1:20-cv-01142-JMF, S.D.N.Y ("Generalmente, la información del DMV se recupera a través del National Law Enforcement Telecommunication System (NLETS)"); hay registros públicos que respaldan eso. Un agente de inmigración pidió ayuda al Georgia Department of Driver Services para verificar una licencia de manejo sólo después de que el agente fue "incapaz de verificar[lo] en NLETS." Georgia DDS, DHS Correo a Georgia DDS (24 de mayo, 2019), GADMV_000436 ("Favor de avisar si [tachado] tiene una DL [licencia de manejo] o identificación estatal de Georgia válida. No logro verificarlo en NLETS."). Otros registros públicos muestran que otro agente de ICE solicitó información de una licencia de manejo a la Secretaría de Estado de Illinois (incluyendo una fotografía) sólo después de intentar una búsqueda en NLETS. Illinois Secretary of State, Correo de ICE HSI Requesting Driver Records (17 de julio, 2019), ILDMV_000207-ILDMV_000209 ("Homeland Security Investigations está solicitando ayuda para obtener la información del DMV y foto del siguiente individuo . . . NLETS arrojó los siguientes resultados . . . [Tachado] RES-PID CLASS/NONE DL/IP STA/ VALID TDL/TIP STA/SEE /LOLNHELP CDL STA/ SEE ILOLNHELP DIGITAL ISSUE . . . El sujeto es un posible testigo en una investigación criminal en curso. En violación de 21 USC § 848, empresa criminal en curso.").

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 (25 de julio, 2020), https://homeland.housi.eov/news/press-releases/thompson-and-rice-announce-investigation-after-administration-gave-inaccurate-testimony-to-congress-about-political-attack-on-new-york.

185. Documento 43-1, presentado el 24 de abril, 2020, en Lewis-McCoy, et al. v. Wolf, et al., Case 1:20-cv-01142-JMF, S.D.N.Y ("Algo de la información contenida en las bases de datos del DMV podría estar disponible en otras fuentes, pero estos datos no son tan precisos, actualizados o completos como los de las bases de datos del DMV. Con el empleo de tiempo y esfuerzo adicionales, algo de la información del DMV podría localizarse en otras bases de datos, pero algunos registros son propios de las bases de datos del DMV. Por ejemplo, bases de datos públicas y comercialmente disponibles, como CP CLEAR, contienen algunos registros residenciales, fechas de nacimiento y fotografías; sin embargo, esta información a menudo está incompleta, incorrecta o desactualizada.").

186. Ver Joseph Cox, DMVs Are Selling Your Data to Private Investigators, VICE (6 de septiembre, 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 (25 de noviembre, 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 (2 de octubre,2019), https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.

188. La empresa madre de LexisNexis, RELX Group, es un contratista importante que ha proporcionado a los agentes de ICE el acceso a bases de datos masivas de información biográfica de las personas. Ver 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 (visitada por úlimta vez el 21 de noviembre, 2021); LexisNexis, Diapositivas PowerPoint para DMV

de Carolina del Sur (May 11, 2016), SCDMV_000239-SCDMV_000249 ("El 12% de los ingresos de LexisNexis Risk Solutions viene del gobierno y el sector salud").

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- (visitada por última vez el 21 de noviembre, 2021).

191. Florida HSMV, LexisNexis Senior Vice President and General Counsel Carta a FLHSMV (16 de abril, 2018), FLDMV_000111-FLDMV_000113 ("LexisNexis apoya a más de 5,000 agencias de gobierno federales, estatales y locales. Muchas de estas agencias tienen responsabilidades de iniciativas de seguridad nacional además de responsabilidades tradicionales de seguridad . . . de acuerdo con F.S.A. §119.0712(2)(b) y 18 U.S.C. §(b)(l), LexisNexis proporciona registros de vehículos motorizados y datos de licencias de manejo de Florida a agencias gubernamentales que usan los datos para cumplir con su trabajo, incluyendo, pero no limitado a, la localización de fugitivos y la determinación de la elegibilidad de un individuo para beneficios, licencias y permisos.").

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 (20 de julio, 2018), AZDMV_000015-AZDMV_000031.

194. Aunque el DMV de California requiere que los solicitantes gubernamentales autorizados se abstengan de usar la información de las licencias de manejo para propósitos de control migratorio civil, no es claro si LexisNexis Risk Solutions ha aceptado la condición. Ver VICE News, California DMV Commercial Requester Accounts, https://drivi.eoogle.com/file/d/1czK4QyHbZRhXivG29oLjk4pl1Ph2JhUp/view?usp=sharing (que incluye en su lista a LexisNexis Risk Solutions como un solicitante comercial autorizado).

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

196. Florida HSMV, LexisNexis Senior Vice President and General Counsel Carta a FLHSMV (16 de abril, 2018), FLDMV_000111-FLDMV_000113.

197. Illinois Secretary of State, Driver Service Agency Sales Activity, Mes de febrero 2019, ILDMV_000064

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

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

200. Nevada DMV, Solicitud de historial de registro, LexisNexis Risk Solutions Inc. (2019), NVDMV_000021-NVDMV_000022.

201. Ver Diane Willson, NCDMV Sells Your Personal Information, Pockets Millions of Dollars, ABC11 Eyewitness News (5 de febrero, 2020), https://abc11.com/lexis-nexis-dmv-nc-ncdmv/5903314/ ("Un representante de NCDMV dijo que el departamento vende tu información personal a estas tres empresas:" Explore Info Services, Envision-Data Driven Safety y Lexis Nexis Corporation).

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

203. South Carolina DMV, Acuerdo, Information Release Agreement (Data Manipulators) with LexisNexis Risk Solutions (28 de junio, 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 (17 de febrero, 2020), https://fox17.com/news/local/personal-information-of-72-million-tennessee-drivers-sold-to-companies-by-state-agency ("La siguiente pregunta que hicimos al departamento fue, ¿qué empresas estaban recibiendo nuestros datos? El departamento enumeró cinco empresas: Acxiom Corporation, Drivers History, Explore Information Services, Lexis Nexis y Samba Holdings.").

205. Ver Rhonda Foxx, WisDOT Earned Millions by Providing Driver Information to Third Parties, WeAreGreenBay.com (10 de febrero, 2020), https://www.wearegreenbay.com/news/local-news/wisdot-earned-millions-by-providing-driver-information-to-third-parties/ ("Archivo de encabezado del registro del conductor: Información del historial del conductor, Explorar servicios de información, Intercambio de información del seguro (IIX), Lexis Nexis, Acxiom, Early Warning Services, LLC, TransUnion, West Services (Thomson Reuters)").

206. A través de estas 13 demarcaciones, hay un total de aproximadamente 88,250,040 conductores, de los cuales aproximadamente 87,182,428 son adultos. 87M/257M = 34%. Ver 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 (número total de adultos).

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 (visitada por última vez el 16 de noviembre, 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 (14 de enero, 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. Ver, i.e., Release of DMV Information, Virginia DMV, https://www.dmv.virginia.gov/general/#records/release.asp.

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

212. Según el procurador general de EE.UU. y el oficial del Comité Judicial de la Cámara de Representantes, la transcripción de la audiencia de dos días de DPPA no fue preservada. Ver Petition for Writ of Certiorari, Okla. Dep't of Pub. Safety v. United States, 528 U.S. 1114 (No. 98-1760), https://www.justici.eov/sites/default/files/osg/briefs/1998/01/01/98-1760.resp.hold.pdf. Pero ver Protecting Driver Privacy: Hearings Before the Subcomm. on Civ. and Const. Rts. of the H. Comm. on the Judiciary 103rd Cong. (1994) (declaración de Janlori Goldman, Director, American Civil Liberties Union), disponible en 1994 WL 212813 (3-4 febrero, 1994); 1994 WL 212833; 1994 WL 212834; 1994 WL 212836; 1994 WL 212696; 1994 WL 212701, 212712; 1994 WL 212720.

213. Ver Just Futures Law, State Driver's License Data: Breaking Down Data Sharing and Recommendations for Data Privacy 4 (Marzo 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, Hoja de cálculo de solicitudes de información de conductores de ICE Spreadsheet of ICE (7 de agosto, 2020), ORDMV_000040-ORDMV_000048 (2015: 35 direcciones consultadas; 2016: 40 direcciones consultadas; 2017: 27 direcciones consultadas; 2018: 3 direcciones consultadas; 2019: 0 direcciones consultadas; 2020: 0 direcciones consultadas).

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

217. Ver Oregon DMV, Disseminator Contract with West Publishing Corporation (21 de febrero, 2020), ORDMV_000025-ORDMV_000033 (El Diseminador puede revender o redivulgar información personal sólo a una persona o agencia gubernamental autorizada a recibirla bajo ORS 802.179. [ORS 802.179(1) El Department of Transportation, bajo solicitud o como lo requiera la ley, divulgará información personal de un registro de vehículo motorizado a una agencia gubernamental para su uso en el cumplimento de su trabajo gubernamental.]); Oregon DMV, Disseminator Contract with LexisNexis Risk Solutions, Inc (22 mayo, 2020), ORDMV_000004-ORDMV_000012 (El Diseminador puede revender o redivulgar información personal sólo a una persona o agencia gubernamental autorizada a recibir tal información bajo ORS 802.179. [ORS 802.179(1) El Department of Transportation, bajo solicitud o como lo requiera la ley, divulgará información personal de un registro de vehículo motorizado a una agencia gubernamental para su uso en el cumplimento de su trabajo gubernamental.]).

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 (8 de diciembre, 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 (12 de octubre, 2019), https://www.nbcsandiego.com/news/local/ice-drivers-license-gonzales/1966317/.

223. La divulgación de los datos de los conductores a ICE para medidas de control migratorio civil no está prohibida por la ley en Connecticut, Delaware, Illinois, Nuevo México, Nevada y Utah.

224. El acceso a NLETS por parte ICE para medidas de control migratorio civil no está prohibido por la ley en Connecticut, Delaware, Hawái, Illinois, Nuevo México, Nevada y Utah.

225. La venta de los datos de los conductores a agencias de datos y su reventa subsecuente a ICE para propósitos de control migratorio civil no está prohibida por la ley en el Distrito de Columbia, Colorado, Hawái, Illinois, New Jersey, Nevada y Vermont.

226. Las búsquedas de reconocimiento facial de los datos de los conductores para propósitos de control migratorio civil no están prohibidas por la ley en Connecticut, Delaware, Hawái, Nuevo México y Nevada.

227. La divulgación sin orden judicial de los datos de los conductores a ICE para propósitos de control migratorio no civil no está prohibida por la ley en California, Colorado, Nueva Jersey, Oregón, Vermont y Virginia.

228. El acceso a NLETS sin orden judicial por ICE para propósitos de control migratorio no civil no está prohibido por la ley en California, Colorado, Nueva Jersey, Oregón, Vermont, Virginia, y el estado de Washington.

229. La venta de los datos de los conductores a las agencias de datos y su reventa subsecuente a ICE para propósitos de control migratorio no civil no está prohibida por la ley en California, Connecticut, Delaware, Virginia y el estado de Washington.

230. Las búsquedas de reconocimiento facial de los datos de los conductores para propósitos de control migratorio no civil no están prohibidas por la ley en Colorado, el Distrito de Columbia, Illinois, Nueva Jersey, Utah, Virginia.

231. Ver The Maryland Driver Privacy Act, H.B. 23 §4-320(g)(2) (2021) (que restringe la compartición de los datos de los conductores "a un agente federal o una agencia federal para propósitos de control migratorio federal"); id. al §4-320.1(B)(1) & (B)(2) (que restringe el acceso a los sistemas

de reconocimiento facial por "cualquier agencia federal que busca el acceso para el propósito de aplicar las leyes migratorias federales").

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

233. Doc 71-1, presentado el 17 de junio, 2020, en 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. ("Más de 50 millones de estadounidenses no cuentan con puntajes crediticios y son "invisibles para crédito". Otros 50 millones tienen puntajes más bajos de lo que deberían, ya que no cuentan con suficientes líneas de crédito para generar un puntaje.").

236. Id.

237. Ver 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 ("Uno de los esfuerzos por promover datos crediticios alternativos insta a las compañías de servicios públicos a comprometerse a emitir informes mensuales de los pagos de sus clientes, incluyendo pagos tardíos, a las tres agencias de informes crediticios (CRA por sus siglas en inglés) más grandes del país: Equifax, Experian y TransUnion. Actualmente, la gran mayoría de compañías de electricidad y gas natural son las que informan a esas tres CRA cuando una cuenta morosa ha sido referida a una agencia de cobranzas, o ha sido declarada como incobrable.").

238. Ver 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 (carta de Buddy Flake, NCTUE Board President, y Michael Gardner, Senior Vice President, Equifax, dirigida a Keith Ellison, miembro, *Commitee on Financial Services).* ("[La *National Consumer Telecom & Utilities Exchange*] es un centro nacional de datos, propiedad de sus miembros y operado por ellos, que cumple con la FCRA, y que alberga datos positivos y negativos alternativos de pagos (ej. datos financieros no tradicionales de informes de pagos, tales como pagos de servicios públicos y de telecomunicaciones) de consumidores, los cuales, a su vez, están disponibles sin miramientos para los miembros de la NCTUE para auxiliarlos en sus decisiones de otorgamiento de créditos y manejo de riesgos… las compañías miembros actualmente reportan y comparten datos de pagos específicos de la industria de más de 180 millones de consumidores de todo Estados Unidos.").

239. Ver 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 (declaración de Hon. Keith Ellison) ("Estoy ansioso por ver a este Congreso tomar acciones para mejorar nuestro sistema [de reportes crediticios] haciéndolo más inclusivo… Mr Fitzpatrick y yo, de una forma bipartidista, tenemos un proyecto de ley llamado Credit Access and Inclusion Act, que subraya que la ley actual no prohíbe que las firmas de servicios públicos y de telecomunicaciones reporten los pagos puntuales de sus clientes.

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 (26 de febrero, 2021), https://oversight.house.gov/news/press-releases/oversight-subcommittee-launches-investigation-into-sale-of-utility-customer-info.

244. Georgia DDS, correo electrónico a Georgia DDS; B1/2 visado sobrepasado por parte de inmigrante, 2 de junio de 2020, GADMV_001230.

245. Id.

246. Ian Kullgren, ICE to Scale Back Arrests During Coronavirus Pandemic, Politico (18 de marzo, 2020) https://www.politico.com/news/2020/03/18/ice-to-scale-back-arrests-during-coronavirus-pandemic-13680. Al parecer, el entonces secretario interino del DHS, Ken Cuccinelli, revirtió esta política, sin embargo, insinuó que los arrestos se darían de manera más pausada. Ver Ken Cuchinelli (@HomelandKen), Twitter (19 de marzo, 2020), https://twitter.com/HomelandKen/status/1240644749176037377.

247. Georgia DDS, correo electrónico a Georgia DDS; B1/2 visado sobrepasado por parte de inmigrante, 2 de junio de 2020, GADMV_001230.

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

249. Ver About Us, NCTUE, https://www.nctue.com/about-us (última visita 27 de nov., 2021) (indica que la base de datos de NCTUE incluye información de más de 218 millones de consumidores únicos); (13 de octubre, 2020), https://www.youtube.com/watch?v=PqAZ5uoRsg0 (a las 2:47, indica el porcentaje de la población por estado en la base de datos de NCTUE); U.S. Census Buró, estimado del total de la población residente y la población residente de mayor de 18 años de EE.UU., Regiones, Estados, el Distrito de Columbia y Puerto Rico, 1 de julio, 2020. https://www2.census.gov/programs-surveys/popest/tables/2010-2020/national/

asrh/sc-est2020-18+pop-res.xlsx (indica la población total y la población adulta por estado, en 2020).108

250. USAspending, Contract to West Publishing Corporation, https://www.usaspending.gov/award/CONT_AWD_HSCEMD11F00003_7012_GS23F0387K_4730 (última visita, 27 de noviembre, 2021).

251. El DHS y ICE se sirven de una red de compañías privadas para sintetizar y recabar esta información. Ver, en lo general, 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. Carta de Kyle Keene, Govt. CLEAR Specialist a Joshua, Thomson Reuters (17 de enero, 2018), https://www.prorfx.com/Storage/110S34471_051/ProRFx/Upload/Attachments/General/Sole%20Source%20Letter%20-Thomas%20Reuters.pdf.

253. Id.

254. Carta de Judy Whalley a Assistant Attorney Gen. Anne K. Bingaman (9 de diciembre, 1993), https://www.justice.gov/sites/default/files/atr/legacy/2014/07/22/303389.pdf. Los miembros fundadores del Centro fueron: Allnet Communication Services, Inc., AT&T, Business Telecom, Inc., Cable & Wireless, Inc., LDDS Metromedia Communications Corporation, MCI Telecommunications Corporation, Sprint, y WilTel Business Networks.

255. 255 Carta de Judy Whalley a Assistant Attorney Gen. Anne K. Bingaman (9 de diciembre, 1993), https://www.justice.gov/sites/default/files/atr/legacy/2014/07/22/303389.pdf. Los miembros fundadores del Centro fueron: Allnet Communication Services, Inc., AT&T, Business Telecom, Inc., Cable & Wireless, Inc., LDDS Metromedia Communications Corporation, MCI Telecommunications Corporation, Sprint, y WilTel Business Networks.

256. El proceso para obtener la aprobación se discute en las regulaciones del. U.S. Department of Justice, What is a Business Review? (25 de junio, 2015), https://www.justice.gov/atr/what-business-review ("Las personas preocupadas por la legalidad, según las leyes antimonopolio, de la conducta propuesta de los negocios pueden solicitar al Departamento de Justicia una declaración sobre sus intenciones actuales de aplicación de la ley con respecto a esa conducta en virtud del Procedimiento de Revisión de Negocios del Departamento. Ver 28 C.F.R. § 50.6").

257. NCTUE, History of NCTUE, https://www.nctue.com/history (última visita 27 de noviembre., 2021).

258. Comunicado de Prensa, Equifax Investor Relations, Equifax Extends Service Agreement with National Consumer Telecom and Exchange (19 de noviembre, 2019), https://investor.equifax.com/news-events/press-releases/detail/89/equifax-extends-service-agreement-with-national-consumer. ("Bajo los términos del acuerdo actual, Equifax continuará operando y gestionando la base de datos de NCTUE. Equifax también mantendrá el derecho exclusivo de entregar productos y servicios de NCTUE, incluyendo: Equifax Insight Scores for Credit, Rental Scores, Advanced Communications Plus, Advanced Energy Plus, y muchos otros hasta el año 2024. La extensión de este acuerdo de servicios asegura la continuación de la ejecución y gestión de la base de datos de NCTUE, sujeta a la supervisión del Consejo Directivo de NCTUE."). La intención de Equifax de vender estos datos a entidades externas parece haber estado presente -y haber sido mutuo- desde el inicio. En una carta al DOJ, las compañías fundadoras citaron "el compromiso de… Equifax. . . de encontrar y explotar las oportunidades propicias para el acceso de terceros para el intercambio de datos" como una razón de su asociación. "Por ende, las ganancias generadas [pasarán] a los miembros del intercambio para que sufraguen sus gastos," afirmaron; formando así una de las "iniciativas económicas más sustanciales y en continuo crecimiento" que motivaron el acuerdo. Ver carta de Craig L. Caesar a Assistant Attorney Gen Hon Charles A James 4 n.5 (17 de agosto, 2001), https://www.justice.gov/atr/page/file/1019991/download.

259. Carta a Judy Whalley a Assistant Att'y Gen. Anne K. Bingaman (9 de diciembre, 1993), https://www.justice.gov/sites/default/files/atr/legacy/2014/07/22/303389.pdf.

260. Un reporte de rastreo que "tendría la dirección actual del cliente para permitir que la compañía… rastree al deudor en su nueva ubicación y busque una recuperación." Id.

261. Carta de Craig L. Caesar al Assistant Attorney General Hon Charles A. James 2 (17 de agosto, 2001), https://www.justice.gov/atr/page/file/1019991/download.

262. NCTUE, History of NCTUE, https://www.nctue.com/history (última visita, 27 de noviembre, 2021).

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

264. Equifax, NCTUE, https://www.equifax.com/business/data-network/nctue/ (última visita, 27 de noviembre, 2021).

265. Thomson Reuters, CLEAR Utility Filing (Julio 2020), https://drive.google.com/file/d/1R2i1fkW1TMLG75duQCpSlJhUFCEAqQ1a/view?usp=sharing (captura de pantalla obtenida por Aaron Lackowski de Empower LLC y compartida con el Center on Privacy & Technology).

266. Equifax Insights, What is the NCTUE?, YouTube (13 de octubre, 2020), https://www.youtube.com/watch?v=PqAZ5uoRsg0&t=103s.

267. Carta de Craig L. Caesar to Assistant Attorney General Hon. Charles A. James 3 (17 de agosto, 2001), https://www.justice.gov/atr/page/file/1019991/download. 100

268. Id.

269. Id. at 3 n.4.

270. Conferencia de usuarios de NCTUE: We're Better Together (Noviembre. 2015), https://www.nctue.com/userimages/2015_NCTUE_Users_Conference_Agenda.pdf.

271. NV Energy usa el Equifax Advanced Energy Risk Model para evaluar los riesgos crediticios de los clientes. Public Utilities Commission of Nevada, Respuesta de Nevada Power Company d/b/a NV Energy y Sierra Pacific Power Company d/b/a NV Energy a la orden procesal No. 1 8 (7 de octubre, 2016), https://drive.google.com/file/d/1Jnf_Vny3n1xcKkpgp3l3HTN53Drjp-ev/view?usp=sharing.

De acuerdo con una hoja de descripción de producto de Equifax, el marcador Advanced Energy Plus toma datos de la NCTUE y solo está disponible para miembros del NCTUE. Equifax, Advanced Energy Plus (3 de marzo, 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 (22 de marzo, 2019), http://www.miamidade.gov/smallbusiness/library/reports/sbe/bw9744-0-22-project-package.pdf (El Miami-Dade County's Water and Sewer Department es un miembro de la National Consumer Telecom and Utilities Exchange (NCTUE), un consorcio de más de 95 compañías miembros para empresas de servicios públicos, telecomunicaciones e industrias de televisión de paga. La NCTUE proporciona a sus miembros servicios de verificación de riesgos de crédito diseñados especialmente para las compañías de servicios públicos.").

273. Thomson Reuters, CLEAR Utility Filing (Julio 2020), https://drive.google.com/file/d/1R2i1fkW1TMLG75duQCpSlJhUFCEAqQ1a/view?usp=sharing; Respuesta de Thomson Reuters 22033003 para proporcionar el servicio de investigación legal en línea al Illinois Central Management Services, Thomson Reuters (12 de junio, 2014) http://www.purchase.state.il.us/ipb/master.nsf/all/D861DF95975DCE42862580360060EA32/$file/Pricing.pdf?OpenElement.

274. Thomson Reuters, CLEAR Utility Filing (Julio 2020), https://drive.google.com/file/d/1R2i1fkW1TMLG75duQ_CpSlJhUFCEAqQ1a/view?usp=sharing. 185

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

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

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

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

279. LexisNexis Risk Solutions, Collections and Recovery Products and Services (última visita 27 de noviembre, 2021), https://www.secondalliance.com/wp-content/uploads/2017/11/LexisNexis.pdf.

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

281. Ver carta de Ron Wyden, U.S. Senator. a Hon. Rohit Chopra, Director, Consumer Financial Protection Bureau 2 (8 de diciembre, 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. Ver también Drew Harwell, Utility giants agree to no longer allow sensitive records to be shared with ICE, Washington Post (8 de diciembre, 2021), https://www.washingtonpost.com/technology/2021/12/08/utility-data-government-tracking/.

282. Ver carta de Ron Wyden, U.S. Senator. a Hon. Rohit Chopra, Director, Consumer Financial Protection Bureau 1 (8 de diciembre, 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; @JustFuturesLaw, Twitter (8 diciembre, 2021), https://twitter.com/JustFuturesLaw/status/1468590605668425729?s=20.

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

284. Comunicado de Prensa, Oficina de Gavin Newsom, Governor Newsom Takes Action on Legislation to Support California's Immigrant and Refugee Communities (27 de septiembre, 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 (28 de septiembre, 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) (Promulgada) (codificada en Cal Civ. Code § 1798.98), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB2788 ("Una corporación de servicios de electricidad o una corporación de servicio de gas no deberá vender los datos de consumo de electricidad o gas de un cliente, así como ningún otro dato de identificación personal para ningún propósito.").

287. City News Service, supra nota 285.

288. Equifax Insights, What is the NCTUE?, YouTube (13 de octubre, 2020), https://www.youtube.com/watch?v=PqAZ5uoRsg0&t=103s (2:24) (Indica que el 50.2% de la información de los residentes de CA se encuentra en la base de datos de NCTUE.) 50

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

290. De acuerdo con un estudio de 1996, aproximadamente 1 de cada 3 estadounidenses optó por que su compañía telefónica los mantuviera fuera de la lista Id. en.142 (citando a 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 (última visita, 27 de noviembre, 2021) http://web.archive.org/web/20020202103820/www.irsg.org/html/termination.htm ("No tiene sentido mantener un programa de autorregulación cuando esta información ya está regulada

bajo el Gramm-Leach-Bliley Act… Todos los miembros de IRSG han acordado continuar obedeciendo los principios de uso de datos de IRSG para los datos recabados antes del 1 de julio de 2001.")

293. Ver, i.e., en re Trans Union Corp., 9255, 200 WL 257766 (F.T.C., 10 de febrero, 2000).

294. Ver Uriel J. Garcia, ICE arrests young immigrant's sponsor months after feds assured him he'd be safe, Santa Fe New Mexican (9 de septiembre, 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. Este pasaje ha sido adaptado del recuento de 2017 de un traductor sobre el proceso regular de admisión de la ORR. Ver Valeria Luiselli, Tell Me How It Ends: An Essay in 40 Questions 49 (2017).

296. Ver Garcia, supra nota 294. 7

297. U.S. 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. Aunque muchos menores sin acompañante están llegando a la frontera a solicitar asilo, muchos de ellos tienen derechos más fuertes a la asistencia bajo las protecciones especiales de los inmigrantes menores de edad. De hecho, la gran mayoría de los menores que llegan a la frontera solicitan protección internacional. Ver, en lo general, Oficina del Alto Comisionado de las Naciones Unidas para Refugiados Regionales de los Estados Unidos y el Caribe, Children on the Run, United Nations High Commissioner for Refugees (Marzo 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. 17 de enero, 1997), disponible en https://www.aclu.org/sites/default/files/assets/flores_settlement_final_plus_extension_of_settlement011797.pdf.

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

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

303. TVPRA, § 235(c)(2).

304. See id.

305. Ver 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/. 7

306. Ver Government Accountability Office, GAO-19-163, supra nota 305 at 9–10.

307. Id. en 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 (Noviembre 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; ver 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. 20

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

312. Id.

313. Ver Neena Satija, Karoun Demirjian, Abigail Hauslohner & Josh Dawsey, A Trump administration strategy led to the child migrant backup crisis at the border, Washington Post (12 noviembre, 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 (La investigación reforzada de los antecedentes de los tutores, así como la compartición de datos de información entre las oficinas de asistencia social infantil y las autoridades de inmigración …"provocaron que miles de menores sin acompañante se quedaran varados bajo la custodia de EE.UU. y acentuaron la sensación de una crisis en la frontera sur"); ver también, i.e., Robert Moore, Border Patrol argues child treatment at Clint migrant facility not as described, gives access to Texas station, Washington Post (16 de junio, 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 ("Los abogados y los trabajadores de salud que visitaron la estación Clint Border Patrol al inicio de este mes calificaron las condiciones de los menores sin acompañante como "deplorables", pues han permanecido aquí de manera prolongada debido a que los albergues especiales para niños se encuentran saturados.").

314. Ver, en lo general, Carta de 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 para Cameron Quinn, Officer of Civil Rights & Civil Liberties en el Department of Homeland Security & John Kelly, Acting Inspector General en el Department of Homeland Security (6 de diciembre, 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. Ver Senator Jeff Merkley, Merkley Reveals Secret Trump Administration Plan to Create Border Crisis, Medium (17 de enero, 2019), https://medium.com/@SenJeffMerkley/merkley-reveals-secret-trump-administration-plan-to-create-border-crisis-f72a7c3de2bd.

316. Memorándum de Acuerdo 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 (13 de abril, 2017) (Este documento de asuntos de consulta y compartición de información en menores extranjeros sin acompañante se encuentra archivado en *Committee on Energy & Commerce* de la Cámara de Representantes) 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 (25 de julio, 2019) (declaración de 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 (Marzo, 2019), https://immigrantjustice.org/sites/default/files/content-type/research-item/documents/2019-03/Children-as-Bait.pdf.

319. Ver National Coalition of State Legislatures, Detention of Migrant Children (24 de noviembre, 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 (12 de septiembre, 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 (19 de septiembre, 2019) (testimonio de 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 (En junio de 2019 hubo cerca de 2,600 menores sin acompañante retenidos en las estaciones de la patrulla fronteriza, cerca de la mitad estuvo bajo custodia durante 72 horas o más).

322. Ver carta para Kirstjen M. Nielsen, U.S. Department of Homeland Security, y Secretary Alex Azar, U.S. Department of Health & Human Services. (28 de noviembre, 2018), http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/govinfo/DHSLetter11.28.18.pdf.

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

324. Memorándum de Acuerdo 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 (11 de marzo, 2021) (Este documento se encuentra archivado en la 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. (11 de diciembre 2019).

330. Jeffrey S. Passel & D'Vera Cohn, U.S. Unauthorized Immigrant Total Dips to Lowest Level in a Decade, Pew Research Center (27 de noviembre de 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 (24 de julio, 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 (3 de abril, 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 (27 de febrero, 2020) (declaración Maribel Cortez a las 1:42:35)

340. Ver Erin Cox, Gov. Hogan opposed to ending ICE's warrantless access to driver's license database, Washington Post (27 de febrero, 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. Ver, i.e., 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. Ver, en lo general, The Census Act, 13 U.S.C. §1 et seq. (en 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. Ver también Kelly Percival, Federal Laws That Protect Confidentiality, Brennan Center for Justice (20 de febrero, 2019), https://www.brennancenter.org/our-work/research-reports/federal-laws-protect-census-confidentiality (resumen de leyes de confidencialidad del Censo).

343. Ver 13 U.S.C. §9(a)(1) (se prohíbe "el uso de información facilitada bajo las disposiciones de este título para cualquier propósito que no sean los fines estadísticos para los que se solicita"); §8(c) ("en ningún caso la información proporcionada [al Census Bureau] podrá usarse en detrimento de un encuestado o de otra persona a quien se relaciona tal información, excepto al perseguir supuestas violaciones de este mismo título,").

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

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

346. Ver Mark Hugo Lopez, Jeffrey S. Passel & D'Vera Cohn, Key facts about the changing U.S. unauthorized immigrant population, Pew Research Center (13 de abril, 2021), https://www.pewresearch.org/fact-tank/2021/04/13/key-facts-about-the-changing-u-s-unauthorized-immigrant-population/ ("Desde 2007 hasta 2017, el porcentaje de inmigrantes ilegales recién llegados (aquellos que llevaban menos de cinco años en EE.UU.) de otras regiones diferentes a Centro América y México -de las cuales la gran mayoría rebasan el tiempo permitido de su estadía- aumentó de 37% a 63%."); 8 U.S.C. § 1325(a) (delito menor de entrada indebida).

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

348. Ver, en lo general, i.e., Clare Garvie, Alvaro Bedoya & Jonathan Frankle, The Perpetual Line-Up: Unregulated Face Recognition in America (16 de octubre, 2016), https://www.perpetuallineup.org; Clare Garvie, Garbage In, Garbage Out (16 de mayo, 2019), https://www.flawedfacedata.com; Clare Garvie & Laura Moy, America Under Watch (16 de mayo, 2019), https://www.americaunderwatch.com/.

349. Ver, i.e., Kashmir Hill, Wrongfully Accused by an Algorithm, New York Times (24 de junio, 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 (29 de diciembre, 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 (28 de abril, 2019), https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html.

350. Ver, i.e., Asad L. Asad, On the Radar: System Embeddedness and Latin American Immigrants' Perceived Risk of Deportation 54 L. & Soc. Rev. 135 ("Los documentos pueden proteger contra la deportación pero también pueden aumentar los miedos, ya que las burocracias que 'documentan' a los inmigrantes tienen una mayor habilidad percibida para vigilarlos y expulsarlos."). id en 162 ("La legibilidad percibida al régimen de inmigración de los Estados Unidos a veces puede resultar en una evasión al sistema, como sucedió en el caso de Josefina, que vio al DACA como un camino para su 'captura'"); ver también Karen Hacker et al., Barriers to Health Care for Undocumented Immigrants, 8 Risk Mgmt. & Healthcare Pol'y 178 (2015) (Una revisión de la literatura muestra que "los inmigrantes [in]documentados reportaron estar evitando el servicio de atención médica y preferían esperar hasta que su situación fuera muy delicada para buscar atención; pues les preocupaba ser reportados por

las autoridades. Esto se vio en países tan diferentes como Francia, Estados Unidos y Dinamarca.”).

351. Ver supra Hallazgo 3; Drew Harwell, ICE investigators used a private utility database covering millions to pursue immigration violations, Washington Post (26 de febrero, 2021), https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data.

352. Ver supra Hallazgo 2.

353. Declaración del Presidente, The White House (7 de junio, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/06/07/statement-president (“Ahora, los programas de los que se ha hablado en la prensa en los últimos días son secretos en el sentido que están clasificados. Sin embargo, no son secretos en el sentido de que, cuando se trata de llamadas telefónicas, cada miembro del Congreso ha recibido un informe de este programa.”).

354. Jim Sensenbrenner, This abuse of the Patriot Act must end, The Guardian (9 de junio, 2013), https://www.theguardian.com/commentisfree/2013/jun/09/abuse-patriot-act-must-end.

355. Ver, i.e., U.S. Courts, Wiretap Report 2020 (31 de diciembre, 2020), https://www.uscourts.gov/statistics-reports/wiretap-report-2020.

356. Hay leyes federales que pretenden evitar que los gobiernos locales y estatales prohíban que se comparta información con el gobierno federal sobre los estatus migratorios de sus residentes. Académicos, y recientemente algunos jueces, han señalado la cuestionable constitucionalidad de estos estatutos. Hasta el día de hoy, los esfuerzos en las cortes judiciales para incitar a que los gobiernos limiten el alcance de los políticas santuario han tenido poco éxito. Sin embargo, los legisladores locales y estatales deberían estar conscientes de la existencia de estas leyes, y por lo tanto tomar medidas para crear leyes y políticas que eviten contravenirlas.

357. Ver The Sanctuary Values Act, D.C. Code § 24–211.07(a) (2020), disponible en https://code.dccouncil.us/us/dc/council/code/sections/24-211.07.html.

358. Ver, i.e., U.S. Immigration and Customs Enforcement,ervicio de Inmigración y Control de Aduanas de EE.UU., National Intellectual Property Rights Coordination Center (12 de enero, 2021), https://www.ice.gov/partnerships-centers/iprc.

359. Ver The Maryland Driver Privacy Act, H.B. 23 §4-320(g)(2) (2021) (restringir la compartición de datos de conductores a “agencias o agentes federales para fines de control migratorio”) id. en §4-320.1(B)(1) & (B)(2) (restringir el acceso a sistemas de reconocimiento facial por parte “de cualquier agencia federal que busque obtener acceso con fines de aplicación de la ley migratoria”).

360. Ver New York Vehicle & Traffic Code, Ch. 71, Title 2, Art. 2, §201 en 12(b).

361. Ver 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 (16 de enero, 2019), https://cmsny.org/publications/essay-2017-undocumented-and-overstays/.

362. Ver Hawaii Rev. Stat. § 286-104.5(h).

363. Ver, i.e., The Public Information Act, Md. Code Ann. § 4-101, en (j)(3) (excluyen de la definición de “expediente público” las imágenes digitales almacenadas por la Maryland Motor Vehicle Administration).

364. Ver Cal. Gov. Code, Title 1, Div. 7, Ch. 15.25 at § 7284.6(a)(1)(D) (una restricción en contra de que las autoridades policiales compartan las direcciones de los residentes añadida por la California Values Act, SB 54, 2017); Cal. Veh. Code, Div. 6, Ch. 1, Art. 3, § 12801.9(j) (prohibición contra la compartición de datos de conductores “excepto si es requerido por la ley,” como se añadió por SB 244, 2018); Cal. Gov. Code, Title 2, Div. 3, Part 6, Ch. 2.5 at § 15160(b)(1) (aclara que ningún usuario del California Law Enforcement Telecommunications System podría usar el sistema para obtener datos de los conductores o para aplicar ciertas disposiciones de la ley de inmigración, añadido por AB 1747, 2019).

365. Ver Cal. Veh. Code, Div. 2, Art. 1, Ch. 3 en § 1810.5. Ver carta de Sonia Huestis, Sonia Huestis, Deputy Dir., Commc’ns Programs Div., California Dep’t of Motor Vehicles, a Hon. Lorena Gonzalez, California Gen. Assembly (4 de febrero, 2019) (en archivo con Voice of San Diego); Maya Srikrishnan, How California Laws Meant to Integrate Immigrants Can Open a Backdoor for ICE, Voice of San Diego (19 de febrero, 2019), https://www.voiceofsandiego.org/topics/news/how-california-laws-meant-to-integrate-immigrants-can-open-a-backdoor-for-ice/ (se explica el contenido de la carta).

366. 8 U.S.C. § 1373 (2006).

367. Amy Howe, Court dismisses “sanctuary cities” petitions, SCOTUSblog (5 de marzo, 2021), https://www.scotusblog.com/2021/03/court-dismisses-sanctuary-cities-petitions/.

368. Ver Hearing before Maryland House of Delegates Environment & Transportation Committee (27 de febrero, 2020) (Testimonio de Del. Dana Stein, D - Baltimore County, Dist. 11, for H.B. 892) (“Antes de una visita al Departamento el año pasado, tenía entendido que este no podía determinar las fechas y momentos en que ICE había tenido acceso al MIRS. Sin embargo, durante una visita legislativa en octubre pasado, nos dijeron que el Departamento sí podía determinar las fechas de acceso al sistema por parte de ICE. También recibimos una carta de seguimiento del departamento en donde se confirmaba esta información.”).

369. Ver, i.e., 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 (última visita, 30 de noviembre, 2021) (“La National Consumer Telecom & Utilities Exchange (NCTUE) es una agencia de informes crediticios que mantiene datos como historiales de cuentas y pagos en servicios como telecomunicaciones, televisión de paga e industrias de servicios públicos, y que son creados por los proveedores miembros de dicha agencia.”).

371. Ver, i.e., Ariz. Admin. Code R14-2-203 (2021) (“2. La información específica de los clientes no deberá ser revelada sin la autorización previa por escrito del consumidor, a

menos que esta sea… requerida de manera aceptable, ya sea para actividades legítimas sobre resúmenes informativos de la cuenta, o que sea necesaria para ofrecer un servicio seguro y confiable al cliente"); Code Del. Regs. 26 3001 ("3.3.4 Un proveedor de servicio eléctrico podría revelar el historial de facturación, pagos e información crediticia de un cliente para el solo propósito de facilitar la facturación, cobranza, y realización de informes crediticios.").Md. Code Regs. 20.53.07.02 ("B. Un proveedor podrá revelar la información de facturación, pagos e información crediticia de un cliente para el solo propósito de facilitar la facturación, cobranza, y realización de informes crediticios.").

372. Ver, i.e., Colo. Code Regs. § 723-3:3027(b) (regulación de compañías de servicio eléctrico: "Una compañía de servicios públicos no divulgará datos de los consumidores a menos que esta divulgación cumpla con las reglas aquí presentadas; excepto según lo requiera la ley o para cumplir con la normativa de la Comisión. De manera ilustrativa, esto incluye respuestas a solicitudes de la Comisión, órdenes judiciales, citatorios, autorizaciones judiciales, o como lo autoriza la § 16-15.5-102, C.R.S."); 4 Colo. Code Regs. § 723-3:3001(i)("'Datos de clientes' significa información o datos específicos de los clientes, excluyendo información personal, como se define en el párrafo 1004 (x)…").; 4 Colo. Code Regs. § 723-1:1004(x) ("'Información personal' significa lo siguiente: …el nombre del cliente únicamente en combinación con cualquiera de los otros elementos informativos enumerados y relacionados a dicho cliente…").

373. Ver Conn. Agencies Regs. 16-47a-1 at (3) (define explícitamente "información del cliente" en donde se incluye la dirección); Conn. Agencies Regs. 16-47a-3 at (b) ("Excepto cuando se permita lo contrario, bajo este Gas Code of Conduct, ninguna compañía de gas o afiliada deberá divulgar información del cliente a ninguna persona o compañía sin el consentimiento de este último, y sólo entonces en la medida que se haya comunicado al cliente de manera específica."); en (f) ("A pesar de las prohibiciones establecidas en esta sección, una compañía de gas podría divulgar información del cliente a un afiliado (incluyendo CSC) o a un tercero no afiliado con el fin de proporcionar a la compañía de gas bienes o servicios (incluyendo servicios de apoyo corporativo, como servicio al cliente, facturación y cobranza), y tras un acuerdo explícito de confidencialidad de esta información del cliente.").

374. El Plan Biden para asegurar nuestros valores como una Nación de Inmigrantes, Biden para Presidente, 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 (26 de octubre, 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 (13 de agosto, 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 (última visita 21 de junio, 2021). Ver también Jack Poulson, Reports of a Silicon Valley/Military Divide Have Been Greatly Exaggerated, TechInquiry (7 de julio, 2020), https://techinquiry.org/SiliconValley-Military/ ("Si bien la FPDS es la fuente definitiva para datos de las contrataciones del gobierno federal de EE.UU., se sabe que han tenido varios errores, tales como inconsistencias e inexactitudes en las cantidades de las adjudicaciones, información incompleta y una documentación lenta e incompleta de los documentos subidos por los funcionarios a cargo (incluyendo retrasos de 90 días para contrataciones del Department of Defense), así como frecuentes correcciones que se llevan a cabo años después de haberse firmado.").

379. USAspending recaba su información del Federal Procurement Data System (FPDS), el cual no comparte datos sobre los pagos y gastos reales de ICE. Como resultado, los gastos de esta agencia no se incluyen en la información sobre adjudicaciones. Ver Analyst's Guide to Federal Spending Data, USAspending Data Lab, https://datalab.usaspending.gov/analyst-guide/ (última visita, 21 de junio, 2021).

380. Una obligación es una "promesa hecha por el gobierno para gastar fondos." Id.

381. Ver Poulson, supra nota 378.

382. Ver Apéndice B.

383. USAspending, https://www.usaspending.gov/.

384. Decidimos establecer estas categorías a medida que revisábamos los contratos de vigilancia de ICE y notamos funciones comunes de vigilancia adquiridas por ICE.

385. Ver, i.e., National Immigration Law Center, Glossary at a Glance: Immigration Databases, Information Sharing Systems, and Case Management Systems (Agosto. 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 (2 de febrero, 2021), https://www.top10vpn.com/research/ice-surveillance-contracts/.

386. Cualquier contrato dado puede tener múltiples transacciones asociadas. Cuando señalamos una transacción como asociada con una de las funciones de vigilancia establecidas, entonces señalamos el contrato entero.

387. Ver Electronic Frontier Foundation, Street-Level Surveillance (28 de agosto, 2017), https://www.eff.org/pages/cell-site-simulatorsimsi-catchers.

388. U.S. Census Bureau, North American Industry Classification System (5 de enero, 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; Ver también 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/celediting#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. Carta de Craig L. Caesar a Assistant Attorney Gen. Hon. Charles A. James 3 (17 de agosto, 2001), https://www.justice.gov/atr/page/file/1019991/download ("los miembros fundadores que se convertirián en la NCTUE son: AT&T Corp.; BellSouth Telecommunications, Inc.; Citizens Communications, Inc; Global Crossing, Inc.; Broadwing Communications, Inc.; Verizon Long Distance Company; Sprint Communications Company LP y MCI Telecommunications, Inc."); Equifax Insights, More Bang for Your Bucks with the NCTUE(R), Youtube (15 de marzo, 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. Carta de Craig L. Caesar, supra nota 396; Equifax Insights, More Bang for Your Bucks with the NCTUE(R), supra nota 396. Algunas filiales de Verizon parecen no ser miembros de la NCTUE. Por ejemplo, en 2016 se le negó a Verizon New York Inc.'s la solicitud de membresía. 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 (22 de abril, 2016), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId=%7BB4A93370-7B4C-43EF-AC41-B6963122089C%7D.

399. Carta de Craig L. Caesar, supra nota 396.

400. Id.

401. Id.

402. Equifax Insights, supra nota 396.

403. Carta de Craig L. Caesar, supra nota 396, en 3 n.4 (Estas personas designadas representan a American Electric Power; Baltimore Gas & Electric; Duke Power; y Southern Company, compañías que han estado activas en los intercambios regionales de servicios públicos."

404. Id.

405. Id.

406. Equifax, NCTUE Association Infographic, http://assets.equifax.com/assets/corp/nctue-association-infographic.pdf ("Además de la cancelación de deudas de $1,000,000, Georgia Power utilizó a NCTUE para anticipar los resultados que le ayudarían a evitar la deuda").

407. Id. ("Con esta información emparejada proveniente de NCTUE, PSNC Energy encontró que su ritmo de realización de contratos es 41 por ciento más alto que antes.").

408. Equifax Insights, supra nota 396.

409. NCTUE Users Conference: We're Better Together, supra nota 397.

410. Equifax Insights, supra nota 396.

411. NV Energy usa el Equifax Advanced Energy Risk Model para evaluar los riesgos crediticios de los consumidores. Public Utilities Commission of Nevada, Respuesta de Nevada Power Company d/b/a NV Energy y Sierra Pacific Power Company d/b/a NV Energy a la orden procesal No. 1 8 (7 de octubre, 2016), https://drive.google.com/file/d/1Jnf_Vny3n1xcKkpgp3l3HTN53Drjp-ev/view?usp=sharing. De acuerdo con una hoja de descripción de producto de Equifax, el marcador Advanced Energy Plus toma datos de la NCTUE y solo está disponible para miembros del NCTUE. Equifax, Advanced Energy Plus (3 de marzo, 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 (Marzo 2017), https://mi-psc.force.com/sfc/servlet.shepherd/version/download/068t0000001UXldAAG ("Basándonos en una combinación de datos de la base de datos de NCTUE (National Consumer Telecom & Utilities Experience [sic]), así como información histórica disponible en SAP, este proyecto usará un modelo de puntuación de riesgo para reducir nuestra exposición al realizar cobranzas antes de que se avance y emprenda un procedimiento de reclamación más agresivo sobre nuestros clientes de alto riesgo").

413. Miami-Dade County Water and Sewer Department, Contract/Project Measure Analysis and Recommendation for Credit and Risk Assessment Services, Miami-Dade County (22 de marzo, 2019), http://www.miamidade.gov/smallbusiness/library/reports/sbe/bw9744-0-22-project-package.pdf (El *Miami-Dade County's Water and Sewer Department* es un miembro de la *National Consumer Telecom and Utilities Exchange* (NCTUE), un consorcio de más de 95 compañías miembros para empresas de servicios públicos, telecomunicaciones e industrias de televisión de paga. La NCTUE proporciona a sus miembros servicios de verificación de riesgos crediticios diseñados especialmente para las compañías de servicios públicos.").

414. Duke Energy, Duke Energy notifying Midwest customers of payment reporting error, Duke Energy News Center (7 de octubre, 2014), https://news.duke-energy.com/releases/duke-energy-notifying-midwest-customers-of-payment-reporting-error (Duke Energy "ya no reporta datos de pagos a la NCTUE, D&B o ECS. Toda la información anteriormente reportada a la NCTUE ha sido bloqueada y ya no puede ser utilizada por otro para decisiones crediticias").

415. Audiencia ante la 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 (18 de marzo, 2016), https://www.edockets.state.mn.us/EFiling/edockets/searchDocuments.do?method=showPoup&documentId=%7B0BE6F0A7-DEC7-42D5-9BC9-B626E74F4BDE%7D&documentTitle=20163-119256-01 ("Sin embargo, con el fin de asegurar que se cumpla con la orden del 24 de junio de 2014 emitida por la Minnesota Public Utilities Commission, la cual exige que las empresas de servicios públicos adopten y documenten los procesos relacionados con la información de identificación personal, otras acciones y órdenes relacionadas contenidas en Docket No. E,G999/CI-12-1344, MERC no planea participar en la [NCTUE].").

GEORGETOWN LAW
Center on Privacy & Technology