Vigilancia Bajo ICE: Documentos obtenidos revelan un alarmante aumento de vigilancia en el programa ISAP

Contexto:

Desde el año 2004, el Servicio de Control de Inmigración y Aduanas (ICE) le ha pagado miles de millones de dólares a BI Inc., una subsidiaria de la empresa desarrolladora de prisiones privadas Geo Group, para que dirija su Programa de Comparecencia y Supervisión Intensiva[1] (ISAP, por sus siglas en inglés), un programa de vigilancia electrónica que se mercadea como una "alternativa a la detención". Actualmente, ICE somete a más de 200,000 inmigrantes a diversas formas de vigilancia a través de ISAP. Entre ellas se encuentran los grilletes de tobillo con GPS y SmartLINK, una aplicación para teléfonos celulares lanzada por ICE durante el gobierno de Trump para rastrear y vigilar a las personas por medio del reconocimiento facial, el reconocimiento de voz y la ubicación.

Las comunidades inmigrantes vienen documentando desde hace tiempo los efectos perdurables del trauma que provocan estas formas electrónicas de encarcelación, también llamadas prisiones digitales. Veinticinco miembros del Congreso han expresado su preocupación en relación con el "aumento drástico" del programa ISAP y el "terrible daño emocional y mental" que provoca esta vigilancia punitiva. Sin embargo, el gobierno de Biden ha aumentado masivamente el financiamiento para ISAP, en tanto ICE ha agregado recientemente pulseras digitales de localización con GPS a la lista de las tecnologías de vigilancia de ISAP. Además, ICE recientemente solicitó propuestas nuevas de empresas para gestionar el sistema de vigilancia electrónica de la agencia, lo cual indica que está planificando una expansión de este programa de encarcelamiento electrónico.

En el año 2022, las organizaciones Just Futures Law, Mijente Support Committee y Community Justice Exchange demandaron a ICE para obligar a la agencia a revelar qué información se recolecta a través de ISAP y cómo se utiliza. Las organizaciones están representadas por Samuelson Law, Technology & Public Policy Clinic, de la Escuela de Derecho de la Universidad de California en Berkeley.

1 Según el Centro de Información de Acceso a Registros Transaccionales (TRAC), ICE y BI han publicado repetidas veces información errónea en relación con la cantidad de individuos y de familias que han sometido a la vigilancia de ISAP. Véase el documento False Reporting by Contractor on Alternatives to Detention Activities [Informes falsos del contratista sobre las actividades en el marco de las alternativas a la detención], TRAC (7 de marzo de 2023): https://trac.syr.edu/reports/710/ [https://perma.cc/WDK8-ZUJV].

Aprendizajes Clave:

Esta hoja informativa enumera los hallazgos más importantes en relación con la vigilancia de ISAP a partir de los documentos de ICE obtenidos gracias a nuestra demanda amparada bajo la ley FOIA. A continuación se describen algunos aprendizajes clave de nuestra revisión:

- **El programa ISAP de ICE está en continua expansión y es un proyecto de vigilancia masiva.** A través de ISAP, la agencia rastrea a cientos de miles de inmigrantes y sus familias por medio de múltiples tecnologías de encarcelación electrónica. ICE usa ISAP para extraer enormes cantidades de información personal altamente sensible de las comunidades de inmigrantes, y almacena gran parte de estos datos sensibles durante 75 años.

- **Las declaraciones públicas en las que ICE afirma que protege los datos y la privacidad de las personas bajo vigilancia por ISAP no son fiables.** Tal como revelan los registros obtenidos en virtud de la ley FOIA, las prácticas de vigilancia que actualmente implementa ICE a través de ISAP a menudo contradicen las declaraciones de ICE y del Departamento de Seguridad Nacional (DHS), que minimizan el alcance de la vigilancia de ISAP. Estas discrepancias dan cuenta del inescrupuloso sistema de extracción de datos y vigilancia electrónica de ICE, y sugieren que la agencia no es capaz de respetar ni siquiera sus propias políticas de privacidad. Por ejemplo, hay múltiples incoherencias en relación con el alcance de la vigilancia continua de la ubicación a la que ICE somete a las personas, a través de la aplicación SmartLINK.

- **En términos generales, los hallazgos demuestran que el objetivo principal de ICE no es crear un programa más humano, sino ampliar el control punitivo de la agencia sobre la vida y la autonomía de las comunidades negras y migrantes.**

Hallazgo #1: La agencia ICE y su contratista privado, BI, extraen y retienen un amplio espectro de datos de los inmigrantes sometidos a sus programas de monitoreo electrónico.

Extracción de datos: En nombre de ICE, BI recolecta una enorme cantidad de información de carácter personal sobre las personas sometidas a ISAP. Gran parte de esa información se extrae a través de tecnologías como la aplicación móvil SmartLINK y los grilletes de tobillo con GPS. Esta información incluye:[2]

- **Información de identificación personal** (domicilio, correo electrónico, número de teléfono, fecha de nacimiento, número de seguro social,[3] número de visa y pasaporte, información laboral, información educativa, información financiera, afiliación religiosa, raza, género, etc.)
- **Datos biométricos e información física y sobre la salud** (imágenes faciales, impresiones de voz, peso, altura, tatuajes, cicatrices, información médica, discapacidades, embarazos y partos,[4] etc.)
- **Datos de geolocalización**
- **Números de teléfono de contactos cercanos**[5]
- **Expedientes judiciales de inmigración**
- **Datos de vehículo y conductor** (por ejemplo, número de placa, número de licencia de conducir, número de inscripción de vehículo)
- **Datos de vigilancia comunitaria** (por ejemplo, información sobre los lazos de una persona en el hogar, en el vecindario o en la comunidad)

Derechos de propiedad de los datos: Si bien BI recolecta y guarda los datos de ISAP, ICE tiene los derechos de los datos (lo que incluye sistemas de información y bases de datos creados por BI). Según los registros de la FOIA, el contrato de ICE con BI señala que la agencia "tendrá derechos ilimitados para usar, disponer o revelar" todos los datos de ISAP, incluyendo los metadatos.[6] Esto sugiere que ICE tiene la capacidad de usar los datos de ISAP del modo que desee; por ejemplo, puede combinar esa información con otras bases de datos o puntos de datos para acceder a una vigilancia aún más detallada sobre la vida de las personas sometidas a ISAP.

Retención de datos: Los datos de ISAP se retienen durante 75 años. Se trata de una recolección de datos casi permanente a través de la vigilancia electrónica a la que ICE somete a las personas. Sin embargo, los registros de la FOIA y la Evaluación de impacto en la privacidad (PIA) sobre ISAP divulgada públicamente por el Departamento de Seguridad Nacional (DHS) muestran en conjunto la información confusa, enmarañada y a veces contradictoria sobre la retención de datos por parte de ISAP.

2 La Oficina de Privacidad del DHS y BI han reconocido públicamente que ISAP recolecta muchos de estos puntos de datos. Los documentos de la FOIA señalan que ISAP recolecta además otros tipos de información, como por ejemplo los números de visas. Véase Departamento de Seguridad Nacional de EE. UU., Privacy Threshold Analysis [Análisis de umbral de privacidad] 8 [de aquí en más Prod. 1, PTA], https://www.law.berkeley.edu/wp-content/uploads/2022/05/2022-09-23_ISAP-FOIA_ICEProduction1_PrivacyThresholdAnalysisVer06-2020.pdf [https://perma.cc/LCP5-4884]. Además, los registros muestran que el ISAP recolecta información sobre expedientes judiciales, tatuajes y cicatrices, discapacidades y "lazos comunitarios". Durante las visitas a los hogares, BI tiene la orden de recolectar información sobre "la disposición de la residencia", "las personas que viven en la residencia", "mascotas, niños, cercas, sistemas de entrada, detalles de la propiedad", y "actividad delictiva vinculada con el participante, la propiedad o el vecindario". Véase Departamento de Seguridad Nacional de EE. UU., Statement of Work [Declaración de trabajo]17-18 [de aquí en más Prod. 3, Statement of Work],https://www.law.berkeley.edu/wp-content/uploads/2022/05/2022-12-09_ISAP-FOIA_ICEProduction3_ISAP4-SectionCStatementOfWork.pdf [https://perma.cc/P4FL-ASSA].

Por ejemplo, la Evaluación de impacto a la privacidad (PIA) del DHS afirma que los registros de ISAP se mantienen en la Base de Datos Integrada de Organismos de Cumplimiento de la Ley[7] (EID, por sus siglas en inglés) de ICE, una gigantesca base de datos que usan todas las agencias del DHS y que exige que todos los registros deben destruirse 75 años después de la fecha de ingreso a la base de datos. Además, señala que BI almacena los datos de ISAP, lo que incluye la información obtenida a través de SmartLINK, en la base de datos "Total Access" de BI hasta 7 años después de que alguien sale del programa. Pero esto contradice los registros de la FOIA. En algunas instancias, estos documentos señalan que BI "no destruirá ni alterará ningún registro ni bitácora" relativos al contrato, lo que sugiere que es posible que BI guarde los registros indefinidamente.[8] En otras instancias, los documentos de la FOIA señalan que los registros de BI en el sistema Total Access son "una extensión" del sistema EID de ICE,[9] lo que sugiere que ICE retiene durante 75 años al menos algunos de los datos que recolecta BI en Total Access.

El DHS afirma que la información que se recolecta en el Programa de Gestión de Casos de Jóvenes Adultos (un nuevo programa de ISAP que monitorea a jóvenes de entre 18 y 19 años) se conservará de forma permanente.

Nota: Los documentos de la FOIA muestran que, en el 2021, BI le señaló a ICE que podía almacenar "datos históricos" sobre los participantes de ISAP en "cintas de respaldo", una práctica de retención que excede el periodo de 7 años de retención.[10]

Hallazgo #2: Los registros de la FOIA contradicen las declaraciones de ICE, que afirman que la vigilancia se limita a datos de ubicación y telefónicos, particularmente cuando se trata de vigilancia a través de SmartLINK.

3 En su Política de privacidad, BI afirma que SmartLINK recolecta los números de seguridad social con fines comerciales. Esto contradice los registros de la FOIA, donde se afirma que ISAP no recolecta números de seguridad social. Véase Prod. 1, PTA, nota 2, pág. 9.

4 Los documentos de la FOIA muestran que a las personas que están en ISAP les exigen notificar "de inmediato" a BI o a ICE si han quedado embarazadas, si han dado a luz, si se incorporó un nuevo hijo, si han sido hospitalizadas, si se enfermaron o se lastimaron gravemente, si recibieron una multa o si han sido arrestadas. Véase Departamento de Seguridad Nacional de EE. UU., Intensive Supervision Appearance Program Participant Handbook [Manual del participante de supervisión intensiva] 3 [de aquí en más Prod. 2, ISAP IV Handbook], https://www.law.berkeley.edu/wp-content/uploads/2022/05/2022-12-09_ISAP-FOIA_ICEProduction2Re-Release_ISAP-IVParticipantHandbookEnglish.pdf [https://perma.cc/YSB3-6U3T]. BI debe notificar a ICE sobre partos, embarazos, fechas de parto estimadas e información personal sobre el "padre del niño" (nombre, domicilio, país de ciudadanía y número de teléfono). Prod. 3, Statement of Work, véase nota 2, págs. 28-29.

5 A las personas que se encuentran bajo vigilancia de ISAP se les exige brindar la información de sus contactos cercanos (parientes y amigos). Los registros de la FOIA muestran que ICE le exige a BI presentar informes diarios, semanales, mensuales, trimestrales o anuales. Por ejemplo, los "informes de inteligencia" se elaboran "según sea necesario" y pueden incluir información como "cuántas veces utilizó un número de teléfono un participante o contacto personal". Véase Prod. 3, Statement of Work, nota 2, pág. 33.

6 Los registros de la FOIA indican que ICE no considera el contrato de ISAP como un "contrato de tecnología de la información". Por lo tanto, BI parece estar exento de algunas normas de privacidad que regulan el uso de datos personales. Por ejemplo, a BI no se le prohíbe usar los datos de ISAP que contengan información de identificación personal con fines de capacitación o de realización de pruebas. Véase Departamento de Seguridad Nacional de EE. UU., Special Contract Requirements [Requisitos contractuales especiales]131 [de aquí en más Prod. 4, Contract Requirements], https://www.law.berkeley.edu/wp-content/uploads/2022/05/2022-12-15_ISAP-FOIA_ICEProduction4_ISAP4-SectionHSpecialContractRequirements.pdf [https://perma.cc/36Z6-PVUN].

7 La Base de Datos Integrada de Organismos de Cumplimiento de la Ley es una base de datos que usan todos los componentes del DHS, incluidos ICE, USCIS y CBP, que almacena datos vinculados con la "investigación, los registros de detención, la detención y la expulsión", y guarda esos registros durante 75 años. Véase DHS/ICE/PIA-015 Enforcement Integrated Database [Base de datos integrada DHS/ICE/PIA-015], Departamento de Seguridad Nacional (mayo del 2019), https://www.dhs.gov/publication/dhsicepia-015h-enforcement-integrated-database-eid-criminal-history-information-sharing.

8 Prod. 3, Statement of Work, véase nota 2, pág. 38.

9 Prod. 1, PTA, véase nota 2, pág. 11.

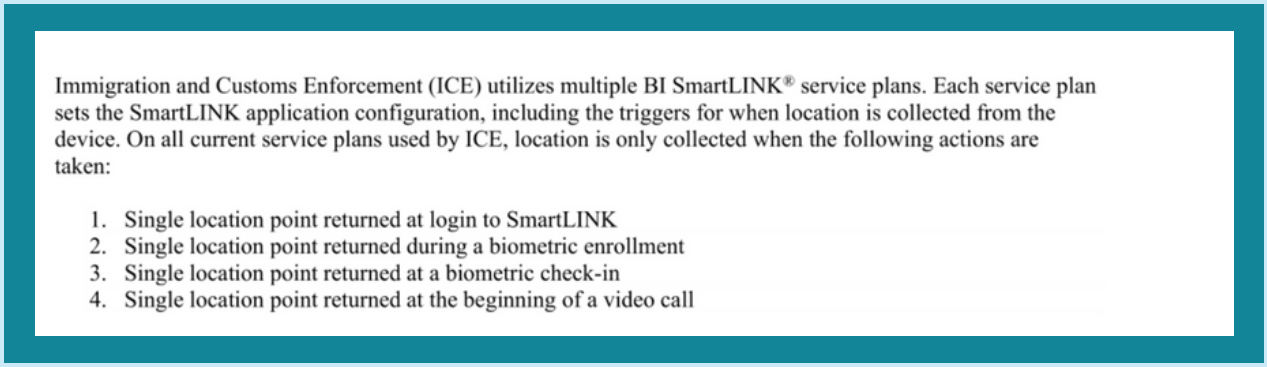
10 Departamento de Seguridad Nacional, BI Inc. Technical Proposal [Propuesta técnica de BI Inc.] 54 [de aquí en más Prod. 5, ISAP IV], https://www.law.berkeley.edu/wp-content/uploads/2022/05/2023-01-19_ISAP-FOIA_ICEProduction5_ISAP4-Attachment15.pdf [https://perma.cc/JNK4-YZ7L].

Vigilancia de datos telefónicos: Los documentos de la FOIA muestran que BI ha declarado que SmartLINK informa sobre el estado de "la cobertura de datos móviles, la conectividad de WI-FI y los servicios de localización", y que la aplicación notificará a ICE o a BI "cuando estos servicios se desactiven".[11] Esto implica que, si las personas intentan limitar o cambiar la configuración de localización de su teléfono, es posible que ICE o BI se enteren. Sin embargo, esto contradice las declaraciones de ICE en relación con la vigilancia telefónica. En su sitio web, ICE afirma que SmartLINK no puede acceder a la información de los dispositivos personales, incluyendo fotos, actividad de navegación o mensajes de texto fuera de la aplicación.

Nota: La política de privacidad de SmartLINK de BI afirma que BI recolecta o recibe los siguientes puntos de datos de los usuarios de SmartLINK: "información comercial sobre transacciones pasadas y futuras", actividad de internet y redes, e información sobre dispositivos como "identificadores de dispositivos, dirección IP, conexiones a internet, sistema operativo, tipo de navegador, redes móviles, información sobre la batería y el número de teléfono del dispositivo".[12] Cabe destacar que la dirección IP y otros datos de dispositivos pueden usarse para recopilar información general sobre la ubicación.

Vigilancia de la ubicación:[13]

SmartLINK: Los documentos de la FOIA señalan que SmartLINK rastrea los datos de ubicación durante el inicio de sesión, en la inscripción biométrica, en las verificaciones y al comienzo de una videollamada.[14]



Immigration and Customs Enforcement (ICE) utilizes multiple BI SmartLINK® service plans. Each service plan sets the SmartLINK application configuration, including the triggers for when location is collected from the device. On all current service plans used by ICE, location is only collected when the following actions are taken:

1. Single location point returned at login to SmartLINK
2. Single location point returned during a biometric enrollment
3. Single location point returned at a biometric check-in
4. Single location point returned at the beginning of a video call

Figura 1: Acuerdo de Participante de SmartLINK de BI para el ISAP, obtenido de los documentos de la FOIA por Just Futures Law

11 Departamento de Seguridad Nacional, BI Inc. SmartLINK Agreement [Acuerdo de SmartLINK]1 [de aquí en más Prod. 2, SmartLINK Agreement], https://www.law.berkeley.edu/wp-content/uploads/2022/05/2022-12-09_ISAP-FOIA_ICEProduction2Re-Release_SmartLinkParticipantAgreement-07112022.pdf [https://perma.cc/Q92V-QBJM].

12 Además, la política de privacidad de SmartLINK le permite a BI revelar información personal a terceros (por ejemplo, a sus contratistas, proveedores de servicios, subsidiarias y filiales). Véase BI SmartLINK Privacy Policy [Política de privacidad de SmartLINK de BI], BI Inc.(18 de marzo del 2022), https://bi.com/bi-smartlink-privacy/. Esto contradice lo que se afirma en el sitio web de ICE, donde se señala que los datos de SmartLINK no se comparten con terceras partes. Véase Alternatives to Detention Frequently Asked Questions [Preguntas frecuentes sobre las alternativas a la detención], Servicio de Inmigración y Control de Aduanas, https://www.ice.gov/atd-faq.

13 ICE exige que las personas bajo vigilancia de ISAP tengan una tarjeta de identificación de participante que incluya su nombre, foto, fecha de nacimiento y un código de barras. No queda claro si estas identificaciones rastrean la ubicación. Los documentos de la FOIA muestran que ICE le ha dado instrucciones a BI de escanear la tarjeta de identificación durante las visitas al hogar y al trabajo, y señalan que en el caso de las visitas en el hogar "El escaneo de la tarjeta de identificación debe verificar que la visita se realizó en la residencia con un dispositivo que registra las coordenadas de GPS y el domicilio más cercano del escaneo". Véase Prod. 3, Statement of Work, nota 2, pág.17.

14 Véase Prod. 2, SmartLINK Agreement, nota 10, pág. 4.

Nota: Los documentos de la FOIA contradicen las declaraciones públicas del DHS y la agencia ICE sobre la vigilancia de la ubicación a través de SmartLINK. Por ejemplo, la Evaluación de impacto en la privacidad (PIA) del DHS establece que los datos de ubicación se recolectan únicamente durante las inscripciones y las verificaciones (no en los inicios de sesión ni en el comienzo de una videollamada). El DHS y la agencia ICE no solo contradicen los documentos de la FOIA, sino que también se contradicen entre sí. El DHS declara en otra sección de la evaluación PIA que se puede acceder a los datos de ubicación "cuando la aplicación está abierta", lo que sugiere que podrían recolectarse datos cuando la aplicación está en segundo plano. De manera preocupante, ICE declara públicamente que SmartLINK es capaz de monitorear los datos de ubicación de manera continua si la aplicación está en un dispositivo de BI (no en un teléfono celular personal). Según ICE, esta característica "actualmente está inactiva".

Estas incoherencias dan cuenta del carácter inescrupuloso e ilimitado de una vigilancia invasiva, y plantean graves banderas rojas en relación con la verdadera naturaleza de lo que está ocurriendo. No hay nada que le impida al ICE cambiar (o ignorar) su práctica declarada y en cambio rastrear datos de ubicación de manera continua a través de la aplicación SmartLINK; de hecho, algunos informes indican que esto ya está ocurriendo. Un artículo reciente presentó el caso de un agente de ICE en Houston que estaba rastreando "los movimientos de una persona con la aplicación SmartLINK de BI a lo largo de 24 horas".[15] Esto sugiere que los agentes de ICE rastrean la ubicación continuamente, a pesar de que ICE sostiene lo contrario.

Grilletes de tobillo con GPS: La agencia ICE y la empresa BI rastrean de manera continua la ubicación precisa de las personas a las que se les exige usar todos los días, las 24 horas, grilletes de tobillo con GPS que son físicamente y psicológicamente nocivos. La ubicación precisa se indexa automáticamente en el sistema de BI cada 4 horas.[16] ICE o BI pueden acceder a "actualizaciones automáticas de la ubicación en tiempo real", así como a "coordenadas paso a paso" de la persona que utiliza la aplicación.[17] Como tienen acceso a los registros de los datos de ubicación históricos que recogen los grilletes de tobillo en el transcurso del tiempo, ICE y BI pueden observar la vida de una persona durante meses o años; por ejemplo, cada vez que llevan a sus hijos a la escuela, a una clínica de salud, a un lugar de culto, a la casa de un familiar, etc.

Nota: BI elabora informes de datos GPS para ICE "según sea necesario".[18] Estos informes pueden incluir los "patrones de ubicaciones habituales" de una persona. Por ejemplo, "la cantidad de veces que acude a ubicaciones específicas en relación con los días de la semana y los horarios del día". En otras palabras, ICE puede pedir un mapa detallado de la vida diaria de una persona y las actividades que realizan en cualquier momento.

15 Elizabeth Trovall, The growing business of immigrant surveillance [El próspero negocio de la vigilancia sobre los inmigrantes], Marketplace (2 de agosto del 2023), https://www.marketplace.org/2023/08/02/the-growing-business-of-immigrant-surveillance/.

16 Véase Prod. 1, PTA, nota 2, pág. 5.

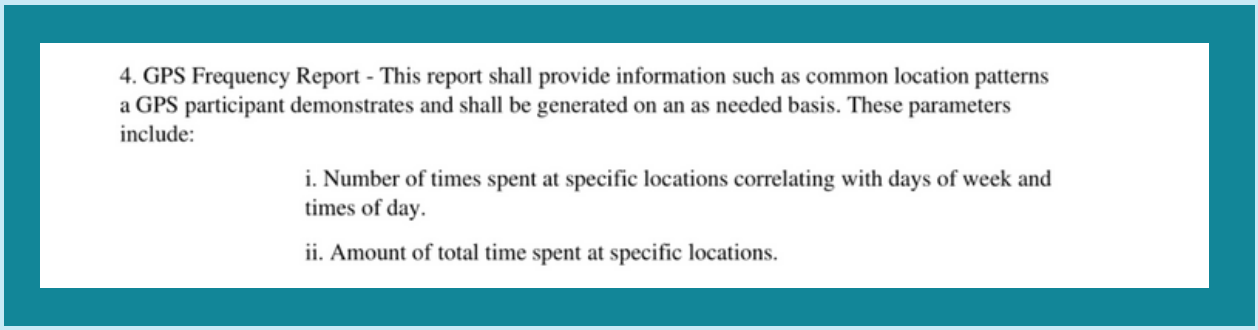


Figura 2: Contrato del ISAP IV de BI, obtenido de los registros de la FOIA por Just Futures Law

Hallazgo #3: Los documentos de la FOIA muestran que ICE usa los datos ISAP para ubicar y arrestar en masa a miembros de la comunidad.[19]

Los documentos de la FOIA confirman que ICE usa ISAP para elegir personas para deportación. Por ejemplo, en el año 2018, al parecer un grupo de empleados de ISAP de BI en Manassas (Virginia) colaboró con ICE para llevar adelante el arresto masivo de 40 personas, lo que incluyó el aporte de datos de geolocalización que le permitieron a ICE detectar la ubicación de las personas escogidas para el arresto. BI llamó a esta operación "el arresto coordinado más grande de la historia de ISAP en la oficina local de Washington D.C.".[20]

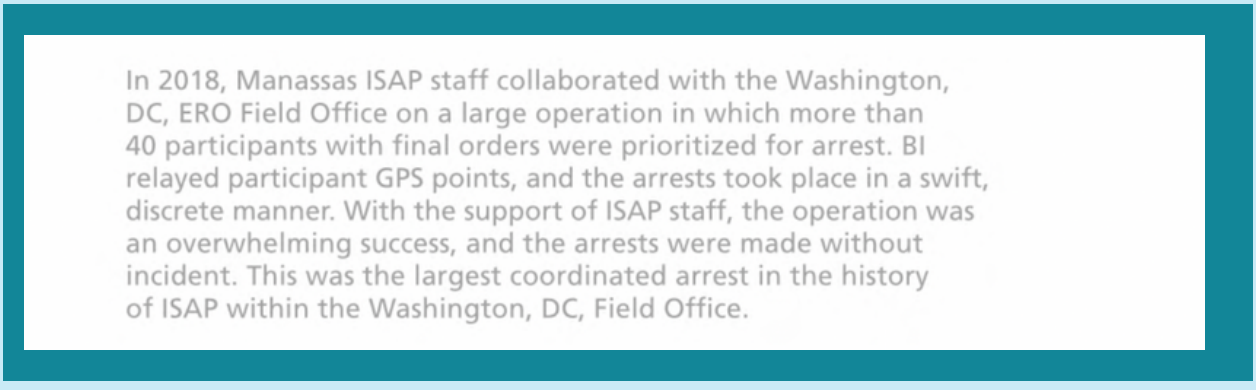


Figura 3: Datos extraídos de los documentos de la FOIA obtenidos por Just Futures Law

Hallazgo #4: BI brindó acceso a ICE a otros datos de vigilancia para sus iniciativas de deportación, y escogió particularmente jurisdicciones santuario que limitan el acceso de ICE a los datos.

17 Departamento de Seguridad Nacional., Attachment 1: Detailed GPS Ankle Bracelets And Tracking/Monitoring System, Telephonic Reporting System, Biometric Reporting System [Anexo 1: Sistema detallado de grilletes de tobillo con GPS y rastreo/monitoreo, sistema de informes telefónicos, sistema de informes biométricos],2-3 [de aquí en más Prod. 4, Attachment 1], https://www.law.berkeley.edu/wp-content/uploads/2022/05/2022-12-15_ISAP-FOIA_ICEProduction4_ISAP4-Attachment1.pdf [https://perma.cc/BL54-QXAX].

18 Prod. 3, Statement of Work, véase nota 2, pág. 3

Los documentos de la FOIA muestran que, en el año 2021, BI llevó adelante un programa piloto de 60 días para monitorear los datos de encarcelación y arresto de casi 10,000 personas que estaban bajo vigilancia de ISAP. Durante el piloto, BI le brindó acceso a ICE a la información de registros de ingreso a las cárceles, lo que incluía "notificaciones diarias de arrestos y encarcelaciones, junto con la información de ingresos, transferencias y liberaciones".[21] BI se asoció con un tercero, una empresa llamada ClearForce que brindaba esa información sobre encarcelamientos, obtenida de cárceles en todo el país. BI señaló que el programa fue "crucial para obtener datos de jurisdicciones santuario, que ICE generalmente ya no recibe", e informó que la mayoría de las personas arrestadas durante el piloto (el 57%) eran "residentes de los siete 'Estados Santuario'". Esos estados son California, Nueva York, Nueva Jersey, Washington, Oregón, Colorado e Illinois.

BI le propuso a ICE usar el programa de datos de encarcelación en el futuro para rastrear la "actividad delictiva" de "personas de interés, ya estén dentro o fuera del programa de ATD".[22] Es sumamente inquietante que ICE utilicé empresas como BI, así como empresas de recolección de datos como LexisNexis, para crear lagunas legales respecto de las leyes locales que limitan la colaboración con ICE y protegen a las comunidades de inmigrantes.

Hallazgo #5: BI participa muy activamente en las decisiones de expulsar personas del programa de Servicios Extendidos de Gestión de Casos (ECMS) de ICE y someterlas a formas aún más invasivas de vigilancia de ISAP.

Una serie de corporaciones carcelarias, organizaciones sin fines de lucro y agencias de servicios sociales en todo el país colaboran con ICE para monitorear a personas jóvenes y adultas[23] a través de varios programas de "gestión de casos" de ISAP.

Uno de estos programas es el de Servicios Extendidos de Gestión de Casos (ECMS). El ECMS es dirigido por BI, ICE y un amplio espectro de organizaciones sin fines de lucro y agencias de servicios sociales. ICE mercadea el ECMS como un programa voluntario que brinda acceso a servicios legales, servicios de salud mental, servicios médicos y de ayuda contra el consumo de sustancias, identificación de traumas, servicios lingüísticos y culturales, y más. Sin embargo, estos programas son coercitivos, porque la participación de las personas que están bajo vigilancia de ICE es controlada por una agencia de cumplimiento de la ley que tiene la potestad de detenerlas y deportarlas.

19 La Evaluación de impacto en la privacidad (PIA) elaborada por la Oficina de Privacidad del DHS sostiene que los datos de ISAP "... también pueden utilizarse para detener, aprehender y expulsar de los Estados Unidos a los participantes" si estos no logran cumplir con el programa. Departamento de Seguridad Nacional de EE. UU.,Evaluación de impacto en la privacidad para el programa de Alternativas a la Detención (ATD) 28 (17 de marzo del 2023), https://www.dhs.gov/sites/default/files/2023-03/privacy-pia-ice062-atd-march2023_1.pdf.

20 Departamento de Seguridad Nacional de EE. UU., BI Capability Statement for a Criminal Activity Monitoring Program [Declaración de capacidades para un programa de monitoreo de actividad delictiva del BI] 123 [de aquí en adelante, Prod. 5, BI Capability Statement], https://www.law.berkeley.edu/wp-content/uploads/2022/05/2023-01-19_ISAP-FOIA_ICEProduction5_ISAP4-Attachment15.pdf [https://perma.cc/8X5V-Y4KS].

Según los documentos de la FOIA, ICE requiere que BI elabore una evaluación cada 60 días para determinar qué participantes del ECMS deberían estar en "ISAP tradicional".[24] Es decir que, aparentemente, BI hace recomendaciones a ICE sobre la posibilidad de que las personas deban someterse a formas más intensivas de vigilancia como SmartLINK. Los documentos no dejan en claro en qué información se basan estas recomendaciones. Además, es posible que haya un conflicto de intereses, pues la empresa aumentaría sus ganancias al tener más personas dentro del programa ISAP "tradicional", que está a cargo de manera más directa del personal de BI y utiliza tecnologías de vigilancia que pertenecen a BI.

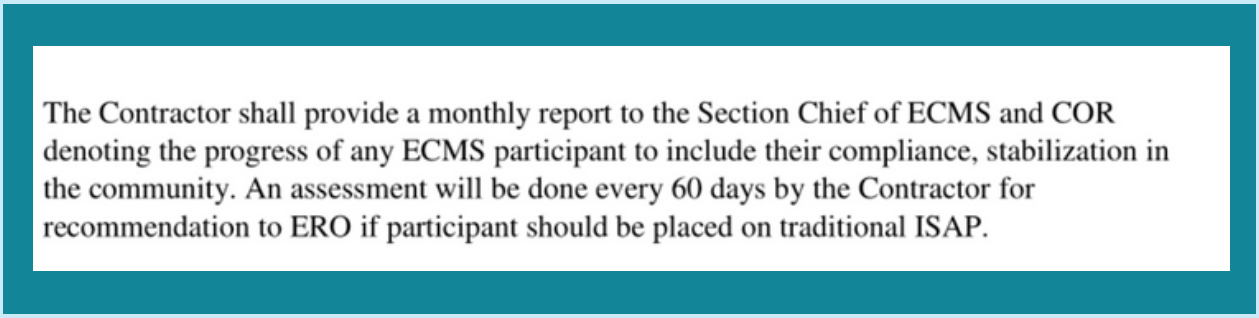

The Contractor shall provide a monthly report to the Section Chief of ECMS and COR denoting the progress of any ECMS participant to include their compliance, stabilization in the community. An assessment will be done every 60 days by the Contractor for recommendation to ERO if participant should be placed on traditional ISAP.

Figura 4: Contrato del ISAP IV de BI, obtenido de los registros de la FOIA por Just Futures Law

Nota: Cuando las personas que están bajo la vigilancia de ISAP y/o sus defensores le solicitan a BI que reduzca la vigilancia a la que son sometidas, o que las liberen completamente de la vigilancia de ISAP, el personal de BI a menudo sostiene que no tiene autoridad para hacer esto, y que los individuos deben acudir a ICE para presentar solicitudes de este tipo. Sin embargo, los documentos de la FOIA muestran que el personal de BI participa activamente de la toma de decisiones junto con ICE cuando se trata de la intensidad y el tipo de vigilancia de ISAP.

Hallazgo #6: Parte de los servicios que le ofrece BI a ICE consiste en gestionar las respuestas negativas a ISAP por parte de la prensa y el público.

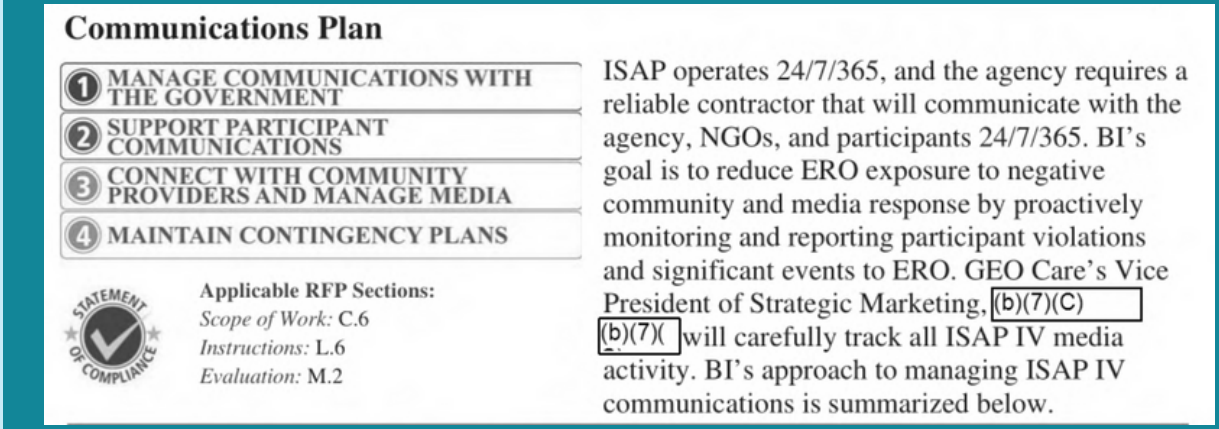
21 Prod. 5, BI Capability Statement, *véase* nota 18, pág. 3-4.

22 Prod. 5, BI Capability Statement, *véase* nota 18, pág. 2.

23 Para saber más acerca del Programa de Gestión de Casos de Jóvenes Adultos (YACMP) de ICE para personas de entre 18 y 19 años (lanzado en enero del 2023), véase *ICE's New Young Adult Case Management Program: Why It Falls Short of Case Management Best Practices and Puts Youth at Risk [El nuevo programa de gestión de casos de jóvenes adultos de ICE: Por qué no cumple con las mejores prácticas de la gestión de casos y pone a los jóvenes en riesgo]*, The Young Center for Immigr. Children's Rights (2023), https://www.theyoungcenter.org/how-ices-new-young-adult-case-management-program-places-youth-at-risk.

24 Departamento de Seguridad Nacional, Attachment 2: Extended Case Management Services (EMCS) [Anexo 2: Servicios Extendidos de Gestión de Casos] 3 [de aquí en más Prod. 4, ISAP IV Contract], https://www.law.berkeley.edu/wp-content/uploads/2022/05/2022-12-15_ISAP-FOIA_ICEProduction4_ISAP4-Attachment2.pdf [https://perma.cc/5VUS-2V36].

Dado el alcance y la escala de la vigilancia digital de ICE descrita anteriormente, no resulta sorprendente que BI considere reducir la exposición de ICE a las "respuestas negativas de la comunidad y los medios" como una prioridad para el futuro de su trabajo con la agencia. En una propuesta de contrato del 2021, BI propuso un plan de comunicaciones en el que la gestión de los medios es una meta central. Allí, se señala que "la meta de BI es reducir la exposición de la Oficina de Detención y Deportación (ERO) a las respuestas negativas de la comunidad y los medios, monitoreando proactivamente e informando a ERO de cualquier violación por parte de los participantes, así como cualquier acontecimiento significativo. El vicepresidente de Marketing Estratégico de GEO Care (...) se ocupará de hacer un minucioso seguimiento de toda la actividad mediática en relación con ISAP IV".[25]



Communications Plan

1. MANAGE COMMUNICATIONS WITH THE GOVERNMENT
2. SUPPORT PARTICIPANT COMMUNICATIONS
3. CONNECT WITH COMMUNITY PROVIDERS AND MANAGE MEDIA
4. MAINTAIN CONTINGENCY PLANS

Applicable RFP Sections:
Scope of Work: C.6
Instructions: L.6
Evaluation: M.2

ISAP operates 24/7/365, and the agency requires a reliable contractor that will communicate with the agency, NGOs, and participants 24/7/365. BI's goal is to reduce ERO exposure to negative community and media response by proactively monitoring and reporting participant violations and significant events to ERO. GEO Care's Vice President of Strategic Marketing, (b)(7)(C) (b)(7)(will carefully track all ISAP IV media activity. BI's approach to managing ISAP IV communications is summarized below.

Figura 5: Propuesta de BI para una solución de monitoreo de actividades delictivas (obtenido de los documentos de la FOIA por Just Futures Law

Además, luego de que BI completó un programa piloto para monitorear datos sobre el encarcelamiento y arresto de miles de participantes de ISAP (tal como se describe más arriba), BI propuso que, al expandir este programa, se alcanzaría el objetivo de "reducir el riesgo que corre la reputación de ISAP al identificar a los participantes que supongan una amenaza para las comunidades".[26] Esto implica que BI e ICE pretenden utilizar los datos de encarcelamiento para justificar la expansión de la criminalización y la vigilancia de comunidades de inmigrantes a través de ISAP.

Hallazgo #7: ICE implementó la aplicación SmartLINK de BI con fallas de exactitud, a la vez que que ISAP sigue posibilitando la vigilancia masiva independientemente de su exactitud.

25 Prod. 5, ISAP IV, véase nota 9, pág. 58.

26 Prod. 5, BI Capability Statement, véase nota 18, pág. 3.

Sean o no precisas las tecnologías de vigilancia de ISAP, lo cierto es que siempre sirvieron el propósito de posibilitar la vigilancia masiva por parte de ICE sobre las comunidades negras e inmigrantes.

Los documentos obtenidos por medio de la FOIA muestran que, en el 2016, BI hizo pruebas de SmartLINK con participantes de ISAP. El piloto monitoreó a más de 600 personas y registró más de 12,000 verificaciones. En el transcurso de este programa, el 56% de las verificaciones de reconocimiento facial fallaron debido a su "tasa de aprobación inaceptablemente baja".[27] Sin embargo, BI siguió implementando SmartLINK y ampliando la vigilancia invasiva sobre las comunidades. En la actualidad, ICE afirma que su tecnología de reconocimiento facial tiene una precisión del 98.5%. La tecnología sigue provocando daños a las comunidades. Los documentos también muestran que, en el año 2017, BI informó que el "índice de aceptación" de la biométrica de voz de SmartLINK era del 75%, y que los factores que contribuyen a esa cifra baja "no se pueden mejorar".[28]ICE no ha declarado cuáles son los índices de precisión actuales. Ahora, ICE está implementando los grilletes de muñeca electrónicos y no ha compartido públicamente ninguna información sobre esta nueva tecnología de vigilancia de ISAP.

Conclusión: A pesar de que ICE presenta públicamente el programa ISAP como una alternativa más "humana" a las celdas físicas, nuestros hallazgos presentan en cambio una imagen profundamente perturbadora de la vigilancia masiva por parte del gobierno sobre las comunidades de inmigrantes, llevada a cabo a través de una serie de tecnologías digitales sumamente invasivas. Estos hallazgos confirman lo que los organizadores y los activistas dicen desde hace años: el programa ISAP es una expansión del impacto carcelario de ICE que tiene como objetivo promover la vigilancia en masa, respaldada por el afán de lucro de una empresa privada como BI.

Just Futures Law, Mijente y Community Justice Exchange trabajan en alianza con personas sometidas a la vigilancia de ISAP para resistir contra las prisiones digitales y exigirle a ICE terminar con la detención de inmigrantes en todas sus formas. A continuación, se incluye una lista de recursos para saber más acerca de las iniciativas para acabar con las detenciones digitales y terminar con todas las formas de encarcelamiento. Hay un consenso cada vez mayor en cuanto a que ISAP no es más que otra forma de encerrar y encadenar a través de la vigilancia de alta tecnología. Si le gustaría involucrarse, no dude en comunicarse con nuestras organizaciones con nuestras organizaciones.

27 U.S. Dep't of Homeland Sec., Refactored Biometric Enrollment for SmartLINK: ISAP Pilot II Findings 2 [hereinafter Prod. 6, ISAP II Pilot Findings], https://www.law.berkeley.edu/wp-content/uploads/2022/05/2023-01-25_ISAP-FOIA_ICEProduction6_RefactoredBiometricEnrollmentForSmartLink.pdf [https://perma.cc/9KN6-59HV].

28 Prod. 6, ISAP II Pilot Findings, *supra* note 25, at 5.

Lista de Recursos

- Elizabeth Trovall, *The growing business of immigrant surveillance* [El próspero negocio de la vigilancia sobre los inmigrantes], Marketplace (Aug. 2, 2023), https://www.marketplace.org/2023/08/02/the-growing-business-of-immigrant-surveillance/.

- African Bureau for Immigration and Social Affairs (ABISA), Shackled Migrants, Tanked Freedom: Black Migrants ATD Report [Migrantes encadenados, fracaso de la libertad: informe de ATD para los migrantes negros] (2023), https://www.abisa.org/reports.

- African Bureau for Immigration and Social Affairs (ABISA), Boston Immigration Justice and Accountability Network (BIJAN), Community Justice Exchange, Detention Watch Network, Envision Freedom Fund, Freedom for Immigrants, Georgia Latino Alliance for Human Rights (GLAHR), Just Futures Law, La Resistencia, Long Beach Immigrant Rights Coalition (LBIRC), Mijente, Organized Communities Against Deportations (OCAD) & Youth Justice Coalition, Rastreo y Captura: Experiencias de las prisiones digitales de ICE (mayo del 2022), https://notechforice.com/wp-content/uploads/2022/05/TrackedTrapped_Spanish.pdf.

- Amy Taxin y Amancai Biraben, *Deportation agents use smartphone app to monitor immigrants* [Los agentes de deportación usan una aplicación para vigilar a los inmigrantes], Associated Press (10 de marzo del 2022), https://apnews.com/article/immigration-covid-technology-business-health-2823ba115ab2c120d728881c0a7bb5e8.

- Johana Bhuiyan, *Poor Tech, Opaque Rules, Exhausted Staff: Inside the Private Company Surveilling US Immigrants* [Tecnología pobre, reglas opacas, personal exhausto: dentro de la empresa privada que vigila a los inmigrantes en Estados Unidos], The Guardian (7 de marzo del 2022), https://www.theguardian.com/us-news/2022/mar/07/Us-immigration-surveillance-ice-bi-isap.

- Carta de 25 miembros del Congreso al secretario del DHS Mayorkas (febrero del 2022), https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/635feae867ae794b6154031a/1667230441492/ICE+ISAP+Congressional+Letter_final.pdf (se debaten asuntos vinculados con el ISAP).

- Just Futures Law y Mijente, ICE Digital Prisons: The Expansion of Mass Surveillance As ICE's Alternative to Detention [Las prisiones digitales de ICE: La expansión de la vigilancia masiva como la alternativa de ICE a la detención] (mayo de 2021) https://www.flipsnack.com/justfutures/ice-digital-prisons-1u8w3fnd1j/full-view.html.

- Todd Feathers, '*They Track Every Move': How US Parole Apps Created Digital Prisoners* ["Siguen cada uno de mis movimientos": en Estados Unidos las aplicaciones de libertad condicional crean prisioneros digitales], The Guardian, 4 de marzo de 2021, https://www.theguardian.com/global-development/2021/mar/04/they-track-every-move-how-us-parole-apps- created-digital-prisoners.

Apéndice

La siguiente es una lista de documentos destacados de la ley FOIA.

- Departamento de Seguridad Nacional de EE. UU., , Privacy Threshold Analysis [Análisis de umbrales de privacidad], disponible aquí.
- Departamento de Seguridad Nacional de EE. UU., SmartLINK Participant Agreement [Acuerdo de participantes de SmartLINK], disponible aquí.
- Departamento de Seguridad Nacional de EE. UU.,ISAP Participant Handbook [Manual del participante del ISAP], disponible aquí.
- Departamento de Seguridad Nacional de EE. UU., Statement of Work [Declaración de trabajo], disponible aquí.
- Departamento de Seguridad Nacional de EE. UU., Extended Case Management Services (ECMS) [Servicios Extendidos de Gestión de Casos (ECMS)], disponible aquí.
- Departamento de Seguridad Nacional de EE. UU., ATD Participant Enrollment Form [Formulario de inscripción a las ATD], disponible aquí.
- Departamento de Seguridad Nacional de EE. UU., Notice to Terminate ATD Participation Form [Formulario de notificación de fin de participación en las ATD], disponible aquí.
- Departamento de Seguridad Nacional de EE. UU., Detailed GPS Ankle Bracelets And Tracking/Monitoring System, Telephonic Reporting System, Biometric Reporting System [Sistema detallado de grilletes de tobillo con GPS y rastreo/monitoreo, sistema de informes telefónicos, sistema de informes biométricos], disponible aquí.
- Departamento de Seguridad Nacional de EE. UU., Special Contract Requirements [Requisitos contractuales especiales], disponible aquí.
- Departamento de Seguridad Nacional de EE. UU., BI Capability Statement for a Criminal Activity Monitoring Program [Declaración de capacidades para un programa de monitoreo de actividad delictiva del B], disponible aquí.
- Departamento de Seguridad Nacional de EE. UU., Refactored Biometric Enrollment For SmartLINK: ISAP Pilot II Findings [Inscripción biométrica refactorizada para SmartLINKS: Hallazgos del piloto ISAP II], disponible aquí.