Fact Sheet on ICE FOIA Lawsuit: ICE Documents Reveal Alarming Scale of Surveillance in ISAP program

Background:

Since 2004, Immigration and Customs Enforcement (ICE) has paid billions to BI Inc., a subsidiary of private prison company Geo Group, to run its Intensive Supervision Appearance Program (ISAP),[1] an electronic monitoring program marketed as an "alternative to detention." Today, ICE subjects over 200,000 immigrants to various forms of surveillance via ISAP. This includes GPS ankle shackles and SmartLINK, a cell phone app ICE first launched during the Trump administration that tracks people via facial recognition, voice recognition, and location surveillance.

Immigrant communities have long documented the lasting trauma caused by these electronic forms of incarceration, also known as digital prisons. Twenty-five members of Congress have expressed concern about the "drastic increase" in the ISAP program and the "extreme physical and mental damage" caused by this punitive surveillance. Yet, the Biden administration has massively increased funding for ISAP and ICE has now added wrist-worn GPS tracking devices to the list of ISAP surveillance technologies. In addition, ICE recently solicited new proposals from companies to manage the agency's electronic surveillance monitoring, indicating ICE's plans to expand this e-carceration program.

In 2022, Just Futures Law, Mijente Support Committee, and Community Justice Exchange sued ICE to force the agency to disclose information about what data ICE is collecting via ISAP and how it is using that data. The organizations are represented by the Samuelson Law, Technology & Public Policy Clinic of UC Berkeley School of Law.

1 According to the Transactional Records Access Clearinghouse (TRAC), BI and ICE have repeatedly published incorrect data regarding the number of individuals and families subjected to ISAP surveillance. See False Reporting by Contractor on Alternatives to Detention Activities, TRAC (Mar. 7, 2023), https://trac.syr.edu/reports/710/ [https://perma.cc/WDK8-ZUJV].

Key Takeaways:

This factsheet lists major findings regarding ISAP surveillance from ICE records obtained through our FOIA lawsuit. Below are some key takeaways from our review:

- **ICE's ever-expanding ISAP program is a project of mass surveillance.** Through ISAP, the agency tracks hundreds of thousands of immigrants and families, including via multiple e-carceration technologies. ICE uses ISAP to extract enormous quantities of highly sensitive personal information from immigrant communities and stockpiles much of this sensitive data for 75 years.

- **ICE's public assurances about protecting the data and privacy of people under ISAP cannot be trusted.** As FOIA records reveal, ICE's actual surveillance practices under ISAP often contradict DHS and ICE's statements minimizing ISAP's surveillance capabilities. These discrepancies point to ICE's reckless system of data extraction and electronic surveillance and suggest the agency is unable to comply with even its own privacy policies. For example, there are multiple inconsistencies about the extent to which ICE subjects people to continuous location surveillance via the SmartLINK app.

- **Overall, the findings demonstrate that ICE's ultimate goal with ISAP is not a more humane program, but to expand the agency's punitive control over the lives and autonomy of Black, brown and immigrant communities.**

Finding #1: ICE and its private contractor BI extract and retain a broad range of data on immigrants subject to its electronic monitoring programs.

Data Extraction: On behalf of ICE, BI collects an enormous amount of personal data about people subjected to ISAP. Much of this data is extracted via technologies such as the SmartLINK mobile app and GPS ankle shackles. This data includes:[2]

- Personally identifying information (address, email address, phone number, birth date, social security number,[3] visa & passport number, employment information, education information, financial information, religious affiliation, race, gender, etc.)
- Biometric and body/health data (facial images, voice prints, weight, height, tattoos, scars, medical information, disabilities, pregnancy and births,[4] etc.)
- Geolocation data
- Phone numbers of close contacts[5]
- Immigration court records
- Vehicle and driver data (e.g. license plate number, driver's license number, vehicle registration number)
- Community surveillance data (e.g. data about someone's home, neighborhood or community ties)

Data Ownership: While BI collects and stores ISAP data, ICE owns the rights to the data – including information systems and databases created by BI. According to the FOIA records, ICE's contract with BI states that the agency "shall have unlimited rights to use, dispose of, or disclose" all ISAP data, including metadata.[6] This suggests that ICE has the ability to use ISAP data any way it wants, for example, by combining it with other databases or data points to gain even more detailed surveillance information about the lives of people subjected to ISAP.

Data Retention: ISAP data is retained for 75 years. This is a near-permanent ICE surveillance collection for those subject to electronic monitoring. However, the FOIA records and a public-facing Dept. of Homeland Security Privacy Impact Assessment (PIA) about ISAP together present confusing, muddled, and sometimes contradictory information about ISAP data retention.

2 The DHS Privacy Office and BI have each publicly stated that ISAP collects many of these data points. FOIA records state that ISAP collects additional information, such as visa numbers. See U.S. Dep't of Homeland Sec., Privacy Threshold Analysis 8 [hereinafter 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]. In addition, the records show that ISAP collects data on court records, tattoos and scars, disabilities, and "community ties." During home visits, BI is instructed to collect data such as "layout of the residence," "information about people residing at the residence," "pets, children, fences, entry systems, property details," and "criminal activity associated with the participant, property or neighborhood." See U.S. Dep't of Homeland Sec., Statement of Work 17-18 [hereinafter 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].

3 In its Privacy Policy, BI states that SmartLINK collects social security numbers for business purposes. This contradicts FOIA records which state that ISAP does not collect social security numbers. See, Prod. 1, PTA, *supra* note 2, at 9.

For example, the DHS PIA states that ISAP records are maintained in ICE's Enforcement Integrated Database (EID),[7] a massive database used by all DHS agencies that requires records be destroyed 75 years from the date of entry. It also states that BI stores ISAP data, including SmartLINK data, in BI's "Total Access" database system for 7 years after someone is terminated from the program. But this contradicts the FOIA records. In some instances, the FOIA records note that BI "shall not destroy or alter any logs or records" pertaining to the contract, suggesting that records may be kept by BI indefinitely.[8] In other instances, the FOIA records state that the records in BI's Total Access system are "an extension" of ICE's EID system,[9] suggesting that at least some data collected by BI in Total Access is retained by ICE for 75 years.

DHS states that data collected in the Young Adult Case Management Program, a new ISAP program that monitors 18 and 19-year olds, will be retained permanently.

Note: FOIA records show that in 2021, BI told ICE that it could store "historical data" on ISAP participants on "backup tapes," a retention practice that would go beyond the established 7 year data retention period.[10]

Finding #2: FOIA records contradict ICE statements that it limits location and phone data surveillance, particularly when it comes to SmartLINK surveillance.

Phone Data Surveillance: FOIA records show that BI has stated that SmartLINK reports the status of someone's "cellular data coverage, Wi-Fi connectivity, and location services" and that the app will notify ICE or BI "when these services are disabled."[11] This implies that if people attempt to limit or change location tracking settings on their phone, ICE or BI could potentially find out. However, this contradicts ICE statements around phone surveillance. On its website, ICE states that SmartLINK is not capable of accessing information on personal devices including photos, browsing activity, or text messages outside the app.

4 FOIA records show that people in ISAP are required to "immediately" notify BI or ICE if they become pregnant, give birth, become a parent of a new child, are hospitalized, become seriously ill, are seriously injured, receive a ticket, or are arrested. See U.S. Dep't of Homeland Sec., Intensive Supervision Appearance Program Participant Handbook 3 [hereinafter 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 must notify ICE about childbirths, pregnancies, expected due dates and personal data on the "child's father" such as name, address, country of citizenship, and phone number. See Prod. 3, Statement of Work, *supra* note 2, at 28-29.

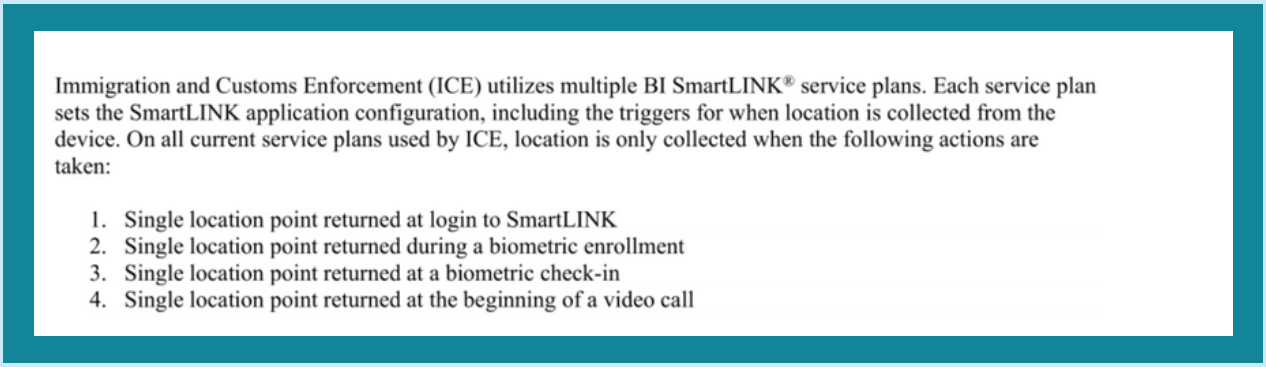
5 People under ISAP surveillance are required to provide contact information for close contacts such as family members or friends. FOIA records show that ICE requires BI to provide various reports submitted daily, weekly, monthly, quarterly or yearly. For example, "Intelligence Reports" are generated "as needed" and can include information such as "how many times a phone number was listed/used by a participant or personal contact." See Prod. 3, Statement of Work, supra note 2, at 33.

6 FOIA records state that ICE has not deemed the ISAP contract an "information technology (IT) contract." Therefore, BI appears to be exempted from certain privacy provisions regarding the use of personal data. For example, BI is not prohibited from using ISAP data containing personally identifiable information for training or testing purposes. See U.S. Dep't of Homeland Sec., Special Contract Requirements 131 [hereinafter 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].

Note: BI's SmartLINK Privacy Policy states that BI collects or receives the following data points from SmartLINK users: "commercial information about prior and prospective transactions," Internet and network activity, and device information such as "device identifiers, IP address, internet connections, operating system, browser type, mobile network information, battery information, and the device's telephone number."[12] Notably, IP address information and other device data can be used to glean general location information.

Location Surveillance:[13]

SmartLINK: FOIA records state that SmartLINK tracks location data during a log-in, biometric enrollment, a check-in, and at the start of a video call.[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

Figure 1: ISAP BI SmartLINK Agreement, from FOIA records obtained by Just Futures Law

Note: The FOIA records conflict with what DHS and ICE have stated publicly about SmartLINK location surveillance. For example, the DHS Privacy Impact Assessment (PIA) states that location data is only collected during enrollment and check-ins – not during login or at the start of a video call. DHS and ICE not only contradict the FOIA records, they also contradict themselves. DHS states elsewhere in the PIA that location data can be accessed "when the app is open," suggesting that this data could be collected when the app is on in the background. Concerningly, ICE publicly states that SmartLINK is capable of continuously monitoring location data if the app is on a BI device (not a personal cell phone). According to ICE, this feature is "currently inactive."

7 ICE's Enforcement Integrated Database is a database used across all components of DHS, including ICE, USCIS, and CBP, that stores data related to the "investigation, arrest, booking, detention, and removal of persons" and retains such records for 75 years. See: DHS/ICE/PIA-015 Enforcement Integrated Database, Dept. of Homeland Security (May 2019), https://www.dhs.gov/publication/dhsicepia-015h-enforcement-integrated-database-eid-criminal-history-information-sharing.

8 Prod. 3, Statement of Work, *supra* note 2, at 38.

9 Prod. 1, PTA, *supra* note 2, at 11.

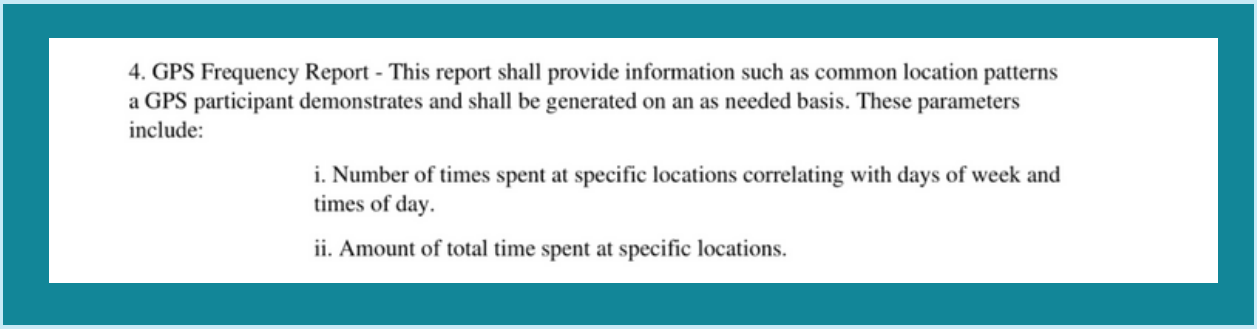
10 U.S. Dep't of Homeland Sec., BI Inc. Technical Proposal 54 [hereinafter Prod. 5, ISAP IV], https://www.law.berkeley.edu/wp-content/uploads/2022/05/2023-01-19_ISAP-FOIA_ICEProduction5_ISAP4-Attachment15.pdf [https://perma.cc/JNK4-YZ7L].

11 U.S. Dep't of Homeland Sec., BI Inc. SmartLINK Agreement 1 [hereinafter 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].

These inconsistencies exhibit ICE's reckless, limitless approach to invasive surveillance and raise major flags about what is really going on. There is nothing preventing ICE from changing (or ignoring) its stated practice to instead continuously track location data via the SmartLINK app – in fact, some reports indicate that this is already happening. A recent article discussed an ICE agent in Houston who was tracking "the movements of one person with the B.I. SmartLink app over the course of 24 hours."[15] This suggests that ICE agents are continuously tracking location, despite ICE's claims to the contrary.

GPS Ankle Shackles: ICE and BI continuously track the precise location of people required to wear physically and psychologically harmful GPS ankle shackles 24/7. Their precise location is automatically indexed in BI's system every 4 hours.[16] ICE or BI can access "automatic location updates in real time" as well as "turn-by-turn directions" to the person's location using an app.[17] With access to logs of historical location data collected by the ankle shackles over time, ICE and BI can gain a window into someone's life over months or years; for example, every trip to a child's school, to a healthcare clinic, to a house of worship, to a family member's home, etc.

Note: BI produces GPS data reports for ICE on an "as needed basis."[18] These reports can include a person's "common location patterns" such as the "number of times spent at specific locations correlating with days of week and times of day." In other words, ICE can request a detailed map of someone's daily life and activities at any time.


4. GPS Frequency Report - This report shall provide information such as common location patterns a GPS participant demonstrates and shall be generated on an as needed basis. These parameters include:

i. Number of times spent at specific locations correlating with days of week and times of day.

ii. Amount of total time spent at specific locations.

Figure 2: ISAP IV BI Contract, from FOIA records obtained by Just Futures Law

12 In addition, BI's SmartLINK Privacy Policy allows BI to disclose personal information to third parties such as its contractors, service providers, subsidiaries and affiliates. See *BI SmartLINK Privacy Policy*, BI Inc.(March 18, 2022), *https://bi.com/bi-smartlink-privacy/*. This contradicts the ICE website, which states that SmartLINK data is not shared with third parties. See *Alternatives to Detention Frequently Asked Questions*, U.S. Immigr. Customs Enf't., https://www.ice.gov/atd-faq.

13 ICE requires people under ISAP surveillance to have a Participant ID card that includes their name, photo, birth date and a barcode. It is not clear whether these cards track location. The FOIA records show that ICE has instructed BI to scan the ID card during office and home visits, noting that for home visits: "Scan of ID card should verify that the Home Visit was conducted at the residence with a device that records the GPS coordinates and nearest address of the scan." See Prod. 3, Statement of Work, supra note 2, at 17.

14 See Prod. 2, SmartLINK Agreement, supra note 10, at 4.

15 Elizabeth Trovall, The growing business of immigrant surveillance, Marketplace (Aug. 2, 2023), https://www.marketplace.org/2023/08/02/the-growing-business-of-immigrant-surveillance/.

16 See Prod. 1, PTA, supra note 2, at 5.

17 U.S. Dep't of Homeland Sec., Attachment 1: Detailed GPS Ankle Bracelets And Tracking/Monitoring System, Telephonic Reporting System, Biometric Reporting System 2-3 [hereinafter 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, supra note 2, at 33.

Finding #3: The FOIA records show ICE uses ISAP data to locate and arrest community members en masse.[19]

FOIA records confirm that ICE uses ISAP to target people for deportation. For example, in 2018, BI ISAP employees in Manassas, Virginia apparently collaborated with ICE to carry out a mass arrest of 40 people, including by providing geolocation data that enabled ICE to pinpoint the location of those targeted for arrest. BI called it the "largest coordinated arrest in the history of ISAP within the Washington, DC, Field Office."[20]

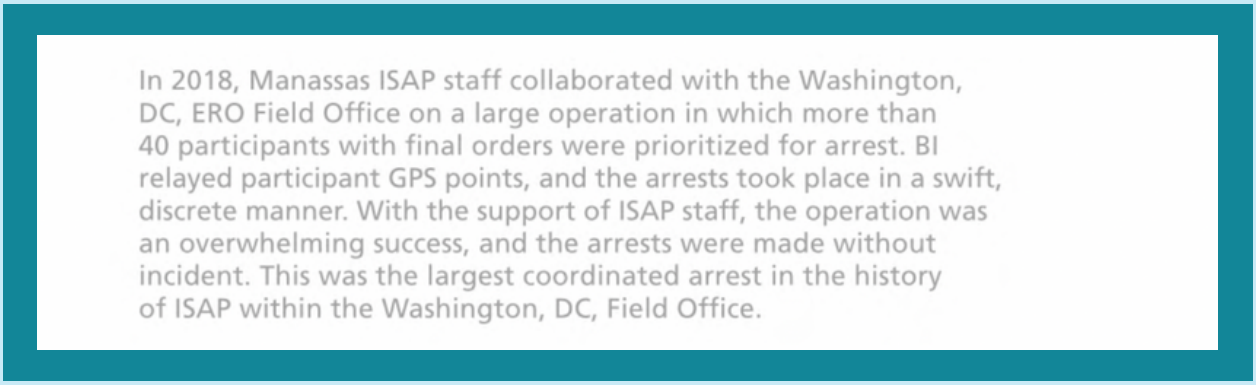

In 2018, Manassas ISAP staff collaborated with the Washington, DC, ERO Field Office on a large operation in which more than 40 participants with final orders were prioritized for arrest. BI relayed participant GPS points, and the arrests took place in a swift, discrete manner. With the support of ISAP staff, the operation was an overwhelming success, and the arrests were made without incident. This was the largest coordinated arrest in the history of ISAP within the Washington, DC, Field Office.

Figure 3: From FOIA records obtained by Just Futures Law

Finding #4: BI provided ICE access to other surveillance data for its deportation efforts – particularly targeting sanctuary jurisdictions that limit ICE access to data.

19 The DHS Privacy Office Privacy Impact Assessment (PIA) for ISAP states that ISAP data ". . . can also be used to detain, apprehend, and remove the participants from the United States . . ." if they fail to comply with the program. U.S. Dep't of Homeland Sec., Privacy Impact Assessment for the Alternatives to Detention (ATD) Program 28 (Mar. 17, 2023), https://www.dhs.gov/sites/default/files/2023-03/privacy-pia-ice062-atd-march2023_1.pdf.

20 U.S. Dep't of Homeland Sec., BI Capability Statement for a Criminal Activity Monitoring Program 123 [hereinafter 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].

FOIA records show that in 2021, BI conducted a 60-day pilot program to monitor incarceration and arrest data pertaining to nearly 10,000 people under ISAP surveillance. During the pilot, BI provided ICE access to jail booking information including "daily notification of arrests and incarceration, including bookings, transfers, and releases."[21] BI partnered with a third party company called ClearForce that provided this incarceration information sourced from jails nationwide. BI noted that the program was "crucial for sanctuary jurisdiction data, which ICE generally no longer receives," and reported that the majority (57%) of those arrested during the pilot "resided in the seven 'Sanctuary States.'" The States listed are California, New York, New Jersey, Washington, Oregon, Colorado, and Illinois.

BI proposed to ICE that the agency could use the incarceration data program in the future to track the "criminal activity" of "persons of interest, either part of the ATD program or outside of it."[22] It is deeply troubling that ICE uses companies like BI, as well as data broker companies like LexisNexis, to create loopholes around local laws that limit collaboration with ICE and protect immigrant communities.

Finding #5: BI is heavily involved in decisions to terminate people from the ICE Extended Case Management Services (ECMS) program and escalate them into even more invasive forms of ISAP surveillance.

A range of carceral corporations, nonprofits, and social service agencies nationwide help ICE monitor adults and young people[23] through its various ISAP "case management" programs.

One of these programs is the Extended Case Management Services (ECMS) program. ECMS is run by BI, ICE and a wide array of nonprofits and social service agencies. ICE advertises ECMS as a voluntary program providing access to legal services, mental health services, substance abuse and medical services, trauma identification, cultural and language services, and more. However, these programs are coercive, given that the participation of people under ICE surveillance is monitored by a law enforcement agency that has the power to detain and deport them.

21 Prod. 5, BI Capability Statement, supra note 18, at 3-4.

22 Prod. 5, BI Capability Statement, supra note 18, at 2.

23 For more information on ICE's Young Adult Case Management Program (YACMP) for 18 and 19-year olds, launched in January 2023, see *ICE's New Young Adult Case Management Program: Why It Falls Short of Case Management Best Practices and Puts Youth at Risk*, 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.

FOIA records indicate that ICE requires BI to produce an assessment every 60 days that evaluates which ECMS participants should be placed on "traditional ISAP."[24] That is, BI appears to be making recommendations to ICE about whether people should be subjected to more intensive forms of ICE surveillance, such as SmartLINK. It is not clear from the records on what information these recommendations are based. Moreover, there may be a conflict of interest as the company would presumably stand to profit more from having individuals placed in the "traditional" ISAP program which is more directly managed by BI staff and utilizes BI proprietary surveillance technologies.

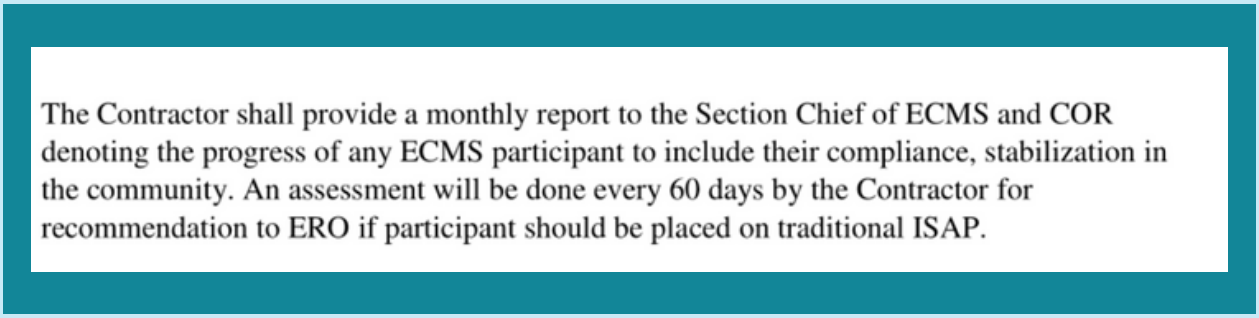

The Contractor shall provide a monthly report to the Section Chief of ECMS and COR denoting the progress of any ECMS participant to include their compliance, stabilization in the community. An assessment will be done every 60 days by the Contractor for recommendation to ERO if participant should be placed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

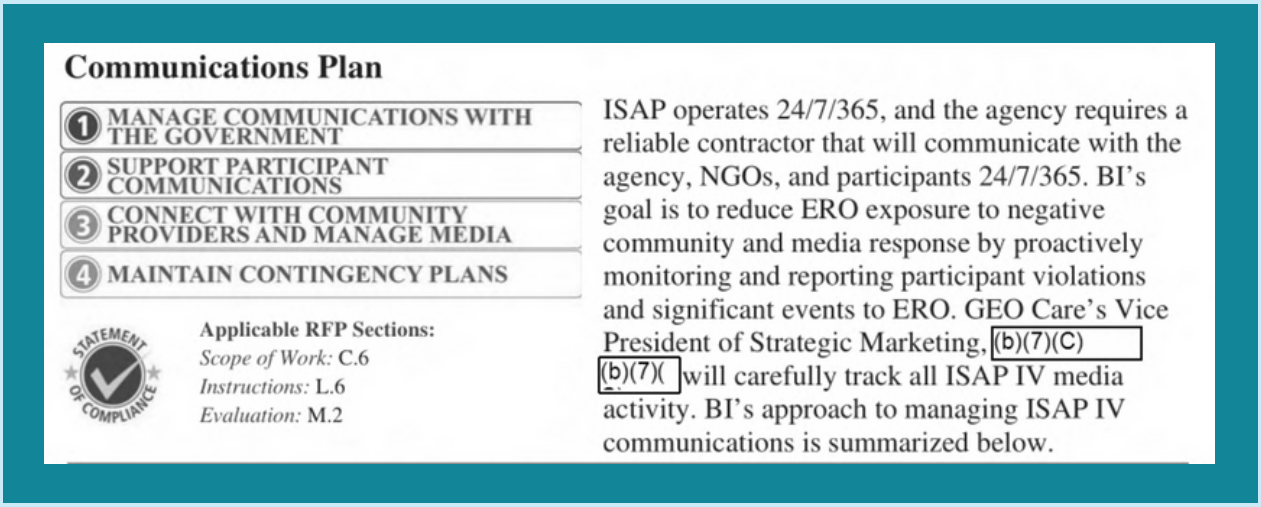
Figure 4: ISAP IV BI Contract, from FOIA records obtained by Just Futures Law

Note: When people under ISAP surveillance and/or their advocates ask BI to decrease the amount of surveillance they are subjected to or release them from ISAP surveillance entirely, BI staff often maintain that they have no authority to do so and that individuals must go to ICE with such requests. Nevertheless, the FOIA records show that BI staff are heavily involved in ICE decisions when it comes to the amount of and type of ISAP surveillance.

Finding #6: Part of BI's proposed work for ICE is managing negative press and public response to ISAP.

24 U.S. Dep't of Homeland Sec., Attachment 2: Extended Case Management Services (EMCS) 3 [hereinafter 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].

Given the scope and scale of ICE digital surveillance described above, it may come as no surprise that BI considers reducing ICE's exposure to "negative community and media response" a priority for its future work with the agency. In a 2021 contract proposal for ICE, BI proposed a Communications Plan where managing media is a central goal. It noted that "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... will carefully track all ISAP IV media activity."[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.

Figure 5: BI Proposal for a Criminal Activity Monitoring Solution, from FOIA records obtained by Just Futures Law

In addition, after BI completed a pilot program to monitor incarceration and arrest data on thousands of ISAP participants (described above), BI proposed that expanding this program would achieve the objective of "reducing the reputational risk for ISAP by identifying participants that pose a threat to the communities."[26] This implies that BI and ICE seek to leverage incarceration data to justify the expanding criminalization and surveillance of immigrant communities via ISAP.

Finding #7: ICE rolled out BI SmartLINK with failing accuracy rates – and ISAP continues to enable mass surveillance regardless of accuracy.

25 Prod. 5, ISAP IV, *supra* note 9, at 58.
26 Prod. 5, BI Capability Statement, *supra* note 18, at 3.

Whether the ISAP surveillance technologies are highly accurate or not, they always serve the purpose of enabling ICE's mass surveillance of Black, brown and immigrant communities.

FOIA records show that in 2016, BI tested SmartLINK on ISAP participants. The pilot monitored over 600 people and logged over 12,000 check-ins. During this program, 56% of facial recognition check-ins failed due to the technology's "unacceptably low pass rate."[27] BI continued to roll out SmartLINK and expand its invasive surveillance of communities. Today, ICE states that its facial matching technology has a 98.5% accuracy rating; the technology continues to harm communities. The records also show that in 2017, BI reported that the "pass rate" for SmartLINK voice biometrics was 75% and that the factors that contribute to the low pass rate "are not subject to improvement."[28] ICE has not stated what today's accuracy rates are for this technology. ICE is now rolling out electronic wrist shackles and has shared no information with the public about this new ISAP surveillance technology.

Conclusion: Despite ICE's public portrayal of the program as a more "humane" alternative to a brick and mortar cage, our findings instead convey a deeply troubling picture of mass government surveillance of immigrant communities carried out through an array of highly invasive digital technologies. These findings affirm what organizers and advocates have been saying for years: the ISAP program is an expansion of ICE's carceral footprint with the objective of bolstering mass surveillance, backed by the profit motives of private company BI.

Just Futures Law, Mijente, and Community Justice Exchange are working in partnership with people subjected to ISAP surveillance to resist digital prisons and demand ICE end the detention of immigrants in all forms. Below is a list of resources to learn more about efforts to stop digital detention and end all forms of incarceration. There is growing consensus that ISAP is just another form of caging and shackling through high-tech surveillance. Please reach out to our organizations if you are interested in getting involved.

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

28 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].

Resource List

- Elizabeth Trovall, *The growing business of immigrant surveillance*, 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 (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, Tracked and Trapped: Experiences From ICE Digital Prisons (May 2022), https://notechforice.com/digitalprisons/.

- Amy Taxin & Amancai Biraben, *Deportation agents use smartphone app to monitor immigrants*, Associated Press (Mar. 10, 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*, Guardian (Mar. 7, 2022), https://www.theguardian.com/us-news/2022/mar/07/Us-immigration-surveillance-ice-bi-isap.

- Letter from 25 Members of Congress to DHS Secretary Mayorkas (February 2022), https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/635feae867ae794b6154031a/1667230441492/ICE+ISAP+Congressional+Letter_final.pdf (discussing concerns with ISAP).

- Just Futures Law & Mijente, ICE Digital Prisons: The Expansion of Mass Surveillance As ICE's Alternative to Detention (May 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*, Guardian (Mar. 4, 2021), https://www.theguardian.com/global-development/2021/mar/04/they-track-every-move-how-us-parole-apps-created-digital-prisoners.

Appendix

The following is a highlight list of records from our FOIA.

- U.S. Dep't of Homeland Sec., Privacy Threshold Analysis, available here.
- U.S. Dep't of Homeland Sec, SmartLINK Participant Agreement, available here.
- U.S. Dep't of Homeland Sec, ISAP Participant Handbook, available here.
- U.S. Dep't of Homeland Sec, Statement of Work, available here.
- U.S. Dep't of Homeland Sec, Extended Case Management Services (ECMS), available here.
- U.S. Dep't of Homeland Sec, ATD Participant Enrollment Form, available here.
- U.S. Dep't of Homeland Sec, Notice to Terminate ATD Participation Form, available here.
- U.S. Dep't of Homeland Sec, Detailed GPS Ankle Bracelets And Tracking/Monitoring System, Telephonic Reporting System, Biometric Reporting System, available here.
- U.S. Dep't of Homeland Sec, Special Contract Requirements, available here.
- U.S. Dep't of Homeland Sec, BI Capability Statement for a Criminal Activity Monitoring Program, available here.
- U.S. Dep't of Homeland Sec, Refactored Biometric Enrollment For SmartLINK: ISAP Pilot II Findings, available here.