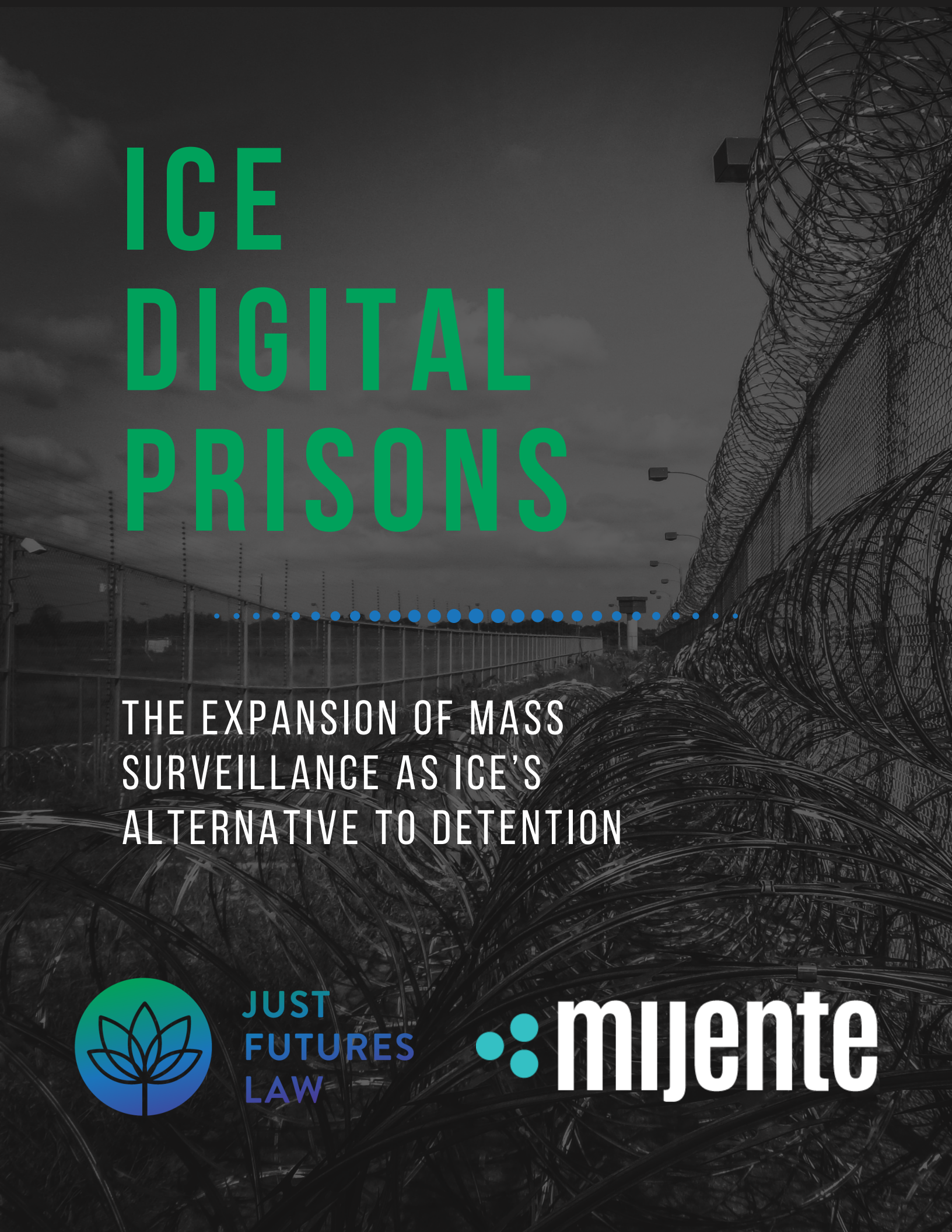


ICE DIGITAL PRISONS

THE EXPANSION OF MASS SURVEILLANCE AS ICE'S ALTERNATIVE TO DETENTION

JUST FUTURES LAW

mijente

MAY 2021

Writer & Report Design: Aly Panjwani,
Take Back Tech Fellow 2020-21

Editor: Julie Mao,
Just Futures Law

Thank you to James Kilgore, Basma Eid, Empower LLC, MediaJustice, Community Justice Exchange, Immigrant Defense Project, Organized Communities Against Deportation, Casa San Jose, Centro de Trabajadores Unidos for participating in the research and review for this report.

JUST FUTURES LAW

mijente

I. INTRODUCTION

As we call on the Biden administration to put an end to immigration detention, it is crucial to scrutinize the so-called "alternatives to detention" that the administration may expand and the harms these programs bring with them. **Calling for the end to immigration detention also means the end to any and all programs that treat immigrants as security threats and subjects of surveillance**. Alternatives to detention programs, throughout the course of Immigration and Customs Enforcement's (ICE) history, have only reified the Department of Homeland Security's (DHS) carceral approach to immigration and increased the number of individuals under ICE's supervision. They are operated by private, for-profit companies with the purpose of extending incarceration beyond the walls of detention centers and do not provide resources like access to education, housing, and legal services for immigrant communities to thrive. The technologies that these programs employ only further entrench the criminalization of immigration and pose barriers to social and economic wellbeing.

This report will provide an overview of ICE's Alternatives to Detention (ATD) program—namely its Intensive Supervision Appearance Program (ISAP)—and the next generation of intrusive surveillance technologies deployed as alternatives to detention, including voice recognition, facial recognition, risk assessment algorithms, and biometric wearables.

II. BACKGROUND

In 2004, ICE commenced its first iteration of the Alternatives to Detention (ATD) program under the agency's Intensive Supervision Appearance Program (ISAP) contract.[1] The program has gone through several iterations since its inception and is now in its fourth iteration, known as ISAP IV. In March 2020, ICE signed a five-year contract for ISAP IV, which started in April 2020.[2] Since 2004, ICE has consistently contracted with B.I. Incorporated for the program.[3] B.I. Incorporated is an electronic monitoring systems provider and a subsidiary of GEO Group. GEO Group is one of ICE's contractors for private immigration detention facilities and is also deeply invested in profiting from other forms of mass incarceration across the country.[4] This partnership alone is an indication that ICE's ATD-ISAP program is a continuation of a system that profits from surveillance and detention.

As of May 2021, 96,574 individuals were subject to the ICE's Alternatives to Detention program.[5] Moreover, the program does not actually reduce the number of individuals who are detained in ICE's custody—as ICE's budget for ATD-ISAP programs increased, so did its budget for detention. From 2006 to 2021, ICE's budget for the program increased from **$28 million to $440 million**, while its budget for detention increased from **$1 billion to $2.8 billion**. And the Biden administration's 2022 budget request calls for increasing the number of individuals in ATD-ISAP to 140,000, approximately 45,000 more than its current enrollment.[6] More individuals are subject to ICE's supervision than would be without the program. For example, asylum seekers who would have previously been released from detention and not responsible for reporting to the agency are often incorporated into the program, expanding its reach.[7] Most importantly, these e-carceration tools exact physical and emotional harm on the immigrants subjected to these surveillance technologies, such as wounds from the ankle shackle or the psychological weight of ICE tracking a person's movement and personal interactions.[8]

The ICE ATD-ISAP program consists of various components and surveillance plans: home visits, office visits, court tracking, and several forms of electronic monitoring, including GPS monitoring, voiceprint verification, and facial recognition through an application known as SmartLINK. Individual ICE agents decide the form of electronic monitoring to which an individual will be subjected. Given the wide discretion, an ICE agent's decision to put someone under a specific type of supervision or surveillance can be arbitrary.

In Section III, we take a deeper dive into the specific surveillance technologies which ICE and contractor B.I. Incorporated employ at various stages of the ATD-ISAP program. For background reference, we provide the following breakdown on the main components of the ISAP program:[9]

Enrollment & Orientation: After an individual is referred to the program by Enforcement and Removal Operations (ERO), they go through an orientation process. Individuals fill out paperwork around their immigration, criminal, and family histories. They are given a "service plan" that determines what type of surveillance they will be subject to, the frequency of home and office visits, and a schedule for compliance checks. Enforcement officers also issue photo ID cards which are used during home and office visits for identity verification. Individuals are enrolled into the technology itself. Depending on the service plan, this step can include setting up the ankle monitor and defining geographic boundaries, capturing a photo for the facial recognition feature of the SmartLINK app and downloading the application to the individual's personal device, and/or collecting the voiceprint for voice verification which is stored on a system known as VoiceID.

Home Visits: Home and office visits are a central part of the ATD-ISAP program.[10] While office visits are scheduled in advance, home visits take place unannounced and unscheduled. The ICE officer arrives at the individual's residence without notice and scans the individual's ID card with a device that also records GPS coordinates. Officers are instructed to conduct surveillance in the home during the visit such as "look for evidence of possible flight risk and verify utilities are working," and to document "criminal activity associated with the participant, property or neighborhood."

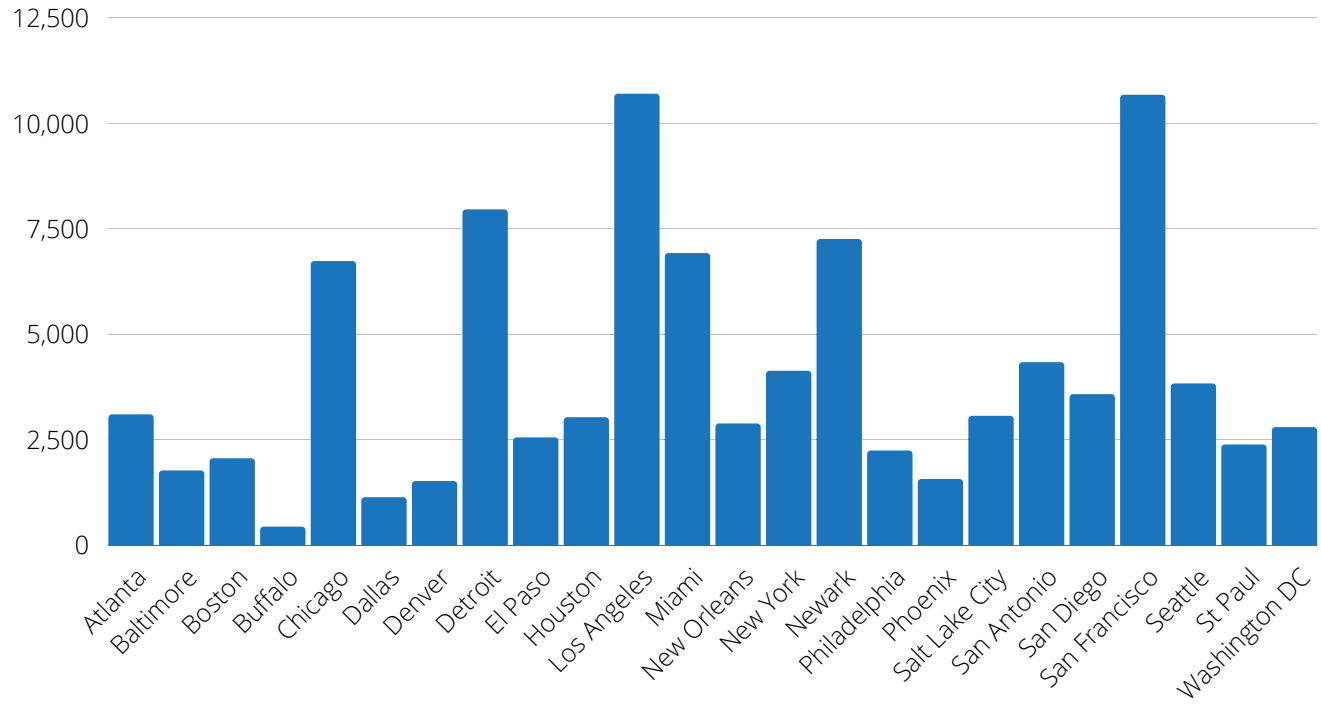
Office Visits: During pre-scheduled office visits, ICE officers or ISAP contractors run individuals through a vetting process—they scan the individual's ID card, verify technology compliance, and conduct various biometric and personal background checks. Officers are instructed to note "clear and visible physical changes to include but not limited to: hair styles, facial hair, scars, marks, tattoos, etc." Such vague guidelines leave the door open to officer discretion and can subject individuals to re-detention on the basis of mere appearance or false suspicion. Individuals also can spend hours at the ICE or contract office awaiting their check-in.

Constant Surveillance: According to ICE's recent statistics, the average time an individual spends in ICE's ATD-ISAP program is 837.8 days.[11] The constant, invasive surveillance can have a physical and emotional impact. Through the above forms of monitoring, both unannounced at home and scheduled at the office, individuals are subject to constant disruption in their everyday lives. Knowing that an enforcement officer could show up at the door at any time can be all-encompassing. It can make it difficult to maintain employment, relationships with and responsibilities to family members, and connections with communities to which they belong. Increased ICE activity with frequent home visits also puts other residents and the entire community at risk.

837.8 DAYS

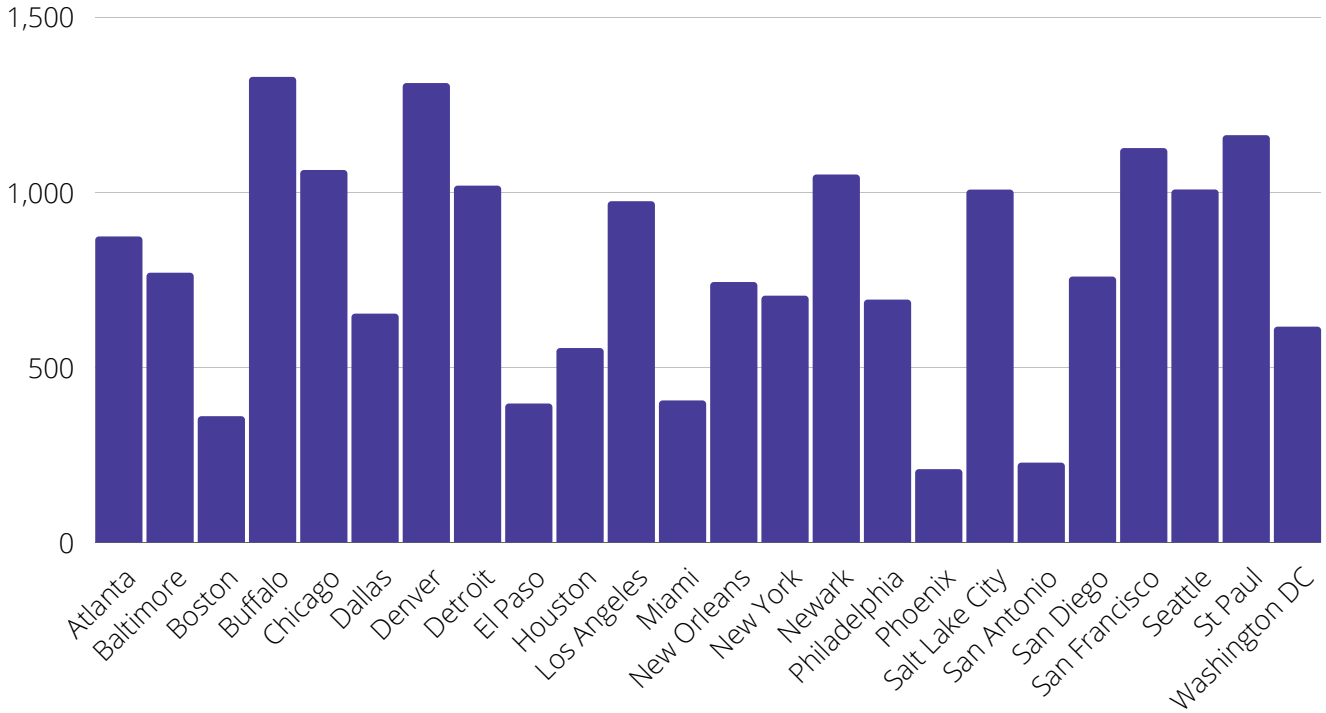
average time an individual spends in ATD-ISAP

TOTAL ENROLLED



Number of individuals enrolled in ICE's ATD-ISAP program by Field Office as of May 2021.
Data compiled from ICE disclosures at https://www.ice.gov/detain/detention-management#tab2.

AVERAGE DAYS IN PROGRAM

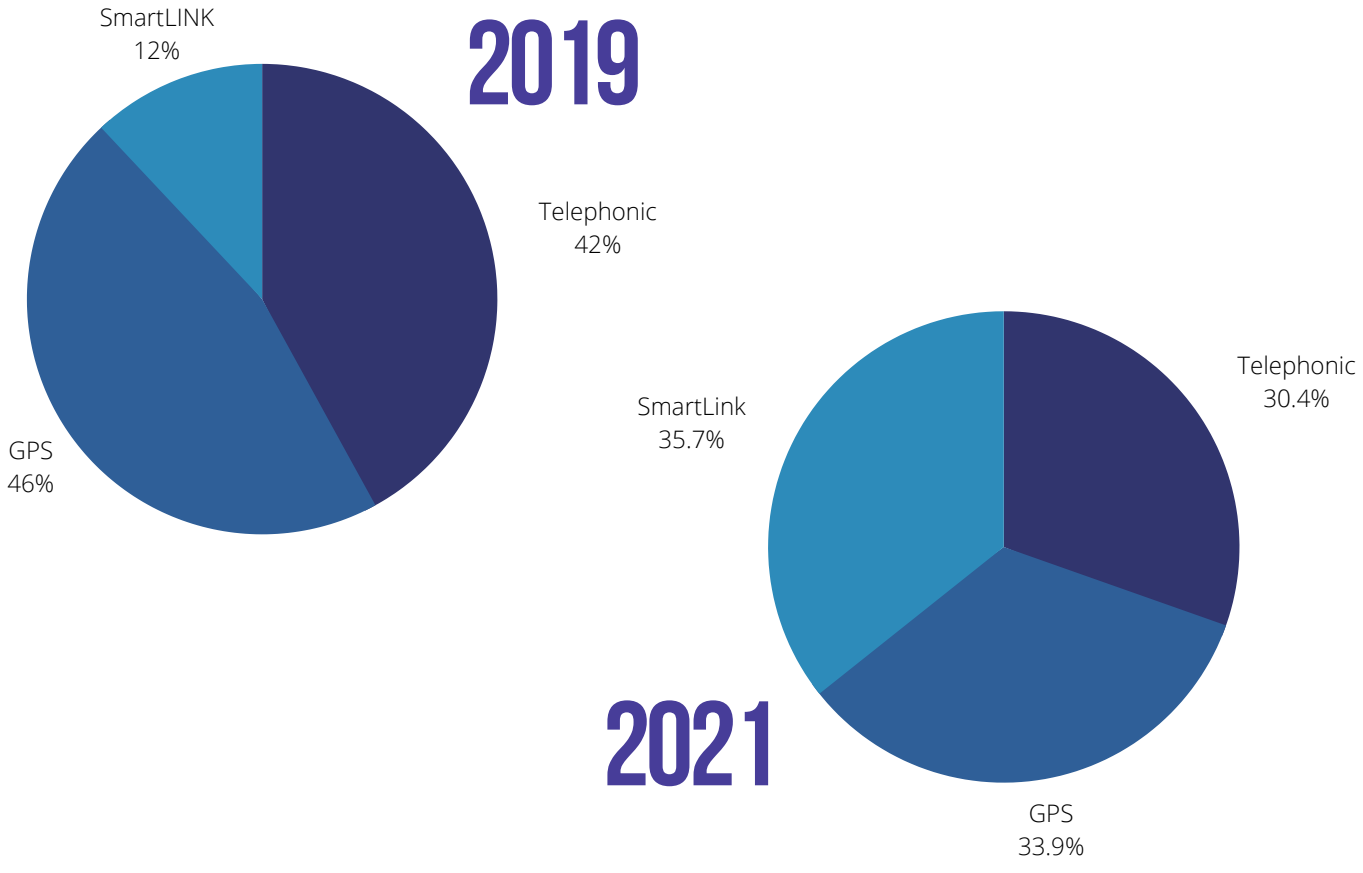


Average number of days an individual is subject to the program by Field Office as of May 2021.
Data compiled from ICE disclosures at https://www.ice.gov/detain/detention-management#tab2.

III. ICE'S ATD PROGRAM TECHNOLOGY DEEP DIVE

The flagship of ICE's Alternatives to Detention (ATD) program, the Intensive Supervision Appearance Program (ISAP), consists of various invasive surveillance plans **including GPS monitoring, voiceprint verification, and facial recognition through an application known as SmartLINK**. All of these forms of surveillance are provided by B.I. Incorporated under its ISAP IV contract.[12]

In June 2019, 42% of individuals in the program used telephonic reporting with voice verification, 46% used GPS monitoring, and 12% used SmartLINK.[13] **As of May 2021, 30.4% of individuals in the program use telephonic reporting, 33.9% use GPS monitoring, and 35.7% use SmartLINK, indicating a shift towards facial recognition check-ins overall**.[14] Advocates attribute at least some of this shift to coronavirus limitations on in-person check-ins and ICE using SmartLINK as a "step down" in the program from GPS monitoring. We discuss each of these surveillance technologies in detail below.



A. GPS Tracking

GPS tracking through an ankle monitor is one of the most prevalent forms of electronic monitoring in the ISAP program.[15] The transmitter, installed during the orientation process, allows ICE to continuously track an individual's location by storing coordinates "at most every three minutes and then uploading those GPS coordinates at least once every four hours to a monitoring system." The monitor offers an on demand "locate function" which allows ICE to obtain an "immediate and accurate one-time location fix in real time." This function can be accessed by an officer through an Internet browser and mobile application to provide "turn-by-turn directions" to the location of the device. In addition, the monitor provides an on demand function to provide "continuous reporting" with "automatic location updates in real time or at a minimum of once every 30 seconds" which can remain active for 20 minutes.

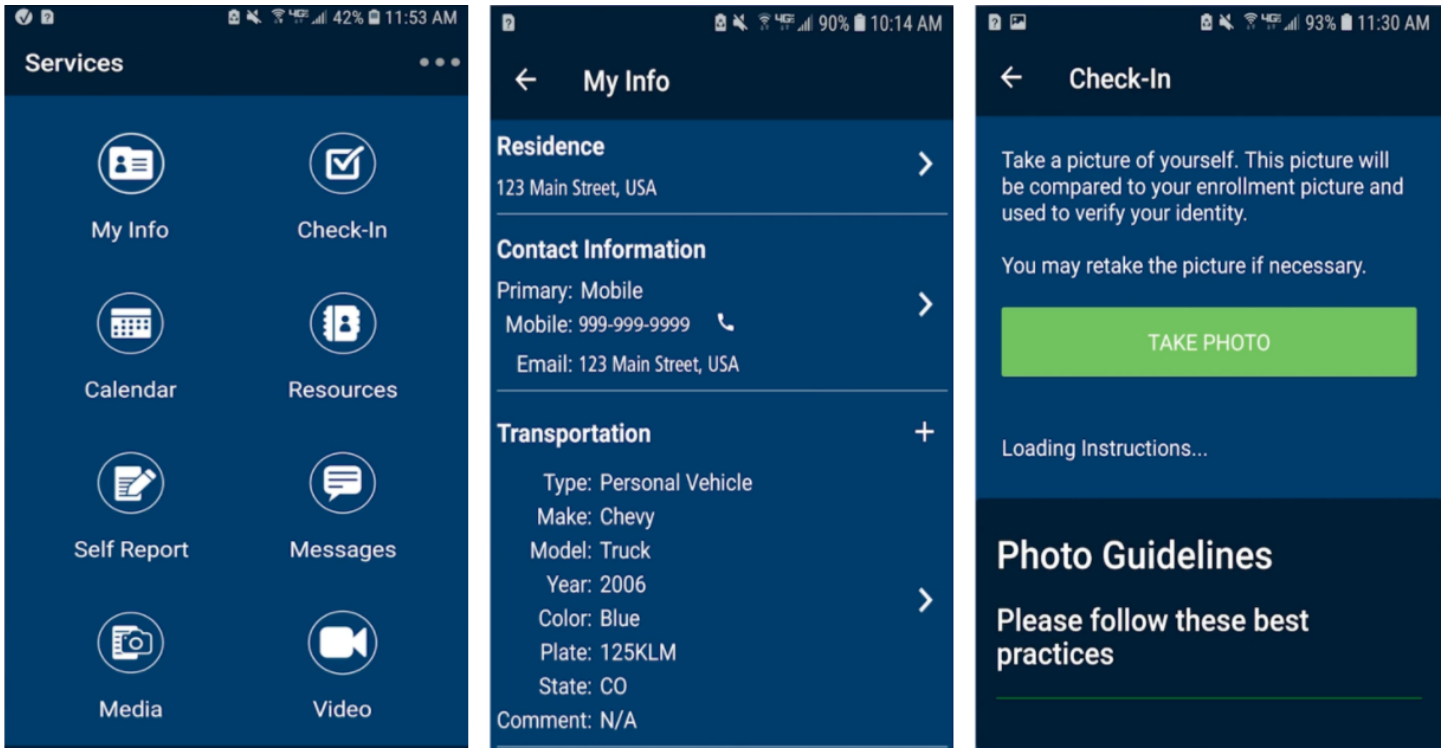
All of this data is stored in a central monitoring facility and then disseminated to ERO by the contractor. As discussed in Section D, ERO can also request a GPS frequency report which pulls data on commonly visited locations of an individual subject to the program. This feature indicates that, though an enforcement officer may not monitor location data in real-time on a continuous basis, ICE has the ability to track the data and retroactively retrieve this information. As discussed below, such GPS surveillance reports were used by ICE to conduct the largest ICE workplace raid in U.S. history.

B. Voice Recognition & Verification

Voice recognition is another form of electronic monitoring used in the ISAP program. At the time of the check-in, an individual receives a notification call from VoiceID. Within a few minutes of the notification, the individual must call VoiceID from an authorized number. The technology then matches the voiceprint of the caller to the voiceprint stored in VoiceID from enrollment.[16]

C. SmartLINK & Facial Recognition

ISAP IV, the most recent ICE contract with B.I. Incorporated for the ISAP program, calls for a "biometric reporting system/mobile platform for various forms of check-in, including facial recognition."[17] B.I. Incorporated utilizes its SmartLINK mobile application for facial recognition reporting.[18] Individuals are required to provide their own phones for the application for fixed and random check-ins and to communicate with ERO, upload photos of documents, request services, confirm appointments, and provide updates on court proceedings. During the COVID-19 pandemic, some individuals have also been required to video conference with their enforcement officers for check-ins.



Screenshots taken from B.I. Incorporated's promotional video on the SmartLINK application. https://bi.com/products-and-services/smartlink-offender-monitoring-mobile-application-software.

When checking in, the individual uploads a photo of themselves which is matched to the photo taken at enrollment using facial recognition software. At the time of the check-in, the app will also capture the coordinates and address of the participant and send them for verification. ICE claims that "SmartLINK does not actively monitor the participant's location through their cell phone as a GPS ankle monitor would. SmartLINK obtains location… during the check-in while using facial recognition but does not gather GPS points at any other time." [19]

The SmartLINK application raises a number of privacy and surveillance concerns. Though ICE claims that the application does not actively monitor location in real-time, it does have the capability to do so. Officers and ISAP contractors can manage their caseloads on their own application called TotalAccess. In TotalAccess, officers can monitor active GPS coordinates of their clients on a shared map. Furthermore, the application's website notes that it provides a "predictive analysis" feature which makes decisions about future risk based on the equipment an individual is using and their movement patterns.[20] While we cannot confirm whether ICE uses this predictive analysis feature as a part of the ISAP program, it is concerning nonetheless that this is an option, especially given ICE's reliance on predictive algorithms in other contexts as explained below.

Finally, SmartLINK's privacy policy indicates that the application can share virtually any information collected through the application, even beyond the scope of the monitoring plan, with the supervising officer.[21] This information includes application usage details and device information like IP address and mobile network information. Reviews on the application also express frustration that it is difficult to use and that the facial recognition feature often does not work correctly, making it even more challenging for those who are responsible for compliance.[22] State criminal justice agencies are also using the application widely and advocates note similar concerns.[23]

Number of Individuals on SmartLINK By Field Office			
Atlanta	859	**New Orleans**	1,365
Baltimore	202	**New York**	717
Boston	724	**Newark**	3,974
Buffalo	19	**Philadelphia**	1,531
Chicago	2,768	**Phoenix**	501
Dallas	258	**Salt Lake City**	2,224
Denver	698	**San Antonio**	791
Detroit	5,254	**San Diego**	1,309
El Paso	972	**San Francisco**	1,827
Houston	549	**Seattle**	1,857
Los Angeles	1,060	**St Paul**	940
Miami	2,321	**Washington DC**	1,725

Number of individuals enrolled in the SmartLINK program by Field Office as of May 2021.
Data compiled from ICE disclosures at https://www.ice.gov/detain/detention-management#tab2.

D. Emergency, Alert & GPS Frequency Reports

ICE outlines a variety of different reports that it can generate from B.I. Incorporated's office or remotely from the ICE Field Office or ICE Headquarters.[24] These reports include emergency reports, alert reports, GPS frequency reports, and court reports. The events that initiate alert and emergency reports demonstrate how strict the monitoring regime is and the impact the surveillance can have on an individual's ability to live freely.

Alert reports are the first level of reports that ICE receives. For voice verification calls, an alert report is generated if an individual does not return a voice verification call within five minutes or if the voice does not match the voice print. For GPS monitoring, an alert report is generated if the device is registering a tamper, or if the device enters a restricted area or leaves an approved area. Emergency reports, the next level of reports, are triggered by other evidence of tampering, unauthorized absence, suicide attempt, police contact, unauthorized travel, contact or threats from individuals connected to "organized crime," or media interest, among others.

These event categories are vaguely defined and provide discretion for broad interpretation to the enforcement officer, raising concerns about how little it may take for an individual to be found in violation of monitoring guidelines and detained. And just as home and office visits pose undue burdens, all of these forms of electronic monitoring impact an individual's ability to gain or retain employment,[25] hinder access to legal resources, limit participation in caregiving, increase risk of domestic violence, negatively impact health, punish family members, and heighten racial disparities.[26] They make it easy for an individual to be subject to detention on the basis of minor mistakes or technology issues, thus resulting in more instances of detention in the end. ICE has also used data from ankle monitors to surveil and conduct workplace raids. **In the case of Koch Foods in Mississippi, historical data from the GPS reports was used to execute search warrants for the largest ICE raid on a workplace in U.S. history, resulting in the arrest of more than 600 individuals.**[27]

IV. FUTURE OF ICE'S DIGITAL PRISONS

Technology companies are constantly developing new technologies and surveillance strategies for immigration and carceral systems. Below we highlight two emerging areas of tech surveillance in which ICE could expand its alternatives to detention program.

A. ICE's Risk Assessment Classification Tool

As is prevalent in the context of criminal detention, ICE has experimented with other predictive technologies to decide who to detain and who to release under supervision. In 2013, ICE began to use a risk assessment classification tool which incorporates about 178 different data fields to calculate the "risk" of release.[28] Information fed into the algorithm includes the following:

- Person details (biographical information, other tracking info including biometrics)
- Encounter description ("apprehension" information, physical description)
- Supporting information (relatives, attorney/representative)
- Special vulnerabilities (physical and mental illness, victim of persecution/abuse)
- Mandatory detention status (subject to mandatory detention/final removal order)
- **Risk to public safety (most severe conviction, disciplinary infractions)**
- **Risk of flight (immigration violation history, community ties)** [29]

Perhaps intentionally so, the algorithm did not lead to the release of large percentages of individuals classified as "low-risk." Between 2013-2017, individuals classified as "low risk" were recommended for pretrial detention with no bond 53% of the time.[30] That percentage went up to 97 percent by 2019. This shift can be attributed to the Trump administration's decision to effectively remove the possibility of release from the algorithm's possible results in 2017.[31] And though ICE claimed that the algorithm is only meant to provide a recommendation to enforcement officers who would then make a final decision, officers followed the algorithm's guidance more than 99% of the time.[32] This example is illuminative of how technology in the detention context is advertised as an unbiased, effective tool but actually used to mask bias.

Furthermore, it is virtually impossible to scientifically and accurately calculate risk to public safety and risk of flight using historical data. Research shows that risk assessments, like ICE's classification tool, are based in racial bias and do not actually provide reliable predictions. A study by ProPublica found that risk assessment algorithms are only slightly more accurate than a coin flip.[33] These algorithms overpredict risk and do not make individualized risk assessments, even if there was a way to do so[34]—they use factors such as race, gender, geography, and criminal history to make biased aggregate group determinations which are then applied to individuals. In addition to rejecting alternatives to detention programs which continue to surveil immigrant communities, we should reject risk assessment classification tools that aim to predict who is a threat.

B. Biometric Wearables

Biometric wearables are tech devices, such as wristbands, watches or head pieces, that can collect biometric data when an individual wears the device on the body. Wearable biometric technology is a lucrative industry anticipated to reach a market value of $27 billion in 2023.[35] Companies traditionally marketed this technology for personal fitness and now advertise uses in the medical, military, labor, prison, and immigration detention sectors. For example, companies like Amazon have developed biometrics wristbands for employees to conduct worker surveillance.[36]

It is important to understand that these biometric devices can collect the most intimate data about an individual such as location, voice, face, iris, blood pressure, heart rate, and even cortisol levels.[37] In the prison and alternatives to detention context, government authorities subject individuals to mandatory wearing of a biometric device and forced data collection.

The use of biometric wearables for prison, pre-trial, probation, and other alternatives to detention programs in the U.S. is nascent but government interest is growing. In 2019, the Department of Justice funded research that supported the use of biometric wearables combined with smartphone app surveillance for individuals in reentry programs.[38] So far, governments in the United Kingdom and Hong Kong have mandated some type of biometric wearable for an individual's incarceration or pre-trial or probation supervision.[39] U.S. companies like E-Cell are selling biometric wearables for pre-trial and probation supervision. In the future, ICE may seek to expand its ATD-ISAP program into biometric wearables.[40]

V. CONCLUSION

There are many forms of alternatives to detention that have surfaced in both the immigration and criminal detention contexts. Most of the solutions provided, including the ones mentioned in this report, do more harm and inhibit any true progress in providing the social and economic tools for immigrants to thrive in their communities. Electronic monitoring not only poses undue burdens on immigrants, including physical harm to their bodies, but increases the number of individuals under ICE's supervision and in detention. These programs further show the links between the immigration and criminal systems and the profit motivations in tying these systems together. Policymakers and advocates should reject calls to invest in carceral alternatives to detention programs and focus on solutions that put an end to all forms of immigrant surveillance and detention.

Are you or someone you know on ICE's ATD-ISAP program? If yes, please fill out this questionnaire to help us learn more about the program.

bit.ly/ATDISAPSurvey

@JustFuturesLaw
@ConMijente

ENDNOTES

1. OIG, *U.S. Immigration & Customs Enforcement's Alternatives to Detention (Revised)*, Report (Feb. 2015), https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-22_Feb15.pdf ("OIG Report 2015").

2. Press Release, *The GEO Group Announces Five-Year Contract With U.S. Immigration & Customs Enforcement for Intensive Supervision and Appearance Program (ISAP)*, Business Wire, Mar. 24, 2020, https://www.businesswire.com/news/home/20200324005145/en/The-GEO-Group-Announces-Five-Year-Contract-With-U.S.-Immigration-and-Customs-Enforcement-for-Intensive-Supervision-and-Appearance-Program-ISAP.

3. *Id.*

4. Jaden Urbi, *Here's Who's Making Money From Immigration Enforcement*, CNBC, Jun. 29, 2018, https://www.cnbc.com/2018/06/28/companies-profiting-immigration-enforcement-private-sector-prison-tech.html.

5. ICE, Detention Management, https://www.ice.gov/detain/detention-management#tab2.

6. DHS, FY2022 Budget in Brief, https://www.dhs.gov/sites/default/files/publications/dhs_bib_-_web_version_-_final_508.pdf. *See also* Jason Fernandes, *Alternatives to Detention and the For-Profit Immigration System*, Center for American Progress, June 9, 2017, https://www.americanprogress.org/issues/immigration/news/2017/06/09/433975/alternatives-detention-profit-immigration-system.

7. National Immigrant Justice Center, *A Better Way: Community-Based Programming As an Alternative to Incarceration*, Report (Apr. 2019), https://immigrantjustice.org/sites/default/files/uploaded-files/no-content-type/2019-04/A-Better-Way-report-April2019-FINAL-full.pdf.

8. *No More Shackles*, MediaJustice (Apr. 2020), https://mediajustice.org/wp-content/uploads/2020/04/NoMoreShackles_PretrialReport_2019-final-draft.pdf. ("MediaJustice Report 2020"); Molly Hennessy-Fiske, *Immigrants Object to Growing Use of Ankle Monitors After Detention*, L.A. Times, Aug. 2, 2015, https://www.latimes.com/nation/immigration/la-na-immigrant-ankle-monitors-20150802-story.html.

9. The following information in this section regarding the orientation process is taken from the ISAP III contract, *available at* https://www.ice.gov/doclib/foia/contracts/biIncorporatedHSCEDM14D00004.pdf. The contract for ISAP IV is not public; *see also* Letter from ICE to Sen. Wyden, Oct. 16, 2018, https://www.documentcloud.org/documents/5014365-102576-Wyden-Final-Signed-Response.html.

10. The following information in this section regarding home and office visits is taken from the ISAP III contract.

11. ICE, Detention Management, https://www.ice.gov/detain/detention-management#tab2.

12. *See supra* n. 9.

13. Audrey Singer, *Immigration: Alternatives to Detention (ATD) Programs, Congressional Research Service* (July 2019), Report, https://fas.org/sgp/crs/homesec/R45804.pdf ("CRS Report 2019").

14. ICE, Detention Management, https://www.ice.gov/detain/detention-management#tab2.

15. The following information in this section regarding requirements for GPS tracking is taken from ISAP IV's Request for Proposal Attachment 1, *available at* https://beta.sam.gov/api/prod/opps/v3/opportunities/resources/files/998637ed5b69c4489092c751f1fa45aa/download?api_key=null&token=.

16. BI VoiceID, B.I. Incorporated, https://bi.com/products-and-services/voiceid-voice-verification-device-biometric-system; ICE, ATD Infographic, https://www.ice.gov/doclib/detention/atdInfographic.pdf.

17. The following information in this section regarding requirements for SmartLINK is taken from ISAP IV's Request for Proposal Attachment 1. *See supra* n 15, at 12.

18. *See supra* n 9.

19. CRS Report 2019.

20. B.I. TotalAccess, B.I. Incorporated, https://bi.com/products-and-services/totalaccess-offender-monitoring-web-based-software; *see also* B.I. SmartLINK, B.I. Incorporated, https://bi.com/products-and-services/smartlink-offender-monitoring-mobile-application-software.

21. B.I. SmartLINK Privacy Policy, B.I. Incorporated, https://bi.com/products-and-services/bi-smartlink-privacy-policy.

22. B.I. SmartLINK, Google Play, https://play.google.com/store/apps/details?id=com.biinc.mobile.client&showAllReviews=true.

23. Todd Feathers, *'They Track Every Move': How U.S. Parole Apps Created Digital Prisoners*, Guardian, Mar. 4, 2020, https://www.theguardian.com/global-development/2021/mar/04/they-track-every-move-how-us-parole-apps-created-digital-prisoners.

24. The following information in this section regarding emergency and alert reports is taken from the ISAP III contract. *See supra* n. 9.

25. See David Yaffe-Bellany, *'It's Humiliating': Released Immigrants Describe Life with Ankle Monitors*, Houston Public Media, Aug. 10, 2018, https://www.houstonpublicmedia.org/articles/news/2018/08/10/299581/its-humiliating-released-immigrants-Describe-life-with-ankle-monitors.

26. MediaJustice Report 2020.

27. Jeff Amy, *Documents: Plant Owners 'Willfully' Used Ineligible Workers*, Associated Press, Aug. 9, 2019, https://apnews.com/article/711d52e4bccd41bc894907a9e1645d09; ICE criminal warrant, at 11-15, *available at* https://www.ice.gov/sites/default/files/documents/Document/2019/kochfoods-319mj.pdf.

28. OIG Report 2015.

29. *Id.*

30. Sam Biddle, *ICE's New York Office Uses A Rigged Algorithm to Keep Virtually All Arrestees in Detention*, Intercept, Mar. 2, 2020, https://theintercept.com/2020/03/02/ice-algorithm-bias-detention-aclu-lawsuit.

31. *Id.*

32. *Id.*

33. Julia Angwin et al., *Machine Bias*, ProPublica, May 23, 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

34. National Association of Criminal Defense Lawyers, *Making Sense of Pretrial Risk Assessments*, Report (June 2018), https://www.nacdl.org/Article/June2018-MakingSenseofPretrialRiskAsses.

35. Market Research Future Release, *Wearable Medical Devices Market Size Projection, Growth Value, Sales Statistics, Share Analysis, COVID-19 Impact and Global Medical Wearable Industry Trends By 2023*, MedGadget, Aug. 18, 2020, https://www.medgadget.com/2020/08/wearable-medical-devices-market-size-projection-growth-value-sales-statistics-share-analysis-covid-19-impact-and-global-medical-wearable-industry-trends-by-2023.html.

36. Ceylan Yeginsulf, *Workers Slack Off, the Wristband Will Know. (And Amazon Has a Patent for It)*, N.Y. Times, Feb. 2, 2018, https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html; Sam Biddle, *Coronavirus Monitoring Bracelets Flood the Market, Ready to Snitch on People Who Don't Distance*, Intercept, May 25, 2020, https://theintercept.com/2020/05/25/coronavirus-tracking-bracelets-monitors-surveillance-supercom.

37. Becca Cady, *5 Sensor Technologies That Are Set to Break Out in Wearables*, Wareable, Feb. 27, 2019, https://www.wareable.com/wearable-tech/5-wearable-sensor-technologies-incoming-7026.

38. Brannon Green & Christopher Rigano, *Specialized Smartphones Could Keep Released Offenders on Track for Successful Reentry*, National Institute of Justice, Apr. 20, 2020, https://nij.ojp.gov/topics/articles/specialized-smartphones-could-keep-released-offenders-track-successful-reentry.

39. *'Sobriety Ankle Tags' Rolled Out Across England*, BBC, Mar. 21, 2021, https://www.bbc.co.uk/news/amp/uk-politics-56583153; Zara Stone, *Cell Tech: China's Futuristic Prisons Plans*, Forbes, Mar. 4, 2019, https://www.forbes.com/sites/zarastone/2019/03/04/cell-tech-chinas-futuristic-prisons-plans/?sh=763e57d7768d; Katya Pivcevic, *Biometrics, Drones and Robotic Guards: Inside Hong Kong's First 'Smart Prison'*, Biometric Update, Dec. 23, 2020, https://www.biometricupdate.com/202012/biometrics-drones-and-robotic-guards-inside-hong-kongs-first-smart-prison.

40. E-Cell Band, https://e-cell.com.

#NODIGITALPRISONS

JUST
FUTURES
LAW

mijente