Harvard Journal of Law & Technology
Volume 36, Number 1 Fall 2022

THE LIMIT DOES NOT EXIST: HOW SMARTPHONE TECHNOLOGY EXPANDS ELECTRONIC MONITORING AND A PROPOSED LIMITATION

*Kristin Oakley**

TABLE OF CONTENTS

---

* Duke University School of Law, Candidate for J.D., 2023; New York University, M.A., Journalism, 2014. Thank you to the editors of JOLT, particularly Mark Sfreddo and Laura Hipple for thoughtful edits and early confidence, to Professor Jolynn Dellinger for encouragement and mentorship, and to Professor Kate Weisburd for her time and scholarship. And — because this Note would not be possible without them — thank you to my parents and my partner, Dhane, for their patience and support throughout the writing process.

I. INTRODUCTION

> YOU HAD TO LIVE — DID LIVE, FROM HABIT THAT BECAME INSTINCT — IN THE ASSUMPTION THAT EVERY SOUND YOU MADE WAS OVERHEARD, AND, EXCEPT IN DARKNESS, EVERY MOVEMENT SCRUTINIZED.
>
> — GEORGE ORWELL[1]

Smartphone tracking is the newest advancement in electronic monitoring,[2] and the practice is proliferating. Electronic monitoring is "a way of remotely regulating and enforcing spatial and temporal schedules, enshrined in law and imposed by courts and prison[s]."[3] Historically, it was limited to ankle monitors used within community supervision (i.e., probation, parole, and supervised release).[4] Ankle monitors are inherently limited by their technology, which primarily enables location tracking. But today's smartphones — and the apps that empower them — are powerful, unparalleled additions to electronic monitoring.[5] They introduce technologies like conversation and network monitoring, phone locking and settings control, facial recognition, and increased metadata recording, among other capabilities.[6]

---

1. GEORGE ORWELL, NINETEEN EIGHTY-FOUR 4 (1st American ed., Harcourt, Brace & World 1949).

2. This Note will use "electronic monitoring" to refer to the overall tracking system that historically uses ankle monitors and "smartphone monitoring," in various forms, to denote tracking via smartphone.

3. Mike Nellis, *Electronic Monitoring, Neoliberalism and the Shaping of Community Sanctions*, *in* CRIMINAL JUSTICE AND PRIVATISATION 32, 32 (Philip Bean ed., 2020).

4. *See* PEW CHARITABLE TRS., USE OF ELECTRONIC OFFENDER-TRACKING DEVICES EXPANDS SHARPLY 2 (2016), https://www.pewtrusts.org/-/media/assets/2016/10/use_of_electronic_offender_tracking_devices_expands_sharply.pdf [https://perma.cc/5XUK-YGJU] ("Correctional authorities use ankle bracelets and other electronic tracking devices to increase compliance with the conditions of pretrial release, probation, or parole among accused and convicted offenders residing in the community.").

5. Before the COVID-19 pandemic, tracking via smartphones was growing within the field of electronic monitoring but was not widespread. *Id.* Such tracking increased during the pandemic, as did all uses of electronic monitoring. *See* April Glaser, *Incarcerated at Home: The Rise of Ankle Monitors and House Arrest During the Pandemic*, NBC NEWS (July 5, 2021, 11:30 AM), https://www.nbcnews.com/tech/tech-news/incarcerated-home-rise-ankle-monitors-house-arrest-during-pandemic-n1273008 [https://perma.cc/X9LT-EMZL] ("During the pandemic, as jails raced to release incarcerated people because prisons became coronavirus hot spots, many judges nationwide responded by putting those who were being released in electronic ankle monitors that tracked their movements 24 hours a day.").

6. *See infra* Part III.

Compared to ankle monitors' limited capabilities, smartphones' advanced features precipitate a fundamental change in electronic monitoring, allowing nearly limitless surveillance.

Widespread use of smartphone monitoring has broad consequences for justice-involved individuals[7] and society at large. In the past decade, electronic monitoring has expanded within community supervision and beyond, notably within immigration enforcement and pretrial release.[8] But the supposed benefits of electronic monitoring are not empirically supported: "[N]o empirical evidence suggests that broadly applied electronic surveillance corresponds to greater public safety, increased rehabilitation, or lower recidivism rates."[9] Privacy scholars, criminal justice activists, and anyone worried about increasing surveillance should be concerned about the possibility of nearly limitless smartphone monitoring in community supervision.[10]

This Note argues that the influx of smartphones and apps — and their seemingly unlimited technological capabilities — requires a new legal approach to protecting the rights and privacy of those being electronically monitored.[11] Though other scholarship explores the implications of smartphone surveillance or electronic monitoring, no known

---

7. "Justice-involved individuals" refers to people who have come into contact with the criminal justice system in some form, from arrest to incarceration and reentry. CONSUMER FIN. PROT. BUREAU, JUSTICE-INVOLVED INDIVIDUALS AND THE CONSUMER FINANCIAL MARKETPLACE 2 (2022), https://files.consumerfinance.gov/f/documents/cfpb_jic_report_2022-01.pdf [https://perma.cc/V8EF-DBSR].

8. *See* MAYA SCHENWAR & VICTORIA LAW, PRISON BY ANY OTHER NAME 19 (2020) ("The surge in law-enforcement-based electronic monitoring over the past decade — more than doubling between 2005 and 2015 — confirms this reality. Today, about 200,000 Americans are chained by monitors.").

9. Kate Weisburd, *Sentenced to Surveillance: Fourth Amendment Limits on Electronic Monitoring*, 98 N.C. L. REV. 717, 723 (2020) [hereinafter *Sentenced to Surveillance*] (citations omitted); *see also* SCHENWAR & LAW, *supra* note 8, at 35 (noting that "intensive supervision actually increases, rather than decreases, the chance that someone will be rearrested and reconvicted."). *See generally* Jennifer L. Doleac, *Study After Study Shows Ex-Prisoners Would Be Better Off Without Intense Supervision*, BROOKINGS INST.: UP FRONT (July 2, 2018), https://www.brookings.edu/blog/up-front/2018/07/02/study-after-study-shows-ex-prisoners-would-be-better-off-without-intense-supervision [https://perma.cc/U4VZ-6YG2] (summarizing several studies that show "we could maintain public safety and possibly even improve it with less supervision — that is, fewer rules about how individuals must spend their time and less enforcement of those rules").

10. *See* Todd Feathers, *'They Track Every Move': How US Parole Apps Created Digital Prisoners*, GUARDIAN (Mar. 4, 2021, 6:00 AM), https://www.theguardian.com/global-development/2021/mar/04/they-track-every-move-how-us-parole-apps-created-digital-prisoners [https://perma.cc/4UQV-D9FY].

11. This Note does not address Fourth Amendment privacy protections because people subject to community supervision are increasingly assumed to have consented to electronic monitoring, either implicitly or explicitly. *See* Weisburd, *Sentenced to Surveillance*, *supra* note 9, at 737 ("Consent, either on its own or as a factor, has recently emerged as an oft-invoked justification by government officials for imposing otherwise unconstitutional electronic searches or surveillance of people on community supervision.").

works explore their legal intersection.[12] This Note recommends using the Fair Information Practice Principles ("FIPPs") to guide law enforcement agencies, judges, and legislatures in limiting the technological expansion and data collection enabled by smartphones and apps. The FIPPs are principles used by governmental organizations — like the Department of Homeland Security[13] and the Organisation for Economic Co-operation and Development ("OECD")[14] — to inform privacy laws worldwide. They originated in a 1973 report by the U.S. Department of Health, Education, and Welfare and were later integrated into the Privacy Act of 1974.[15] The FIPPs guide best practices regarding the collection, use, and disclosure of data both inside and outside the criminal justice system. This Note seeks to illuminate how the FIPPs can provide appropriate limits on potentially limitless smartphone monitoring. Because available technology no longer inherently limits the reach of surveillance, the law must create such boundaries.

Part II details electronic monitoring's history, functionality, justifications, and recent growth. Part III explains how the criminal justice system's use of smartphones and apps in electronic monitoring fundamentally changes the practice by introducing technology that is no longer inherently limited. Part IV explores why now is the time to limit this rapidly evolving and unregulated use of smartphones in electronic monitoring. Finally, Part V recommends a harm-reduction framework based on well-regarded, widely applied privacy principles — the FIPPs — and suggests how judges, legislators, and law enforcement agencies may limit smartphone surveillance.

---

12. *See, e.g.*, Avlana K. Eisenberg, *Mass Monitoring*, 90 S. CAL. L. REV. 123, 127 (2017) (presenting the "first sustained examination of mass monitoring and its place in the criminal justice landscape"); Kate Weisburd, *Punitive Surveillance*, 108 VA. L. REV. 147, 152 (2022) [hereinafter *Punitive Surveillance*] (citations omitted) ("Punitive surveillance has become not so much an actual alternative to incarceration, but rather an alternative *form* of incarceration"); Weisburd, *Sentenced to Surveillance*, *supra* note 9; Kentrell Owens, Anita Alem, Franziska Roesner & Tadayoshi Kohno, *Electronic Monitoring Smartphone Apps: An Analysis of Risks from Technical, Human-Centered, and Legal Perspectives*, PROC. 31ST USENIX SEC. SYM. 4077, 4077 (2022), https://www.usenix.org/system/files/sec22-owens.pdf [https://perma.cc/63LG-JMUR] (conducting "a privacy-oriented analysis of [sixteen] Android apps used for electronic monitoring" technically and through user reviews).

13. *The Fair Information Practice Principles*, DEP'T OF HOMELAND SEC. (2008), https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles [https://perma.cc/C385-C3BE] ("The Fair Information Practice Principles are the framework for privacy policy at the Department of Homeland Security.").

14. OECD, THE OECD PRIVACY FRAMEWORK 65, 75 (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [https://perma.cc/5X83-FY44].

15. *See* Cheryl Saniuk-Heinig, *50 Years and Still Kicking: An Examination of FIPPs in Modern Regulation*, IAPP NEWS (May 25, 2021), https://www.iapp.org/news/a/50-years-and-still-kicking-an-examination-of-fipps-in-modern-regulation [https://perma.cc/5NZB-TYH3].

II. ELECTRONIC MONITORING: HOW WE GOT TO NOW

Electronic monitoring is a vast enterprise. While there are no comprehensive statistics about electronic monitoring in the criminal justice system, U.S. Immigration and Customs Enforcement ("ICE") releases data about monitoring in the immigration system. In 2022, ICE's Alternative to Detention program electronically monitored 316,700 people, including 255,602 who were monitored through BI Incorporated's SmartLink smartphone app.[16] Electronic monitoring is managed jurisdiction-by-jurisdiction, making data collection difficult.[17] Typically, courts and parole boards require consent to electronic monitoring as a condition of prison or jail release, either pretrial or post-sentencing.[18] All fifty states, the District of Columbia, and the federal government use electronic monitoring.[19] A survey of 101 agency electronic monitoring policies across forty-four states and the District of Columbia showed that 49.50% of policies governed people on pretrial release, 50.50% of policies governed people on probation, and 39.60% of policies governed people on parole.[20]

A. Electronic Monitoring's History and Functionality

The original technology behind electronic monitoring was developed in the 1960s when Harvard social psychology students and twin brothers Robert and Kirk Gable created radio-operated devices to help juvenile offenders achieve rehabilitation through positive

16. *See* Gaby Del Valle, *ICE Is Subjecting a Record Number of Asylum Seekers to Electronic Monitoring*, THE NATION (Oct. 18, 2022), https://www.thenation.com/article/society/migrants-ice-alternatives-detention [https://perma.cc/G62X-PAG6] (citing *ICE Increases Use of Ankle Monitors and Smartphones to Monitor Immigrants*, TRANSACTIONAL RECS. ACCESS CLEARINGHOUSE (Sept. 30, 2022), https://trac.syr.edu/whatsnew/email.220930.html [https://perma.cc/6QVZ-PUFU]); *see also* PEW CHARITABLE TRS., *supra* note 4, at 2 (noting that in 2015, the number of people on electronic monitoring in the criminal justice system "probably exceeded 131,000," not including those tracked within the immigration system).

17. KATE WEISBURD ET AL., GEO. WASH. U. L. SCH., ELECTRONIC PRISONS: THE OPERATION OF ANKLE MONITORING IN THE CRIMINAL LEGAL SYSTEM 3 (2021) [hereinafter ELECTRONIC PRISONS] ("While some agencies track the number of people on monitors, there is no comprehensive statistical portrait of how many people are on monitors in the United States today, much less any demographic data.").

18. *Id.*; *see also* CHARLES DOYLE, CONG. RSCH. SERV., RL31653, SUPERVISED RELEASE (PAROLE): AN OVERVIEW OF FEDERAL LAW 2 (2021) (footnotes omitted) ("Federal courts ordinarily set the terms and conditions of supervised release when they sentence a criminal defendant to prison, and '[t]he duration, as well as the conditions of supervised release are components of a sentence.'" (quoting United States v. Wilson, 707 F.3d 412, 414 (3d Cir. 2013))).

19. PEW CHARITABLE TRS., *supra* note 4, at 1.

20. The records collected detailed "specific policies, procedures, contracts and rules." WEISBURD ET AL., ELECTRONIC PRISONS, *supra* note 17, at 2, 5. The percentages do not add to 100% due to overlap between categories.

reinforcement.[21] "The purpose was to give rewards to the offenders when they were where they were supposed to be, that is they were in [a] drug treatment session, or went to school or a job," as Robert Gable explained to *NPR*.[22] Then, in the 1970s, a Spiderman comic inspired an Arizona judge to develop the first ankle monitor using this same rehabilitative technology with the goal of reducing overcrowding and inhibiting prison escapes.[23]

Ankle monitors historically relied on radio signal technology called Radio Frequency Identification ("RFID").[24] RFID is a simple tag-and-reader system.[25] The ankle monitor is the tag, and a radio device within someone's home is the reader.[26] The tracking is thus primarily limited to knowing whether someone is within range of the reader, i.e., their home.[27] RFID monitors are typically worn around the ankle or wrist[28] and are battery-operated (often requiring two or more hours of charging per day).[29] More complex versions of RFID tags can track temperature, location, and motion.[30] RFID-enabled ankle monitors are typically used to verify compliance with a curfew or house arrest, but their use is declining.[31] RFID is a limited binary technology that knows whether someone is near the tag reader — and nothing more.[32]

By contrast, modern ankle monitors employ Global Positioning System ("GPS") technology.[33] Unlike RFID, which only knows

21. Emma Anderson, *The Evolution of Electronic Monitoring Devices*, NPR NEWS (May 24, 2014, 5:26 AM), https://www.npr.org/2014/05/22/314874232/the-history-of-electronic-monitoring-devices [https://perma.cc/JXT7-GT77].

22. *Id.* (explaining that rewards included options such as "a free haircut, pizza, concert tickets").

23. *See* Robert S. Gable, *The Ankle Bracelet is History: An Informal Review of the Birth and Death of a Monitoring Technology*, 27 J. OFFENDER MONITORING 4, 5 (2014).

24. *See* PEW CHARITABLE TRS., *supra* note 4, at 2.

25. DEP'T OF HOMELAND SEC., SMART BORDER ALLIANCE RFID FEASIBILITY STUDY FINAL REPORT attach. D, at D-1 (2005), https://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachD.pdf [https://perma.cc/84BN-59JB].

26. *See* PEW CHARITABLE TRS., *supra* note 4, at 2 (explaining RFID devices "are most commonly used to supervise those on house arrest or confinement and to enforce curfews by monitoring an offender's presence either continuously or during specified times").

27. *Id.* ("RF devices monitor offenders' presence in or absence from a fixed location.").

28. *Id.*

29. As one report explains, "[p]eople on monitors must charge their devices at regular times every day and for a predetermined and significant number of consecutive hours." WEISBURD ET AL., ELECTRONIC PRISONS, *supra* note 17, at 8. One such charging rule states that wearers must charge "for 2 hours a day" and "will NOT sleep while charging." *Id.* In some jurisdictions, failure to keep the device charged is a crime and/or violation of the terms of release and results in a return to prison or jail. *See id.*

30. *See* DEP'T OF HOMELAND SEC., *supra* note 25, at D-3.

31. *See* PEW CHARITABLE TRS., *supra* note 4, at 4.

32. WEISBURD ET AL., ELECTRONIC PRISONS, *supra* note 17, at 4 ("This technology is binary — the surveillance simply confirms someone's presence at a particular location.").

33. PEW CHARITABLE TRS., *supra* note 4, at 2.

whether someone is in the reader's range,[34] GPS enables real-time tracking through monitoring centers, triangulated cell towers, and satellite signals.[35] Further, this technology allows supervising agencies to set up "exclusion zones," barring offenders from places such as schools, playgrounds, or victims' homes and places of employment.[36] GPS-enabled ankle monitors can also have other capabilities, such as voice recording,[37] blood alcohol monitoring,[38] and other behavior-tracking features. While these additional technologies have expanded the data collection scope, GPS-enabled ankle monitors are still relatively limited in their capabilities and are used primarily for location tracking.

B. Reasons for Use and Correlated Expansion

Many justifications for electronic monitoring are interrelated and foreshadow its recent expansion. Electronic monitoring trends during the COVID-19 pandemic demonstrate how, as jails and prisons sought to reduce overcrowding, corrections officials released incarcerated people and instead tracked them through electronic monitoring.[39] Similarly, pretrial detention was avoided in favor of release and tracking via electronic monitoring.[40] Putting more people on electronic monitoring during the initial stages of the pandemic provided two key benefits for law enforcement: cost savings[41] and the increased role of prison alternatives.[42]

---

34. *See id.*

35. *Id.*

36. *Id.* ("When monitored offenders enter such exclusion zones, GPS devices alert supervising agencies, which can then take action.").

37. Ankle monitors with voice capabilities have been used in Chicago to call and record juveniles without their consent. *See* Kira Lerner, *Chicago's Ankle Monitors Can Call and Record Kids Without Their Consent*, BLOOMBERG: CITYLAB (Apr. 8, 2019, 1:30 PM), https://www.bloomberg.com/news/articles/2019-04-08/ankle-monitors-introduce-a-new-form-of-surveillance [https://perma.cc/54F7-TQC8].

38. *See, e.g.*, *SCRAM CAM Continuous Alcohol Monitoring*, SCRAM SYS. (2021), https://www.scramsystems.com/monitoring/scram-continuous-alcohol-monitoring [https://perma.cc/N49H-5D9S]; *BI TAD: Transdermal Alcohol Detector*, BI INC. (2021), https://www.bi.com/alcohol [https://perma.cc/MK8Y-3R5D].

39. *See* Glaser, *supra* note 5, at 1.

40. *Id.*

41. *See id.* Given budgets strained by additional cleaning, testing, and caretaking needs, electronic monitoring provided a cheaper solution to the problems posed by the pandemic. *Id.*

42. Weisburd, *Punitive Surveillance*, *supra* note 12, at 149–50 ("Fueled by the COVID-19 pandemic and increasingly bipartisan support for decarceration efforts, punitive surveillance is often touted as a humane alternative to incarceration and is expanding substantially with little oversight or regulation."); *see also* Michelle Alexander, *Foreword* to MAYA SCHENWAR & VICTORIA LAW, PRISON BY ANY OTHER NAME: THE HARMFUL CONSEQUENCES OF POPULAR REFORMS ix, ix (2020) ("We are now living in a moment in which large numbers of people are suddenly paying attention to the United States' astronomical incarceration rate and 'alternatives' to incarceration have become a topic of mainstream debate.").

1. Cost Savings

One of the biggest reasons to use electronic monitoring is cost savings for agencies.[43] Not only does electronic monitoring save the state money (by reducing costs for housing, feeding, and caring for prisoners), it can also *make* money (in some cases offsetting the cost of lost cash bail revenue).[44] Whereas prisons and jails are state-funded, electronic monitoring is paid for by the monitored individuals themselves.[45] Charges include a setup fee (usually a few hundred dollars) and a daily usage fee (commonly around $10 per day or about $300 per month).[46] Some jurisdictions even profit by stacking surcharges on top of the service provider's fee. For example, Mountlake Terrace, Washington, charges $20 per day for electronic monitoring, even though the private company only charges the town $5.75 per person.[47] Thus, some individuals have opted for direct monitoring by a private company to avoid paying the state's additional fees.[48] Overall, the cost-saving — or cost-shifting — plus the promise of efficiency appeals to agencies.

2. Prison Alternatives

Law enforcement agencies increasingly use electronic monitoring to respond to calls for prison alternatives.[49] Prisons and jails responded to pressure to reform the cash bail system by increasing electronic monitoring in pretrial release.[50] But it has not worked as some reformists

43. *See* Nellis, *supra* note 3, at 43 (electronic monitoring "in some shape or form, has been seen by all governments as a more efficient solution to re-offending"); SCHENWAR & LAW, *supra* note 8, at 42 ("[I]n La Crosse County, Wisconsin, monitors cost $6 daily whereas a jail bed costs $83 per day."); Joe Russo & George Drake, *Monitoring With Smartphones: A Survey of Applications*, 30 J. OFFENDER MONITORING 5, 5 (2017) ("Agencies often look to technology to help them do more with less and many are now exploring smartphone applications as a way of providing cost-effective supervision services to large groups of offenders.").

44. *See* SCHENWAR & LAW, *supra* note 8, at 41–42 (explaining the different ways in which local agencies manage the costs and fees of electronic monitoring systems).

45. *Id.* at 10. At least one company refers to this payment plan as the "offender-funded" model. *Funding Options for All Programs*, SENTINEL (2021), https://www.sentineladvantage.com/offender-funded-programs [https://perma.cc/KS4Y-KEHF] ("This revolutionary offender-funded model removes all of the agency's financial responsibilities for their offender monitoring programs.").

46. SCHENWAR & LAW, *supra* note 8, at 41 (explaining that one company charges a $179 setup fee and then $9.25 per day a device is in use).

47. *Id.* at 42 ("According to the city's website, the revenue generated from the fees 'fully funds the Custody Officer position, the rental of the EHM [electronic home monitoring] equipment, and EHM fees for indigent defendants.'").

48. *Id.* at 43 (detailing how one person chose to be monitored by "a private company [that] is less intrusive — and less costly — than the county-run program").

49. As Schenwar and Law note, it is "a stark example of how pervasive incarceration has become that even many of the alternatives, which are couched in the language of healing, actually rely on forcible confinement, surveillance, and utter control." *Id.* at 18.

50. *Id.* at 31 (footnote omitted) ("But of those who were released without having to pay bail [in Cook County, Illinois], 22 percent were placed in electronic shackles. (The previous

hoped. Electronic monitoring scholar Mike Nellis explains that "sanctions introduced as alternatives to imprisonment get used alongside imprisonment rather than instead of it, often with less serious offenders (net-widening), with the result that prison and community sanction use expand in tandem . . . ."[51] In cities like Chicago, San Francisco, and Indianapolis, an even higher number of people are subjected to electronic monitoring during pretrial release periods than would have been jailed under the previous system.[52] People may assume that those on electronic monitoring would otherwise be in prison, but "[t]here is no empirical evidence . . . that monitoring is used [solely] as an alternative to incarceration."[53] So, in addition to using monitoring as a substitute for jail, agencies also monitor people who would be released anyway.[54] The surveillance net of electronic monitoring thus widens in many directions.

III. SMARTPHONES AND THE LEVELING UP OF ELECTRONIC MONITORING

Smartphones are changing what electronic monitoring means. As explored in Part II, electronic monitoring was previously limited by the capabilities of the technology itself. Though ankle monitor capabilities have grown over time (from RFID to GPS),[55] they are still limited by the available technology. The same cannot be said for smartphone monitoring. As Chief Justice John Roberts remarked in *Riley v. California*, cell phones are "now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[56] Shifting electronic monitoring to a device that is part and parcel with American society tells of a future of relentless, unbounded surveillance.[57] This Part details the reasons for

---

year, only 2 percent of gun defendants had been placed on monitoring.)"). Further, in Los Angeles County, California, pretrial electronic monitoring increased 5,250% between 2015 and 2021 (from 24 people to 1,284 people). ALICIA VIRANI, UCLA SCH. L. CRIM. JUST. PROGRAM, PRETRIAL ELECTRONIC MONITORING IN LOS ANGELES COUNTY 2015–2021 (2022), https://law.ucla.edu/sites/default/files/PDFs/Criminal_Justice_Program/Electronic_Monitoring_in_Los_Angeles_Report-FINAL.pdf [https://perma.cc/8X8K-KJTH].

51. Nellis, *supra* note 3, at 32; *see also* Owens et al., *supra* note 12, at 4077 ("[Electronic monitoring] has typically been administered to people deemed 'high risk,' but prison industry companies are marketing their apps as a low-cost and efficient way to expand the scope of surveillance to include 'low risk' people as well.").

52. *See* SCHENWAR & LAW, *supra* note 8, at 31. Further, "in jurisdictions that have recently reduced their jail populations — often in response to local organizing — house arrest with electronic monitoring has become a substitute for jail." *Id.* at 27.

53. Weisburd, *Punitive Surveillance*, *supra* note 12, at 151.

54. *See id.*

55. *See supra* Section II.A.

56. Riley v. California, 573 U.S. 373, 385 (2014).

57. *Mobile Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile [https://perma.cc/7U2N-YPU4] ("The vast majority of Americans —

shifting to smartphones, the types of devices used, and the devices' technological capabilities. Then, it summarizes how smartphones are used for supervision and outlines relevant concerns.

A. Reasons for Shifting to Smartphones

For agencies, smartphone monitoring provides an appealing, if not irresistible, alternative to traditional incarceration.[58] According to an industry report with self-reported data from eleven smartphone monitoring companies, there are two major forces behind the move toward smartphones in electronic monitoring: (1) the ubiquity of smartphones and (2) the capability of the technology.[59] In other words, companies see smartphone monitoring as a growth opportunity — they are tracking via smartphone because everyone has one and because they can.

B. Types of Devices

Smartphone monitoring takes two forms: "bring your own device" ("BYOD") and "corporate-owned" device programs.[60] First, BYOD requires people to install tracking software onto their personal phones.[61] As a 2020 report from the American Probation and Parole Association ("APPA") explained, BYOD is less expensive for the agencies (not the person who must purchase a phone and pay fees to be tracked) but may involve more security concerns.[62] Second, corporate-owned device programs involve a "locked-down, customized smartphone available for purchase or lease from the vendor."[63] Corporate-owned devices are costlier for the state.[64] But these devices are considered more secure because they are "capable of monitoring *all* phone activity and

97% — now own a cellphone of some kind. The share of Americans that own a smartphone is now 85%, up from just 35% in Pew Research Center's first survey of smartphone ownership conducted in 2011.").

58. Russo & Drake, *supra* note 43, at 5 ("Agencies often look to technology to help them do more with less and many are now exploring smartphone applications as a way of providing cost-effective supervision services to large groups of offenders.").

59. *Id.*

60. *Id.* at 7–8.

61. *Id.*

62. *Id.* at 8. The security concerns include basic phone attributes such as power buttons, access to SIM cards and batteries, Wi-Fi settings, airplane mode, and the ability to install or delete apps because these features allow those being tracked to do things like turn off their phones. AM. PROB. & PAROLE ASS'N, LEVERAGING THE POWER OF SMARTPHONE APPLICATIONS TO ENHANCE COMMUNITY SUPERVISION 4 (2020), https://www.appa-net.org/eweb/docs/APPA/stances/ip-LPSAECS.pdf [https://perma.cc/JJ6J-44RV].

63. Russo & Drake, *supra* note 43, at 8.

64. *Id.*

restricting the individual's access to particular functionality as determined by the officer."[65]

C. Types of Tracking Technology

Verifying the identity and location of justice-involved individuals at all times is one of electronic monitoring's primary purposes. There are three ways to verify identity and location: "periodic confirmation, continuous confirmation, and a hybrid approach."[66] Periodic confirmation "typically employs some type of automated biometric (e.g., fingerprint, voice verification, facial recognition)"[67] and/or "credential/password to validate identity at points where key information (e.g., location) is collected."[68] Conversely, continuous confirmation "generally employs a secure, body-worn tether linked via radio frequency, with the smartphone," and "an alert may be generated if the two devices are separated or if the tether is removed."[69] Finally, hybrid "offers multiple layers of confirmation, for example, a tether combined with a biometric validation to operate the smartphone."[70] Identity and location verification, as measured by proximity to the device, can occur continuously (via a Bluetooth tether), up to five times per hour (via ID/password or facial recognition), or as defined by the officer (via methods including fingerprint, photo comparison, and facial recognition).[71]

D. Supervision Uses

Smartphones fundamentally change electronic monitoring by expanding surveillance and reducing the human element of rehabilitation. As industry insiders explained:

> As smartphone technology is continuously advancing, agencies can leverage these developments into the future in *ways that traditional electronic monitoring devices simply can't support*. With the rapid

65. AM. PROB. & PAROLE ASS'N, *supra* note 62, at 4 (emphasis added). These devices allow probation officers to restrict or limit Internet access, limit ability to call or text certain individuals, and restrict activity based on schedule. *Id.* For example, BI Inc.'s privacy policy for its SmartLINK app says it can collect data, including "responses to notifications, in-App search history, web browsing, phone calls, video conferencing, and other actions conducted and information entered within the App." *BI SmartLINK Privacy Policy*, BI INC. (Mar. 18, 2022), https://www.bi.com/bi-smartlink-privacy [https://perma.cc/3NEG-EM3G].

66. Russo & Drake, *supra* note 43, at 28.

67. *Id.*

68. AM. PROB. & PAROLE ASS'N, *supra* note 62, at 4.

69. *Id.* at 5.

70. *Id.*

71. Russo & Drake, *supra* note 43, at 8 tbl.2.

> development of applications and integrated and compatible sensors, the capabilities of smartphones are constantly evolving. These advances promise *flexibility and expandability* that community corrections [have] not yet experienced with any other tool, and it is anticipated that smartphones will play a very prominent role in community supervision moving forward.[72]

Monitoring companies understand this new technology's value and business expansion potential.

Understanding supervision basics contextualizes how the technology is used. Smartphone monitoring can: block certain websites,[73] limit calls or texts,[74] record audio or make calls,[75] deny device access during school hours,[76] monitor location,[77] continuously track via radio or Bluetooth tether,[78] and periodically sample location.[79] Supervised people can be required to enable all permissions for the app to work, including many that Android labels "dangerous," such as "fine" location tracking (which can be accurate within ten feet), activity recognition ("which reports if someone is in a vehicle, on a bicycle, running, or still"), and phone state (which could "monitor whom someone talks to and how frequently they speak").[80] While purportedly geared toward rehabilitation, these features are often used paternalistically: to control those who cannot be trusted to make good choices.

Smartphone monitoring also enables hands-off rehabilitation by allowing probation officers to conduct remote supervision.[81] Remote features include: "mobile wallets" (which allow those on monitoring to pay for the tracking service directly) and submission of medical records, employment records or paystub info, information about living arrangements, and contact information.[82] Some apps even allow "simultaneous mass-messaging" from officers to all clients, saving

---

72. *Id.* at 5 (emphasis added).
73. AM. PROB. & PAROLE ASS'N, *supra* note 62, at 10.
74. *Id.*
75. Giulia McDonnell Nieto del Rio, *Meet SmartLINK, the App Tracking Nearly a Quarter Million Immigrants*, MARKUP (June 27, 2022, 7:00 PM), https://www.themarkup.org/thebreakdown/2022/06/27/meet-smartlink-the-app-tracking-nearly-a-quarter-million-immigrants [https://perma.cc/3UZM-2L7M] ("SmartLINK's permissions are not limited to accessing the device's camera and location to carry out check-ins, but rather the application also requests permissions to record audio and make calls without requiring user permission.").
76. AM. PROB. & PAROLE ASS'N, *supra* note 62, at 10.
77. *Id.* at 5.
78. Russo & Drake, *supra* note 43, at 33.
79. *Id.*
80. Owens et al., *supra* note 12, at 4081.
81. Russo & Drake, *supra* note 43, at 29–30.
82. *Id.* at 29–31, 33.

officers time.[83] Utilizing the phone's camera, officers can conduct face-to-face interviews and walk through clients' homes, including inspecting drawers, cabinets, and refrigerators.[84] These features are all presented as increasing officers' efficiency and helping those being tracked to meet the requirements of their community supervision.

Additionally, officers can manage the calendars of those on monitoring by sending or automating reminders for court appearances, drug tests, and other programming.[85] People can add events to their calendars to request movement from their officers, without even having to speak to them.[86] Once movement is approved, the calendar can then be used to automatically create a geofence restricting someone to the approved time and place.[87] Finally, location monitoring can be used with automated reminders to send messages when someone makes curfew, arrives to work on time, or receives a negative drug test.[88]

E. Problems

These smartphones, however, do not always work as desired or expected. Technical problems can cause major issues, the most severe of which would be a technical violation that could lead to reincarceration.[89] Issues can arise regarding cellular provider coverage area (which is unpredictable with BYOD), minutes or data exhaustion (since the person is generally paying for this themselves), and battery life (usually due to continuous location tracking).[90] Specifically, one analysis of sixteen electronic monitoring apps revealed "widespread lack of functionality" and disruptiveness.[91] Problems included an inability to check in,

83. *SCRAM TouchPoint: Electronic Monitoring Mobile App*, SCRAM SYS. (2021), https://www.scramsystems.com/monitoring/scram-touchpoint [https://perma.cc/8BX8-QAMP].

84. Russo & Drake, *supra* note 43, at 28. BI's SmartLINK app collects images taken for weekly check-ins, as well as the latitude and longitude of where each photo was taken and stores this data for an unknown period. *See* Johana Bhuiyan, *A US Surveillance Program Tracks Nearly 200,000 Immigrants. What Happens to Their Data?*, GUARDIAN (Mar. 14, 2022, 6:05 AM), https://www.theguardian.com/us-news/2022/mar/14/us-immigration-surveillance-isap [https://perma.cc/4BYM-WLNN].

85. Russo & Drake, *supra* note 43, at 33. There is even an Application Programming Interface ("API") that allows for drug tests to be automatically scheduled and added to the person's calendar in line with the jurisdictional requirements. *Id.* at 30; *see also* AM. PROB. & PAROLE ASS'N, *supra* note 62, at 6–7.

86. Russo & Drake, *supra* note 43, at 35.

87. *Id.* at 36.

88. *Id.* at 30.

89. *See* WEISBURD ET AL., ELECTRONIC PRISONS, *supra* note 17, at 3 ("The number and nature of monitoring rules, combined with the capacity of surveillance technology, facilitates easier detection of technical rule violations, which in turn drives reincarceration."). With BI's SmartLINK app, glitches are not uncommon; one former employee said "[t]he technology was not good," describing several of the app's recurrent glitches. McDonnell Nieto del Rio, *supra* note 75.

90. *See* AM. PROB. & PAROLE ASS'N, *supra* note 62, at 9.

91. Owens et al., *supra* note 12, at 4084.

loud alerts that could not be silenced in social settings like work or church, and app-caused phone crashes that "potentially jeopardiz[e] an [electronic monitoring] condition that their phone is always running."[92]

IV. LIMITING THE UNLIMITED: WHY CHANGE NOW

Because the technology enabling electronic monitoring is no longer inherently limited, the law needs to set boundaries. There are five main concerns regarding the limitless tracking that smartphones facilitate: (1) expansion of electronic monitoring, which is furthered by smartphones, particularly through device normalization; (2) privacy intrusions for monitored persons, the communities they live in, and society as a whole; (3) nearly infinite data collection and its haphazard management, use, storage, and security; (4) increased role of private companies, which are not as accountable as government entities; and (5) depersonalization of a purportedly rehabilitative system. This Part tackles each in turn.

A. Electronic Monitoring Expansion Through Smartphone Normalization

The same factors driving electronic monitoring expansion are driving smartphone monitoring expansion.[93] But smartphone monitoring is additionally justified: the smartphone market is larger (everyone has one) and these devices are normalized (again, everyone has one). Because smartphones are easily accessible and socially acceptable, agencies can justify smartphone monitoring for lower-risk offenders post-release and for those who would not have been supervised pretrial with an ankle monitor.[94] Accordingly, the market expands in two directions, encapsulating lower-risk offenders and justice-involved individuals at any stage.

The net-widening is not incidental; it is a business opportunity. As one industry report explained: "The power of this multifaceted technology combined with its *prevalence* within our society has made smartphone applications a very attractive tool, one without the *stigma* associated with more traditional devices."[95] Prevalence and stigma are interrelated. Law enforcement agencies know ankle monitors are

92. *Id.* at 4078.

93. *See supra* Part II.

94. Nellis, *supra* note 3, at 45 ("Smartphones are increasingly being pitched as a highly versatile *and still relational* monitoring technology for lower-risk offenders, a potentially vast market in comparison to the smaller market of medium- to high-risk offenders on whom [RFID] and GPS monitoring has been targeted.").

95. Russo & Drake, *supra* note 43, at 5 (emphasis added).

stigmatized[96] while smartphones are normalized because nearly everyone has them. This awareness creates a preference for smartphone monitoring as the lesser evil. Since most Americans already own smartphones, agencies do not have to purchase expensive new equipment to monitor them.[97] And while ankle monitors have always been limited technologically, smartphones have advanced capabilities which — given the ubiquity of smartphones and the tremendous resources devoted to their technological development — will continue evolving rapidly.[98]

Lastly, smartphone monitoring expansion normalizes the idea that the justice-involved should be tracked. As Nellis explains, "[t]he ideal of mobile, networked, real-time connectivity . . . [normalizes] the idea that a person's location must be known and could be tracked."[99] Without much questioning, agencies use smartphone monitoring because they can.

B. Collateral Surveillance and Collective Privacy

The increase in smartphone monitoring also subjects community and family members of those being monitored to collateral surveillance and impacts society's collective privacy. Ankle monitors began collateral surveillance, as family members who lived in the same home were often subject to the same searches as those wearing monitors.[100] Smartphones expand collateral surveillance through the comprehensive breadth of monitoring.[101] Although voice recorders on ankle monitors could overhear conversations and intrude on the privacy of people nearby,[102] today's message monitoring and overall phone tracking capabilities surveil an even wider net. Anyone who texts, calls, or interacts via phone with a person who has a monitoring app installed is

96. *Id.* at 33 (explaining that smartphones offer "much of the functionality of traditional offender-tracking systems . . . without the stigmatization that can occur with bulky ankle bracelets").

97. *Id.* at 6, 8 (noting that when "the application is installed on the offender's personal, commercial smartphone," it "generally is less expensive" for the agency).

98. *See supra* Section III.D.

99. Nellis, *supra* note 3, at 35.

100. WEISBURD ET AL., ELECTRONIC PRISONS, *supra* note 17, at 12 ("In about 40% of jurisdictions in the study, people on monitors are subject to searches at any time without reasonable suspicion or probable cause, subjecting people who live with them to searches as well.").

101. One monitoring company even boasts a patent for "System and Method for Tracking Interaction Between Monitored population and Unmonitored Population," implying intentional collateral surveillance. *Patents*, SECURUS MONITORING (2022), https://www.securusmonitoring.com/about-us/patents [https://perma.cc/Q9N5-QCPR].

102. For a discussion on surveillance and consent, see Lerner, *supra* note 37 ("[A] young person or an adult has consented to be on a monitor in lieu of being in prison or jail. The problem with that is that consent can't just be a blanket, carte blanche excuse for any type of privacy invasion.").

collaterally surveilled — anything they say could be stored in a database (and used later for a police investigation).[103] Moreover, because video calls are used for check-ins and identification, anyone in the same house could potentially be monitored if they walked into the camera frame, as could strangers if the call took place in public.

As privacy scholars Daniel Solove and Danielle Keats Citron have noted: Privacy is a collective right, the violation of which affects individuals as a group and not just personally.[104] Given these technologies are being used with minimal oversight,[105] the breadth of the privacy violations — for those under direct surveillance as well as those being collaterally surveilled — is unknowable. As limitless surveillance of a subset of the population becomes normalized, so does the idea of limitless surveillance generally. And because privacy is a collective good, when anyone's privacy is violated, everyone's privacy is violated.

C. Individual Privacy and the Collection, Management, and Storage of "Endless" Data

Given the lack of oversight or regulation, the massive amount of monitoring data — some centralized within single private companies but largely distributed across individual jurisdictions — is troubling. The APPA report summarizes why smartphone monitoring data is problematic: "Since smartphones are effectively mobile computers with immense processing power and ever-smaller sensors, the amount of data that can be collected is almost endless."[106] The report recommends agencies consider data management practices, but there is little evidence any agencies are doing so since much discretion is left to vendors.[107] There is also little guidance about how this data should be used or maintained.[108] Few agencies inform people that their data is saved or could be shared with law enforcement for purposes other than

---

103. *See* McDonnell Nieto del Rio, *supra* note 75 ("Several SmartLINK users said they go so far as to limit contact with relatives and friends on their devices, especially with those who are undocumented, for fear that ICE could intercept their communications.").

104. Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 816 (2022) ("From the standpoint of each individual, the harm is minor, but from the standpoint of society, where the harm to everyone is aggregated, the total amount of harm is quite substantial.").

105. *See* WEISBURD ET AL., ELECTRONIC PRISONS, *supra* note 17, at 27 (explaining how the electronic monitoring contracts reviewed did not mention oversight or quality control); *see also* Hannah Bloch-Wehba, *Visible Policing: Technology, Transparency, and Democratic Control*, 109 CALIF. L. REV. 917, 921 (2021) ("Sophisticated policing technologies . . . are often implemented without robust oversight or public awareness.").

106. AM. PROB. & PAROLE ASS'N, *supra* note 62, at 9.

107. WEISBURD ET AL., ELECTRONIC PRISONS, *supra* note 17, at 2 ("Agencies in every state contract with private companies to track, analyze and store location, activity and movement data. . . . The majority of records in our study were silent as to privacy protections or rules governing the use of the data.").

108. *Id.*

community supervision monitoring, such as crime scene correlations and active police investigations.[109] And some apps sell data to advertisers like Google and Meta, allowing vendors to further monetize the app.[110]

Privacy protections include how data is stored and managed, not just how it is used. As APPA warns, "agencies should be cognizant of how smartphone applications, particularly those installed on the client's personal device, may impact the client's right to privacy."[111] Agencies generally do not inform anyone how long their data will be stored (vendors can store it for a fixed term, return it to the agency, or destroy it).[112] Six agency records from five states specifically require people to submit their devices for warrantless searches.[113] And, though many vendors store data with third-party cloud storage providers, there are no universal secure storage guidelines.[114] The design of the apps themselves also can violate privacy: some apps include Facebook trackers that allow the app to access the person's profile and inform Facebook that the person is using an electronic monitoring app.[115] Additionally, several apps connect to the Internet in a way that clearly identifies the electronic monitoring vendor.[116] Thus, Internet Service Providers and others using the same Wi-Fi could also discover someone's monitoring status.[117]

Lastly, widespread collection and storage of potentially mismanaged data impacts people's fundamental rights. Constant monitoring, whether or not one has been convicted, substantially impacts how freely

---

109. *Id.* at 10. For example, the D.C. Metropolitan Police Department shares location data from its VeriTracks GPS tracking software with D.C.'s Homeland Security Emergency Management Agency. Chris Gelardi, *Inside D.C. Police's Sprawling Network of Surveillance*, INTERCEPT (June 18, 2022, 6:44 AM), https://www.theintercept.com/2022/06/18/dc-police-surveillance-network-protests [https://perma.cc/W6UW-3SRY]; *see also* VERITRACKS, VERITRACKS CRIME INCIDENT DATA EXTRACT SPECIFICATION, https://s3.documentcloud.org/documents/22056325/attachement-veritracks-crime-incident-data-v2.pdf [https://perma.cc/BMZ6-RB4L] ("If a tracked person is identified to be near a crime incident at the approximate time of the incident, a 'hit' occurs, and the proper officials are notified by e-mail.").

110. Owens et al., *supra* note 12, at 4082. A review of app privacy policies showed that "five of the policies said explicitly that they do not sell one's data. Seven of the policies mention that data will be used for marketing, sometimes for marketing the company's own product and advertisements." *Id.* at 4086.

111. AM. PROB. & PAROLE ASS'N, *supra* note 62, at 10.

112. *See* WEISBURD ET AL., ELECTRONIC PRISONS, *supra* note 17, at 11 (summarizing general practices used by private tracking companies).

113. *Id.* The cited report, for instance, provides examples from Colorado, Kansas, West Virginia, and Wisconsin. *Id.* at 40 n.89.

114. Russo & Drake, *supra* note 43, at 35 tbl.6 (detailing how most companies use some form of unspecified secure cloud service, while others rely on companies such as Amazon, Google, and Microsoft for cloud storage services).

115. Owens et al., *supra* note 12, at 4082. One app "contacted Facebook once every five minutes." *Id.* at 4083.

116. *Id.* at 4083.

117. *Id.* ("This information could allow passive observers — e.g., coffee shops, airports, schools, employers, Airbnb hosts — to know if someone is under EM.").

people feel to speak or simply exist as citizens.[118] As Professor Chaz Arnett has argued, electronic monitoring maintains the social stratification that incarceration creates by separating those being monitored from their social networks and rehabilitative services, and straining their "privacy, liberty, and democratic participation."[119]

D. Private Companies' Increased Role in Electronic Monitoring

Private companies' role in supervising and developing electronic monitoring technologies is important, concerning, and growing concurrently with increased smartphone use. Because law enforcement agencies do not usually have the resources to develop proprietary monitoring technology, they must rely on third-party vendors to do so.[120] Agencies typically have no choice but to work with a vendor, giving the vendors a powerful bargaining position and remarkable control over both the surveillance mechanisms and the data collected.

Often, jurisdictions contract with various private companies that develop the technology, manage the monitoring, and then share the data with agencies.[121] How each jurisdiction supervises people on electronic monitoring varies by city, county, and state.[122] At least one major electronic monitoring company, BI Incorporated, is owned by one of the largest private prison companies, GEO Group.[123] Private companies view electronic monitoring as the next market opportunity in the prison industry and have invested in its development[124] because "private

---

118. Weisburd, *Punitive Surveillance*, *supra* note 12, at 147 (arguing that electronic monitoring is a form of punishment and that "[w]ith virtually no legal oversight or restraint, punitive surveillance deprives people of fundamental rights, including privacy, speech, and liberty").

119. Chaz Arnett, *From Decarceration to E-Carceration*, 41 CARDOZO L. REV. 641, 642 (2019).

120. Though a comparison to private prisons might seem apt here, it is not. "While there are many state-operated and -run prisons . . . there are no state- or government-run surveillance companies. The only way a government agency can engage in monitoring and surveillance is by contracting with a private company." WEISBURD ET AL., ELECTRONIC PRISONS, *supra* note 17, at 22; *see also* Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 19, 20 (2017).

121. *See* WEISBURD ET AL., ELECTRONIC PRISONS, *supra* note 17, at 10 ("Contracts from 22 states provide that private companies track the movements of people on electronic monitoring devices and maintain a database of that location data.").

122. *See id.* (explaining the variation between state, city, and county approaches to electronic monitoring).

123. *See Job Seekers*, BI INC. (2022), https://bi.com/careers [https://perma.cc/UXY7-HHWJ] ("BI Incorporated, a GEO Group Company . . . is the largest provider of GPS, alcohol, and RF technology and services in the United States."); Renae Merle & Tracy Jan, *Wall Street Pulled Its Financing. Stocks Have Plummeted. But Private Prisons Still Thrive*, WASH. POST (Oct. 3, 2019, 3:37 PM), https://www.washingtonpost.com/business/2019/10/03/wall-street-pulled-its-financing-stocks-have-plummeted-private-prisons-still-thrive [https://perma.cc/KC2D-WRCR] (describing GEO Group as a "private prison giant[]").

124. *See* Nellis, *supra* note 3, at 34 (citations omitted) ("Initially, the industry comprised companies with interests in private prisons, security, communications, outsourcing state

companies increase their profits as more people are placed, remain and re-placed on monitors."[125]

These vendors also wield immense power over electronic monitoring operations. They often serve as gatekeepers between the data and software and the law enforcement or probation offices.[126] Sometimes vendors receive first reports of violations before sending them to the supervising agency.[127] While local agencies sign the contracts and partially manage people on electronic monitoring, private companies play a significant role.

This trend is concerning because, as Professor Elizabeth Joh has argued, private surveillance technology companies have undue influence over policing in ways that have "enormous consequences for civil liberties and police oversight."[128] As she notes, "[w]hen private companies influence policing through their role as vendors, [] the usual mechanisms of oversight do not easily apply; they have little obligation to permit public access, and the usual constitutional constraints over the police do not regulate them at all."[129] As private companies gain more control over the industry, accountability and insight into their practices is restricted.[130] Unlike governmental agencies, private companies are not accountable to the public. If private companies serve as the primary developers, managers, and supervisors of this monitoring technology, there is tension between accountability for justice and accountability for profits.[131]

---

functions and purpose-designed [electronic monitoring] businesses, all of whom believed that growing international concern about the costs (and, sometimes, inhumanity) of 'prison overcrowding' would fuel a lucrative new market in offender monitoring.").

125. WEISBURD ET AL., ELECTRONIC PRISONS, *supra* note 17, at 27 ("Several of the companies that market monitors have been the subject of civil rights lawsuits and should not be relied on.").

126. *Id.* at 21–22 ("In many jurisdictions, private vendors play a large role, including supervising people and overseeing and approving schedule changes.").

127. *Id.* at 10 ("The private companies then share the monitoring data with the state and local agencies that oversee electronic monitoring."). Case managers at BI Incorporated can be responsible for up to 300 monitored people, meaning there is likely not enough time to offer tailored support. *See* Johana Bhuiyan, *Poor Tech, Opaque Rules, Exhausted Staff: Inside the Private Company Surveilling US Immigrants*, GUARDIAN (Mar. 7, 2022, 7:48 PM), https://www.theguardian.com/us-news/2022/mar/07/us-immigration-surveillance-ice-bi-isap [https://perma.cc/8MZV-AGFE].

128. Joh, *supra* note 120, at 20 ("That police rely on private vendors is unremarkable as a general proposition.").

129. *Id.* at 21.

130. *See id.* at 20; *see also* WEISBURD ET AL., ELECTRONIC PRISONS, *supra* note 17, at 22 (explaining that "because private companies are not governed by public record laws, it is virtually impossible to determine how these companies function"); Bloch-Wehba, *supra* note 105, at 954 ("The informational dynamics of modern policing technologies grow even more complex when private sector vendors are involved. . . . [S]urveillance and other new policing programs are often initiated without any kind of public input.").

131. *See* Joh, *supra* note 120, at 20 ("Through different mechanisms intended to promote their own interests and profits, these companies exert control over the police long after their products have been adopted.").

E. Depersonalization and In-Person Contact Elimination

Smartphone monitoring depersonalizes rehabilitation and reduces vital in-person contact.[132] These technologies are advertised as facilitating officer caseload management, and some advertisements even emphasize the reduced need for in-person contact or actual conversations.[133] Some capabilities — such as a digital calendar that allows monitored persons to request movement by simply scheduling an event — further diminish any in-person contact someone might otherwise have with their supervising officer.[134]

Moreover, constant oversight by probation officers has led some scholars to deem traditional electronic monitoring "punitive."[135] But allowing probation officers to disconnect totally from their clients forebodes a stratified world where people are monitored by computers with little human connection. Being electronically monitored already has many of the same social stratification consequences as incarceration.[136] As Arnett explains, "current forms of electronic correctional surveillance . . . contribute to social marginalization."[137] Reduced in-person contact, depersonalization, and interactions made solely through software lack the personal connections crucial to rehabilitation.

V. A FRAMEWORK FOR ELECTRONIC MONITORING PRIVACY PROTECTION

This Note recommends incorporating basic privacy principles into electronic monitoring to reduce the harms exacerbated by smartphone monitoring. The FIPPs could help protect the rights of citizens on electronic monitoring because they incorporate individual rights and

---

132. Professor Chaz Arnett explains that e-carceration methods (electronic monitoring in all forms) can have significant social impacts on monitored persons by diminishing "community bonds and ties critical for successful reentry." Arnett, *supra* note 119, at 712.

133. One company highlights the fact that its app enables mobile check-ins and monitoring and allows officers to use text-to-all for simultaneous mass-messaging. *See* SCRAM SYS., *supra* note 83.

134. *See* AM. PROB. & PAROLE ASS'N, *supra* note 62, at 6–7; Russo & Drake, *supra* note 43, at 36.

135. *See* Weisburd, *Sentenced to Surveillance*, *supra* note 9, at 757 (footnote omitted) ("Because supervisees know they are being potentially searched at all times, electronic surveillance — more than physical surveillance — 'shapes and restricts behavior.'" (quoting Scott Skinner-Thompson, *Performative Privacy*, 50 U.C. DAVIS L. REV. 1673, 1694 (2017))); *see also* Weisburd, *Punitive Surveillance*, *supra* note 12, at 151 ("In practice, punitive surveillance is often part of a criminal punishment, imposed on top of probation, parole or supervised release.").

136. *See generally* Arnett, *supra* note 119 (explaining how electronic monitoring, or "e-carceration," contributes to social marginalization in myriad ways); WEISBURD ET AL., ELECTRONIC PRISONS, *supra* note 17, at 12 ("People on electronic monitors are frequently subject to a range of rules and requirements that undermine family and social relationships.").

137. Arnett, *supra* note 119, at 645.

obligations for entities that collect and use data.[138] These principles are widely used by various governmental agencies, both in Europe and the United States.[139] Given the dearth of guidelines for electronic monitoring data privacy,[140] the long legacy and widespread use of the FIPPs make them a good initial framework.

The FIPPs contain eight basic principles: (1) collection limitation, (2) data quality, (3) purpose specification, (4) use limitation, (5) security safeguards, (6) openness, (7) individual participation, and (8) accountability.[141] The FIPPs are "interrelated and partly overlapping" and should be "treated together and studied as a whole."[142] This Part examines each principle within the smartphone monitoring context to provide a framework around which law enforcement and probation agencies, the judiciary, and the legislature may set limits. Comprehensive protections for electronic monitoring require a multifaceted, holistic approach.

A. Collection Limitation

Collection limitation describes the principle that "[t]here should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."[143] This principle has two prongs: limiting what data is collected and how it is collected.[144] Common collection limitation concerns include data quality, data processing purposes, earmarking especially sensitive data, limits for certain data controllers, and civil rights.[145]

In smartphone monitoring, much of the data — like drug test results, criminal records, and medical records — is especially sensitive because it relates to extremely private elements of a person's life. The entire electronic monitoring system also raises civil rights concerns because unlimited data collection, especially in the criminal justice context, can limit a person's willingness to speak or assemble.[146]

In applying this principle, agencies should consider ways to limit data collection only to what is needed.[147] First, agencies can determine

---

138. *See* Saniuk-Heinig, *supra* note 15.

139. *Id.*

140. WEISBURD ET AL., ELECTRONIC PRISONS, *supra* note 17, at 2 ("The majority of records in our study were silent as to privacy protections or rules governing the use of the data.").

141. OECD, *supra* note 14, at 14–15.

142. *Id.* at 55.

143. *Id.* at 14.

144. *Id.* at 55.

145. *See id.* at 55–56.

146. *See* WEISBURD ET AL., ELECTRONIC PRISONS, *supra* note 17, at 27.

147. OECD, *supra* note 14, at 55. This principle "represents an affirmative recommendation to lawmakers to decide on limits which would put an end to the indiscriminate collection of personal data." *Id.*

what data they actually need to reach their stated goals before monitoring anyone. Second, judges can limit what types of data are collected when writing sentencing orders. Third, the legislature can pass privacy laws to limit the indiscriminate collection of personal data from monitored persons.

B. Data Quality

Data quality is the principle that "[p]ersonal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date."[148] This principle's first prong notes that data is only high quality if it is relevant to its purpose.[149] In electronic monitoring, that could mean defining quality data as relevant to community safety, reducing recidivism, or any stated agency purpose related to community supervision. Further, given the issues that some smartphone monitoring apps have, data quality standards could require agencies to ensure that collected data is accurate, complete, and up-to-date. Judges can also assess the quality and relevance of any monitoring data used in hearings or subsequent investigations. Finally, legislatures can set data quality standards and require agencies to meet those standards.

C. Purpose Specification

Purpose specification is the principle that the purpose of data collection should be specified before any data is collected and that subsequent use of said data should be limited to that specified purpose (or at least uses not incompatible with the stated purpose).[150] Any change in purpose should also be specified, compatible with the original purpose, and not arbitrary.[151] The OECD provides many examples of ways in which data purpose can be specified, including "public declarations, information to data subjects, legislation, administrative decrees, and [supervisory body] licences."[152] Once data no longer serves the specified purpose, it may be necessary to delete or anonymize it, lest the data not be maintained properly, which could create risks of theft or unauthorized use.[153]

At least some data collection through smartphone monitoring is justifiable. Agencies can specify the data collection purpose before monitoring begins. Then, they can make that purpose known, at

148. *Id.* at 14.
149. *See id.* at 56.
150. *Id.* at 14.
151. *Id.* at 56–57.
152. *Id.* at 57.
153. *Id.*

minimum, to the person being monitored, and possibly to the public. There is also a clear role for the legislature to create standards for purpose specification that apply to all agencies in any respective jurisdiction. Lastly, judges should require the use of collected data in subsequent police investigations to be clearly stated and made known to any monitored individual, just as subpoenas and warrants would typically be served and made public.

D. Use Limitation

The use limitation principle is intimately related to the purpose specification principle. It states that purpose specification should not be violated "except: a) with the consent of the data subject; or b) by the authority of law."[154] This principle is particularly important given private companies' outsized role in supervising electronic monitoring, developing smartphone apps, and storing associated data.

The number of entities that can access the data should be limited to those for whom access is necessary, as aligned with the specified purpose.[155] There should be limits on how private companies can use, store, transmit, or sell this data — especially in light of how personal and comprehensive much of it can be. Agencies should be sure to evaluate vendor contracts thoroughly and include terms that limit how monitoring data may be used or disclosed, such as forbidding sales to data brokers. Legislatures could also set use limitations by statute. This principle includes exceptions for use limitation based on consent, which implies there could be a mechanism for those on electronic monitoring to consent to how their data is used. This consent to data use could provide another layer of control.

E. Security Safeguards

The security safeguards principle states that "[p]ersonal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data."[156] Note that security is not the same as privacy; security reinforces privacy.[157] Security safeguards can include physical measures (e.g., locked doors), organizational measures (e.g., hierarchical access), and informational measures (e.g., threat monitoring).[158]

---

154. *Id.* at 14.
155. *See id.* at 57.
156. OECD, *supra* note 14, at 15.
157. *See id.* at 57.
158. *Id.*

This principle also requires that data processing personnel maintain confidentiality.[159]

Because of the ways in which smartphone monitoring apps work,[160] there are many potential entry points for clients, agencies, and vendors. Requiring vendors to ensure proper physical safeguards in storing data is crucial, even though they often work with third-party cloud providers. Other precautions could include requiring agencies and officers to comply with security practices, such as appropriate password management for their devices and accounts, two-factor authentication, and physical device security. Agencies should also be sure to create "access hierarchies,"[161] so that only people who need access to an individual's monitoring data have that access. Additionally, vendors should be held to the same standard and be required to ensure internally that no one can access personal data without proper authority. Agencies should constantly evaluate the contracts and relationships they have with vendors to ensure confidentiality is maintained. Judges can also require confidentiality safeguards during sentencing or prohibit the admission of evidence obtained in contravention of this principle.

F. Openness

The openness principle relies on the idea that "[t]here should be a general policy of openness about developments, practices, and policies with respect to personal data."[162] This principle states that "[m]eans should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller."[163] "Readily available" means the information can be obtained "without unreasonable effort as to time, advance knowledge, travelling, and so forth, and without unreasonable cost."[164] The openness principle is in part a transparency

159. *Id.*

160. Smartphone monitoring apps have many potential security weaknesses because they are managed by both vendors and agencies and are used by clients. The more people who have access to the app's data, the higher the risk that the data will be left unsecure. This informational security depends on vendors and agencies. Clients are in charge of the physical security of the device, but physical security can also be compromised or affected by those who can access background computers from which the data is accessible. *Cf.* Teju Shyamsundar, *Today's Mobile Security Threats: What Are They and How Can You Prevent Them?*, OKTA: BLOG (Oct. 22, 2020) https://www.okta.com/blog/2020/10/mobile-security-threats-and-prevention [https://perma.cc/ES9F-WK9U] (discussing mobile security threats generally).

161. "Access hierarchies" are systems involving multiple tiers of permissions based on the needs of each person who has access to data. Thus, only some data would be available to the lowest position on the hierarchy, whereas moving up the hierarchy would provide increased access to data.

162. OECD, *supra* note 14, at 15.

163. *Id.*

164. *Id.* at 58.

principle and in part a requisite for the following individual participation principle; individual participation is not possible unless people know the data exists.

Agencies must increase transparency about smartphone monitoring use and the breadth of data collected. Individuals should be able to ascertain what data has been collected from them. Emphasizing transparency and openness would be a large change for many agencies and vendors[165] and would contribute to building trust with local communities. If data is being collected for specified reasons, stored only for the time needed, and is accessible by monitored persons, then communities may value agencies' open communication. Here, judges and legislatures can also ensure, through rulings and statutes, that individuals can access their data.

G. Individual Participation

The individual participation principle suggests that monitored individuals have a right to access their personal data.[166] This right should be simple to exercise: People should be able to access their own data without legal process, though in some cases (such as for medical data), it may be appropriate to have an intermediary.[167] Data related to the criminal justice system likely also requires an intermediary because of the sensitive nature of the data and its relation to public safety and law enforcement goals.

Agencies can provide mechanisms by which the reasonable timeframe is actually reasonable.[168] Access can occur at regular

---

165. As Professor Hannah Bloch-Wehba explains in *Visible Policing*, "[l]aw enforcement has an opacity problem." Bloch-Wehba, *supra* note 105, at 919 ("[N]ew surveillance technology tends to operate in opaque and unaccountable ways, augmenting police power while remaining free from meaningful oversight . . . [and] shifts in Fourth Amendment doctrine have expanded law enforcement's ability to engage in surveillance without oversight or scrutiny by courts or the public.").

166. *See* OECD, *supra* note 14, at 58. As the OECD Privacy Framework explains in detail:

> Individuals should have the right:
> a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;
> b) to have communicated to them, data relating to them
> i. within a reasonable time;
> ii. at a charge, if any, that is not excessive;
> iii. in a reasonable manner; and
> iv. in a form that is readily intelligible to them;
> c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
> d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

Id. at 15.

167. *See id.* at 58.

168. *Id.*

intervals or shortly after an individual request.[169] If there is a reason individual access is refused, that reason should be shared.[170] Lastly, individuals should be able to challenge any access refusals through a legal process.[171] It is perhaps counterintuitive to suggest that people subject to electronic monitoring should have access to their own data, but it is an important element of overall privacy.

H. Accountability

Finally, the accountability principle states that "[a] data controller should be accountable for complying with measures which give effect to the [other] principles . . . ."[172] Accountability measures can take the form of legal sanctions or codes of conduct, and this obligation is not relieved because a third party processes the data.[173]

Accountability means changing the status quo. If private companies continue to be the primary controllers of data, they should be held accountable for these principles. While third parties are harder to hold accountable than government agencies, accountability measures are possible. Agencies could demand accountability in their vendor contracts, the judiciary could require accountability each time they sentence someone to electronic monitoring, and the legislature could set statutory standards for how these third-party companies collect data. Ultimately, it is the responsibility of these governmental bodies to hold the private companies they work with accountable for complying with privacy protection rules and guidelines.

Overall, applying the FIPPs provides an initial harm-reduction approach that addresses many concerns associated with the technological advancements in surveillance enabled by smartphone monitoring. These principles work best in tandem, and agencies, judges, and legislatures implementing any principle should consider each as part of the whole.

VI. CONCLUSION

Adding smartphones to electronic monitoring heralds unprecedented, limitless surveillance. Historically, electronic monitoring was inherently limited by ankle monitors' own technological capabilities, but today, advanced smartphones provide no such limits. Boundless smartphone monitoring is concerning because it expands overall electronic monitoring; implicates both collective privacy, as shown through

169. *Id.*
170. *Id.* at 15, 59.
171. *Id.* at 59.
172. *Id.* at 15.
173. *Id.* at 59.

collateral surveillance, and individual privacy, as shown by the endless data collection possibilities; increases the role of private companies; and depersonalizes a purportedly rehabilitative system.

A harm-reduction approach based on the FIPPs presents an initial solution. Though introducing privacy principles into criminal justice may seem odd, these principles — used by national and international governmental agencies — provide a comprehensive set of guidelines that can assist agencies, judges, and legislatures in addressing concerns raised by smartphone monitoring's technological advancements. While the FIPPs may seem unnecessary because many justice-involved individuals have ostensibly consented or because the needs of the state outweigh privacy concerns, there is still room to limit this type of surveillance. Because the technology used in electronic monitoring is no longer self-limiting, the law must set limits.