SENTENCED TO SURVEILLANCE:
FOURTH AMENDMENT LIMITS ON ELECTRONIC
MONITORING*

KATE WEISBURD**

As courts and legislatures increasingly recognize that “digital is different” and attempt to limit government surveillance of private data, one group is conspicuously excluded from this new privacy-protective discourse: the five million people in the United States on probation, parole, or other forms of community supervision. This Article is the first to explore how warrantless electronic surveillance is dramatically transforming community supervision and, as a result, amplifying a growing privacy-protection disparity: those in the criminal legal system are increasingly losing privacy protections even while those not in the system are increasingly gaining privacy protections. The quickly expanding use of GPS-equipped ankle monitors, as well as other forms of electronic searches, reflects unprecedented government surveillance that has yet to be regulated, scrutinized, or limited in any meaningful way.

This Article explores this phenomenon in its own right but also contends that the expanding disparity in privacy protections is explained by two underappreciated but significant shifts in Fourth Amendment jurisprudence. First, on the theory that defendants “choose” surveillance in exchange for avoiding incarceration, courts increasingly invoke consent to justify otherwise unconstitutional surveillance of people on community supervision. While the debate over criminal justice bargaining is not new, the expanded reliance on consent in this context reveals blind spots in the existing debate. Second, courts also increasingly accept government arguments in favor of otherwise unconstitutional electronic monitoring under a general “reasonableness” standard, as opposed to the traditional “special needs” doctrine. This insidious shift toward “reasonableness” threatens to jeopardize the precise interests the Fourth Amendment was designed

* © 2020 Kate Weisburd.
to protect. But even under a reasonableness standard, electronic surveillance of people on community supervision should be more circumscribed. Ultimately, this Article reveals how the significance of these two shifts extends beyond electronic surveillance and represents a new frontier of sanctioning warrantless searches without any level of suspicion or exception to the warrant requirement.

INTRODUCTION .................................................................................................. 719

I. MECHANISMS OF SURVEILLANCE SENTENCES ................................. 725
   A. Taxonomy of Electronic Surveillance in Community Supervision ................................. 726
      1. Electronic Monitoring Technology .................................................. 726
      2. Electronic Search Conditions and Computer Monitoring ...................................... 728
   B. Explaining the Expansion .......................................................................... 729
   C. Justifying the Expansion .............................................................................. 732

II. "CONSENSUAL" SURVEILLANCE SENTENCES .................................... 736
   A. The Rise of Consent ..................................................................................... 737
   B. Concerning Consent ...................................................................................... 739
      1. The Lack of a “Knowing” and “Voluntary” Waiver .......................................... 740
      2. The Lack of a True Discount: Unconstitutional Conditions .................................... 743
         a. The Failure To Focus on “Wrongful Coercion” in the Absence of a True Discount .............................................. 743
         b. Why Electronic Surveillance May Not Be a True Discount ..................................... 745
   C. Should Privacy Be Subject To Bargaining? ................................................. 746

III. "REASONABLE" SURVEILLANCE SENTENCES ..................................... 748
   A. The Evolution of “Reasonable” Community Supervision Searches ............................. 748
   B. Problematizing the “Reasonableness” of Surveillance Sentences ................................. 750
   C. Applying Reasonableness ............................................................................... 752
      1. Significant Privacy Intrusion .......................................................................... 753
         a. Privacy as Refuge ......................................................................................... 753
         b. Discouraging Dissent .................................................................................. 757
         c. Racialized Intrusions .................................................................................. 759
      2. Limited Government Interests .......................................................................... 761
         a. Undermines Rehabilitation ........................................................................... 761
         b. Increases Recidivism .................................................................................. 766
         c. Lack of Outcome Evidence .......................................................................... 767

IV. SUSPICION-BASED SURVEILLANCE: A PATH FORWARD ................. 770
INTRODUCTION

The key government witness against Zackary Jackson was not a person but the GPS-equipped monitor strapped to his ankle. It was the GPS monitor, and the GPS monitor alone, that placed Mr. Jackson at the scene of a robbery in Washington, D.C., in 2015. And it was the GPS monitor that led the police to Mr. Jackson's location where he was arrested. Mr. Jackson's arrest for robbery, and his ultimate conviction, was the culmination of a coordinated effort between the D.C. Metropolitan Police Department and the D.C. Court Services and Offender Supervision Agency. At the time of the 2015 robbery Mr. Jackson was on probation for a prior offense. A few weeks prior to the robbery, his probation officer was contacted by a D.C. police detective asking that Mr. Jackson be placed on a GPS monitor so that the police could track him and see if he committed any crimes. Mr. Jackson's probation officer then reviewed his file, concluded that he was in violation of some technical rules, including his failure to find employment and participate in programming, and required that Mr. Jackson wear a GPS ankle monitor. As a condition of wearing the monitor, Mr. Jackson signed a contract agreeing to twenty-two GPS-specific rules, including that he obtain pre-approval to change his daily schedule, that he charge his device twice a day, that he not fall asleep while the device charges, and other rules. There was no term about Mr. Jackson's location data being shared with the police. Although the trial court found that the government's use of the GPS data infringed on Mr. Jackson's reasonable expectation of privacy, the D.C. Court of Appeals disagreed, reasoning that the “Fourth Amendment permits probation supervision to intrude significantly on probationers’ privacy.”

Mr. Jackson's case is no anomaly; in the past few years, surveillance technology has dramatically transformed community supervision. The use of

2. Id. at 468.
3. Id. at 468–69.
4. Id. at 469.
5. Id. at 475.
electronic monitoring has more than doubled in the past decade, with people now routinely placed on ankle monitors that they must pay for, that track their every move 24–7, and that are accompanied by dozens of rules that govern all aspects of daily life. Those who have been on a monitor describe it as a “digital shackle,” a “satellite prison,” and that it made them “feel like an animal.” Likewise, many people on community supervision—both adults and children—are subject to continuous suspicionless searches of their personal electronic devices and data. To an unprecedented degree, the state now has the power to monitor the political speech, religious affiliations, health information, and romantic or personal communications of thousands of young people and adults on community supervision.

Curiously, this level of increasingly invasive and largely unregulated electronic surveillance of those on community supervision stands in stark contrast to recent statutory efforts and constitutional court decisions significantly limiting government surveillance of private citizens who are not in the criminal legal system. Critics on both ends of the political spectrum oppose large-scale government collection of DNA and have lamented the extent to which law enforcement agencies analyze social media data. At the same time,


10. James Kilgore, Monica Cosby—‘Out Here We Have So Much More To Lose’, YOUTUBE (Mar. 24, 2018), www.youtube.com/watch?v=gON7U5Szdmc [https://perma.cc/V8KD-MUE4].


13. See infra Section I.A.1.


15. See, e.g., Free Speech and Toleration, CHARLES KOCHE INST., https://www.charleskochinstitute.org/issue-areas/free-speech-and-toleration [https://perma.cc/4VZF-CV3U]; Hugh Handeyside, We’re Demanding the Government Come Clean on Surveillance of Social Media,
reports of private companies collecting and selling cell phone location data, as well as private photos on social media websites, have set off bipartisan alarms and a call for greater regulation. Likewise, efforts are underway at the local, state, and federal levels to regulate—and sometimes ban—the use of facial recognition technology. And the oft-divided Supreme Court has taken unanimous stands against warrantless electronic surveillance and cell phone searches of arrestees, even when officers have probable cause to arrest the suspect. The Court has likewise recognized that the concept of a “reasonable expectation of privacy” for Fourth Amendment purposes must reflect the “seismic shifts in digital technology” that now allow for “near perfect surveillance” of digital records that “hold for many Americans the ‘privacies of life.’” These efforts reflect a bipartisan consensus that, when it comes to government surveillance of private citizens, “digital is different.”

ACLU (May 24, 2018), https://www.aclu.org/blog/privacy-technology/internet-privacy/were-demanding-government-come-clean-surveillance-social [https://perma.cc/6WTZ-SZWE].


22. Id. at 2210.

23. Riley, 573 U.S. at 403 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

And yet, for the 4.5 million people in the United States on probation, parole, and other forms of community-based court supervision,25 “digital is different” has come to mean digital is worse.26 Perversely, the surge in electronic surveillance mechanisms has amplified a growing privacy-protection disparity: those not in the criminal legal system are increasingly gaining privacy protections while those inside of the system, like Mr. Jackson, are increasingly losing privacy protections. There is a general and growing consensus that “[w]ithin America’s own representative democracy, citizens would surely rise losing privacy protections while those inside of the system, like Mr. Jackson, are in a tracking device that revealed their location 24 hours a day.”27 Yet this is the lived experience of those on probation and parole who wear GPS ankle monitors, and the disparity in privacy protections does not impact everyone equally.28 As other scholars have observed, surveillance and other forms of automated big data policing reflect both a history of racialized social control and inequity.29

Of course, the unequal distribution of privacy rights between those in the criminal legal system and those not is hardly a new phenomenon.30 People on

26. See infra Section III.C.2.c.
27. Thompson & Warzel, supra note 25.
29. See SIMONE BROWNE, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS 8 (2015) ("[E]nactments of surveillance reify boundaries along racial lines . . . the outcome of this is often discriminatory and violent treatment."); ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, and THE FUTURE OF LAW ENFORCEMENT 131–40 (2017); Ruha Benjamin, Introduction, in CAPTIVATING TECHNOLOGY: RACE, CARCERAL TECHNOSCIENCE, and LIBERATORY IMAGINATION IN EVERYDAY LIFE 3, 3 (Ruha Benjamin ed., 2019) (describing automated policing as the “New Jim Code—innovation that enables social containment while appearing fairer than discriminatory practices of a previous era”); Elizabeth E. Joh, Automated Policing, 15 OHIO ST. J. CRIM. L. 559, 563 (2018) (claiming that automated policing “may exacerbate social inequalities in ways that have to be addressed”).
30. See Capers, supra note 28, at 1290; Christopher Sloboegin, The Poverty Exception to the Fourth Amendment, 55 FLA. L. REV. 391, 401–05 (2003) (arguing that poorer people and their property generally receive weaker Fourth Amendment protection than others); William J. Stuntz, The Distribution of Fourth Amendment Privacy, 67 GEO. WASH. L. REV. 1265, 1267 (1999) [hereinafter Stuntz,
probation and parole have, admittedly, long existed in a legal “netherworld” in that they are neither in prison nor totally free.31 Both people on community supervision and in prison inevitably have certain rights curtailed as conditions of their sentence. Yet these conditions—from strip searches to mandatory drug testing—must still pass constitutional muster.32

This Article explores and critiques this puzzling privacy disparity, offering both an explanatory account for its insidious rise and a reformist path forward. As explained below, this growing disparity does not reflect a public consensus that those on community supervision should have even less privacy than in the past. Rather, the disparity stems from two underappreciated but seismic shifts in Fourth Amendment law. First, courts are increasingly invoking consent to justify otherwise unconstitutional intrusions upon supervisees, the premise being that a defendant consents to surveillance in exchange for avoiding incarceration.33 While the debate over criminal justice bargaining is not new, the expanded reliance on consent in this context reveals significant blind spots in the existing debate. Second, otherwise unconstitutional surveillance is increasingly justified based on a general “reasonableness” standard, as opposed to traditional exceptions to the warrant requirement.34

These two shifts, which untether electronic surveillance from any meaningful constitutional restraint, set a new precedent that jeopardizes the precise privacy interests the Fourth Amendment drafters sought to protect, which is discussed later in this piece. Unlike physical searches conducted occasionally by police and supervision officers, electronic searches have no natural limit and can be conducted continually without defendants knowing if, or when, they are being surveilled. The result is a highly racialized panopticon of unprecedented proportion.35 Meanwhile, no empirical evidence suggests that broadly applied electronic surveillance corresponds to greater public safety, increased rehabilitation, or lower recidivism rates.36 Indeed, “probation by machine” may in fact lead to greater rates of re-arrest and incarceration, and in turn be criminogenic, by focusing on perfect detection and enforcement of
violations of technical rules drafted with the limits of the physical world in mind.

The profound Fourth Amendment implications of invasive electronic surveillance of people on probation and parole have, until now, not been well examined. While scholars, as well as the mainstream media, have begun to expose the hidden costs of electronic monitoring, none of the critiques focus on the unique Fourth Amendment problems with this level of broad surveillance.\(^{37}\) And while other scholars have examined how technology is altering policing and Fourth Amendment jurisprudence, as well as other forms of criminal justice surveillance,\(^{38}\) the same robust scrutiny has yet to be applied to surveillance of those on community supervision, a unique context because of its perceived status as a lenient alternative to incarceration. Additionally, the rich literature on probation and parole has yet to address the degree to which surveillance technology challenges the traditional legal justifications for diminished privacy rights for those on community supervision.\(^{39}\)

---


39. For comprehensive critiques of community supervision, see, for example, Fiona Doherty, Obey All Laws and Be Good: Probation and the Meaning of Recidivism, 104 Geo. L. J. 291, 294 (2016), for an examination of probation systems’ “almost farcical level of control over people’s lives,” and Michelle S. Phelps, The Paradox of Probation: Community Supervision in the Age of Mass Incarceration, 35 LaW & Pol’y 51, 52-53 (2013) [hereinafter Phelps, The Paradox of Probation], for a description of probation as both a net widener and an alternative to traditional incarceration.
This Article is the first to interrogate the Fourth Amendment consequences of electronic surveillance of people on community supervision. Part I chronicles the expansion of electronic surveillance in the context of community supervision and why it has flown under the scholarly and legislative radar. Part II of the Article documents and critiques the increased use of consent as a justification for perpetual electronic surveillance. This part of the Article challenges the assumption that defendants freely and knowingly “choose” supervision conditioned on electronic surveillance over incarceration and reveals how electronic surveillance is often not an alternative to incarceration but simply an add-on. Part III examines the erosion of the traditional “special needs” warrant exception and the emergence of the “reasonableness” standard as a basis to justify electronic surveillance of people on community supervision. Part IV then explores the unique way that electronic surveillance reveals deep fissures in the reasonableness standard.

The Article concludes with a prediction and a prescription. The prediction is that the increased reliance on consent and general “reasonableness” will extend beyond the supervision context, representing a new and troubling frontier of sanctioning suspicionless, warrantless searches with no natural limits. The prescription is two-fold: (1) require a warrant for electronic surveillance of supervisees while retaining the ability to conduct physical searches based on “special needs”; and (2) decrease reliance on intensive community supervision and electronic surveillance as de facto sentences. This shift would curb net widening and help restore community supervision to its proper role as a more precisely targeted intervention.

I. MECHANISMS OF SURVEILLANCE SENTENCES

This part both offers an overview of types of surveillance used in community supervision and charts the expansion of surveillance, noting the extreme dearth of data and research on these subjects. This part highlights two points. The first is that the expansion does not appear to be the result of deliberate policymaking based on rational penological concerns related to community supervision. The second is that this unprecedented level of surveillance would be unconstitutional under recent Fourth Amendment case law related to electronic searches, absent the ability to rely on consent or a newly created roving “reasonableness” standard.

40. This Article is part of a larger research project aimed at better understanding how electronic monitoring operates in the criminal legal system. As part of this project, I am collecting agency policies that govern the use of electronic monitoring for people on pretrial release, probation, parole, and other forms of court supervision. These records include the terms and conditions of electronic monitoring, internal agency policies, as well as the contracts between municipalities and private companies that provide electronic monitoring services. Many of the agency records referenced in this paper are part of this larger research endeavor.
A. Taxonomy of Electronic Surveillance in Community Supervision

Increasingly precise surveillance technology emerges every day. What follows are a few common types of surveillance currently used to monitor people on probation, parole, and other forms of supervised release.\(^4\)

1. Electronic Monitoring Technology

All fifty states, the federal government, and the District of Columbia use some form of electronic monitoring to track the movement and activities of people on pretrial release, probation, and parole.\(^4\) According to a Pew Charitable Trusts research report, there were about 131,000 people on electronic monitors in 2015, which represented a one hundred forty percent increase over the prior ten years.\(^4\) The number of people on monitors today is likely much higher as monitoring has proliferated and expanded to include juveniles and people in immigration proceedings.\(^4\)

People on community supervision are subject to electronic monitoring in several different ways. The first is radio frequency monitoring, which tracks whether someone is at a particular location, most often their home.\(^4\) This system relies on a transmitter worn by a defendant that is connected to a landline phone and alerts the probation officer if the defendant leaves his or her home.\(^4\) The use of this system skyrocketed in the 1980s, and, although it is used less now, some states and federal courts continue to rely on it.\(^4\)

The second and more widely used technology is a GPS-equipped ankle monitor that relies on cell phone towers and satellites to, according to the International Association of Chiefs of Police, “pinpoint the actual location of the offender and track an offender’s movements over time.”\(^4\) The ankle monitors

\(^4\) Although the focus of this Article is the use of electronic surveillance of people on probation and parole, the same technology is also used in the context of pretrial release and lifetime GPS monitoring of sex offenders. Many of the arguments presented in this Article apply with equal force to those settings, but both settings have additional attributes that complicate the analysis and are beyond the scope of this Article.

\(^4\) THE PEW CHARITABLE TRS., supra note 7.

\(^4\) Id.

\(^4\) See Kofman, supra note 6. This number also did not include children. For example, in California alone there were 10,000 children on electronic monitors in 2017. See Crump, supra note 37, at 797. Determining the precise number of people on a GPS monitor should be a high priority for future research.

\(^4\) THE PEW CHARITABLE TRS., supra note 7.

\(^4\) Id.

\(^4\) Id.
vary in size, but most are the size of a cigarette box. The accompanying software allows the location of people on monitors to be viewed, stored, and analyzed by the private company administering the program, probation and parole agents, the police, or some combination thereof. Generally, these devices must be charged at least once a day. Some have the capacity to buzz or beep when an officer tries to contact the probationer or if the battery is low. Other varieties of monitors have two-way microphones that allow officials to talk with people on monitors at any time.

A third form of surveillance involves smartphone applications that allow GPS tracking via cell phones and instant communication without the use of a GPS-equipped ankle monitor. These systems vary but often rely on a GPS-equipped cell phone and a small ankle strap that must be within the range of the cell phone at all times. Both the cell phone and strap vibrate and emit audible alerts when they are separated. Another variation involves a cell phone without an ankle monitor and requires the defendant to submit to random and frequent voice verification check-ins.

Common across these variations is the use of a range of applications that allow monitoring of compliance with exclusion zones, curfew, exact pinpoint location, and video or photo check-ins. Some applications also allow probation

50. THE PEW CHARITABLE TRS., supra note 7, at 2.
51. A number of jurisdictions require that defendants charge their devices at least once a day. See, e.g., ADULT PROB. DEPT’; SUPREME COURT OF ARIZ., EXACUTRACK ONE GLOBAL POSITIONING SYSTEM (GPS) RULES (2014) (on file with author); BUREAU OF CMTY. CORRS., DEL., DEPT’ OF CORR., CONDITIONS OF ADDENDUM FOR GPS PROGRAM (2016) (on file with author); COURT OF COMMON PLEAS PROB. DEPT’; CUYAHOGA CTY., OHIO, ELECTRONIC MONITORING/GPS TRACKING UNIT RULES (2019) (on file with author); DEPT’ OF JUSTICE SERVS., ST. LOUIS CTY., ELECTRONIC HOME DETENTION CONTRACT/AGREEMENT (on file with author); IOWA DEPT’ OF CORRS., GLOBAL POSITIONING SYSTEM AND EQUIPMENT ASSIGNMENT RULES (2017) (on file with author); OFFICE OF OPERATIONS SUPERVISION PROGRAM, PRETRIAL SERVS. AGENCY FOR THE D.C., GLOBAL POSITIONING SYSTEM (GPS) ONLY CONDITION (2015) (on file with author); ORANGE CTY. PROB. DEPT’; TERMS & CONDITIONS FOR CONTINUOUS ELECTRONIC MONITORING SUPERVISION VIA GLOBAL POSITIONING SYSTEM (GPS) (on file with author).
52. Telephone Interview with Rosa Bay, Attorney, East Bay Cnty. Law Ctr. (May 2019).
56. Id.
57. Id. at 5–6.
officers to send reminders about court dates, job opportunities, or other appointments. 58 Still other applications allow for instant breathalyzer tests, with the results communicated to officials via Bluetooth technology. 59 Related technology includes sleep pattern analysis and general motion detection analysis. 60

Individual judges, and sometimes probation or parole officers, generally have discretion to impose electronic surveillance as a condition of community supervision or as a sanction for violations of community supervision, a decision which is made either at sentencing or at subsequent status hearings. 61 In some places, state law mandates that certain classes of individuals be placed on monitors. 62 People on electronic monitors must also agree to abide by dozens of rules, often in addition to the host of separate probation and parole conditions. 63

2. Electronic Search Conditions and Computer Monitoring

With increasing frequency, judges and prosecutors require defendants to agree to continuous suspicionless searches of their personal electronic devices and electronic data as a condition of supervision. These search conditions allow law enforcement to monitor supervisees’ e-mail, social media activity, texting, location and cell phone usage, and all other information contained on devices, twenty-four hours a day. For example, the following language is now common in standard plea agreements in some federal jurisdictions: “The defendant shall submit his person, residence, office vehicle, electronic devices and their data (including cellphones, computers, and electronic storage media), and any property under defendant’s control to a search. Such a search shall be conducted . . . at any time, with or without suspicion.” 64

58. See Nellis, supra note 54, at 5.
60. See INT’L ASSN’N OF CHIEFS OF POLICE, supra note 48, at 5. These features are used, presumably, by state officials monitoring people on supervision.
62. See, e.g., MICH. COMP. LAWS ANN. §§ 750.520c(2)(b), 750.520n(1) (Westlaw through P.A. 2019, No. 178, of the 2019 Reg. Sess., 100th Legis.); N.C. GEN. STAT. § 14-208.40(b) (2019); WIS. STAT. ANN. § 301.48 (Westlaw through 2019 Act 76)
63. For a discussion of these rules, see infra Part II
Even if probation or parole conditions do not explicitly include an electronic search condition, some courts have upheld such searches, once they occur, as implicitly authorized by general probation and parole search conditions.  

Both electronic monitoring and electronic searches produce a range of data, including the person’s exact locations, both real-time and historical, as well as the contents of cell phones. 66 These data are then relied on by probation, parole, and other law enforcement officers as evidence of noncompliance with the terms of community supervision, or a new criminal allegation. 67 As in United States v. Jackson, 68 police also often rely on electronic monitoring for crime investigation—like identifying who was near a crime scene. 69

Beyond judicial proceedings and police investigations, it is not at all clear what happens to the collected data or with whom it is shared. In juvenile courts in California, for example, only one county in the state explicitly notes in the contract that the data from electronic monitoring will be stored and shared with other agencies. 70 In adult court, some electronic monitoring rules provide that the data is shared with police, 71 and conversely, some policies say nothing about what happens to the collected data. 72

B. Explaining the Expansion

No one catalyst explains the increased use of electronic surveillance in community supervision. Instead, the expansion has been gradual, irregular, and was likely the result of several related forces. In this sense, the expansion

---


67. See, e.g., Commonwealth v. Johnson, 119 N.E.3d 669, 699 (Mass. 2019) (concluding that police reliance on historic GPS-ankle monitor data from when defendant was on probation was reasonable).


70. See LCA ELEC. MONITORING PROGRAMS, SAN FRANCISCO SHERIFF DEPARTMENT CLIENT ENROLLMENT PACKET 1, 5 (2019) (on file with author).


mirrors the evolution of probation in general, which has been described as “haphazard[] and with no real thought.”

First, the expansion of electronic surveillance may be a spillover effect of targeted electronic searches of supervisees charged or convicted of a subset of serious crimes. For years, people convicted of certain crimes associated with computers or the internet have routinely been required to have their computers monitored by or provide their passwords to their probation officers. For example, people convicted of receiving child pornography through the internet may have limitations placed on their internet use while they are on probation.\textsuperscript{74} As of 2008, at least twenty-two states had laws requiring that people convicted of certain child sex offenses be electronically monitored, and at least six states require monitoring for life.\textsuperscript{75}

In recent years, however, the use of surveillance technology has quietly expanded beyond these few crimes. For example, under the First Step Act, federal inmates qualified to be released may be placed on house arrest enforced by electronic monitoring.\textsuperscript{76} And until recently, electronic searches and surveillance of computers and personal devices were ordered in juvenile court in California regardless of the underlying offense.\textsuperscript{77} Similarly, in Illinois, recent research revealed that electronic monitoring was imposed in a wide range of cases and not limited to a particular subset of serious offenses.\textsuperscript{78}

Second, the rise of electronic surveillance may relate to increased pressure on municipalities to cut short-term supervision costs and lower incarceration rates at the front end rather than focus on quality of supervision and lowering long-term recidivism rates.\textsuperscript{79} Bail reform efforts aimed at either eliminating cash bail altogether or making it much easier for people to be released pretrial may help explain the impetus for municipalities to find “alternatives” to

\textsuperscript{73} Joan Petersilia, Probation in the United States, 22 CRIME \& JUST. 149, 157 (1997) (citing DAVID J. ROTHMAN, CONSCIENCE AND CONVENIENCE: THE ASYLUM AND ITS ALTERNATIVES IN PROGRESSIVE AMERICA 244 (1980)).

\textsuperscript{74} See, e.g., United States v. Love, 593 F.3d 1, 12 (D.C. Cir. 2010).

\textsuperscript{75} See INT’L ASS’N OF CHIEFS OF POLICE, supra note 48, at 1.


\textsuperscript{77} In re Ricardo P., 446 P.3d 747, 749–50 (Cal. 2019).

\textsuperscript{78} SALTMARSH, supra note 36, at 4.

incarceration.\textsuperscript{80} In some places with newly enacted bail reform, like San Francisco and St. Louis, the use of electronic monitoring has steadily increased.\textsuperscript{81} Pretrial agencies, advocates, and academics alike have highlighted monitoring as a positive alternative to cash bail.\textsuperscript{82} At least one of the recently elected prosecutors, who are seen as part of the “reform prosecutor” movement, has put forth a new bail policy that explicitly provides for electronic monitoring as an alternative to cash bail.\textsuperscript{83}

As a result of the increased pressure to lower incarceration rates more generally, the growth in the number of people on probation and parole has recently, and significantly, outpaced the growth in the prison population.\textsuperscript{84} At the same time, probation and parole agencies have always been historically underfunded.\textsuperscript{85} As caseloads have gone up, probation and parole officers have been asked to do more, but with fewer resources.\textsuperscript{86} Faced with such constraints, “officers have little choice but to concentrate on surveillance, and the impersonal monitoring of offenders.”\textsuperscript{87} Faye Taxman, director of the Center for Advancing Correctional Excellence at George Mason University, explains that “electronic monitoring and other data provide important information that can be used in supervision . . . . This is an untapped resource.”\textsuperscript{88}


\textsuperscript{85} Petersilia, supra note 73, at 152.

\textsuperscript{86} VERA INST. OF JUSTICE, supra note 79, at 11; Christine S. Scott-Hayward, The Failure of Parole: Rethinking the Role of the State in Reentry, 41 N.M. L. REV. 421, 439 (2011).

\textsuperscript{87} Scott-Hayward, supra note 86 (internal quotation marks omitted) (quoting Richard P. Seiter, Prison Reentry and the Role of Parole Officers, FED. PROB., Dec. 2002, at 50, 51).

\textsuperscript{88} Faye S. Taxman, Community Supervision in the Post Mass Incarceration Era, 79 FED. PROB. 41, 43 (2015).
The third and related trend that may have incentivized and facilitated the expansion of electronic surveillance in community supervision is the influence of private industry. Surveillance technology is a big business. For example, several large publicly traded companies offer private probation services as well as a range of electronic monitoring programs. Private companies, with names such as “Leaders in Community Alternatives,” advertise “evidence-based” surveillance services such as “PureTag,” “PureTrack,” and “PureMonitor.” These private services are attractive to jurisdictions looking for ways to cheaply but effectively expand community supervision.

C. Justifying the Expansion

This section explains why electronic surveillance of this magnitude, absent the newly emerging use of consent and general reasonableness as legal justifications, would surely be unconstitutional under recent Supreme Court cases constraining electronic surveillance.

The recent Supreme Court decisions in Riley v. California, Carpenter v. United States, and United States v. Jones reflect the Court’s growing concern with expansive electronic searches. In Riley, the Supreme Court held that cell phones generally cannot be searched incident to arrest without a warrant. Although an arrestee has “reduced privacy interests upon being taken into police custody,” the Court emphasized that this fact “does not mean that the Fourth Amendment falls out of the picture entirely.” The Court focused on the unique privacy interests related to cell phones and cell phone data and concluded that “when ‘privacy-related concerns are weighty enough’ a ‘search
may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee.”

In *Carpenter*, the Court expressed similar concerns with respect to the privacy implications of searching historic cell phone location data. The Court observed that when the government tracks the location of a cell phone, “it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.” These concerns explain the Court’s decision to limit the third-party doctrine and instead require a warrant for the search of historic location data at issue in *Carpenter*. As privacy expert Orin Kerr recently noted, “*Carpenter* signals a new kind of expectation of privacy test, one that focuses on how much the government can learn about a person regardless of the place or thing from which the information came.”

Similarly, in *Jones*, the Supreme Court relied on comparable logic in holding that a GPS-tracking device attached to a suspect’s vehicle constituted a search. The privacy concerns expressed by Justice Sotomayor in her concurrence could apply with equal force to any type of government surveillance:

> [T]he government’s unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the government, in its unfettered discretion, chooses to track—may “alter the relationship between citizen and government in a way that is inimical to democratic society.”

If there is one common theme uniting *Jones*, *Riley*, and *Carpenter*, it is that “[d]igital [i]s [d]ifferent.” As a result, Fourth Amendment case law is adapting, or, as Kerr describes it, experiencing an “equilibrium-adjustment” in which Fourth Amendment law responds to “the digital age to restore the earlier balance of government power.” Indeed, the logic behind limiting the third-party doctrine in *Carpenter* flows from the recent recognition that when people use modern indispensable digital devices like cell phones, there is no voluntary

---

99. *Id.* (quoting *Maryland v. King*, 569 U.S. 435, 463 (2013)).
100. *Carpenter*, 138 S. Ct. at 2218.
101. *Id.* at 2223.
104. *Id.* at 416 (Sotomayor, J., concurring) (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).
106. Kerr, *Implementing Carpenter*, *supra* note 102 (manuscript at 8).
disclosure in a “meaningful sense.” Increased privacy protections for location data is not limited to court decisions. The intrusiveness of government electronic surveillance was precisely what the California Legislature intended to limit when it passed the Electronic Communications Privacy Act (“CalECPA”). The Act, arguably the most sweeping in the country, requires that law enforcement obtain a search warrant to track the location of private electronic devices and to search the data contained on them or on the internet.

But these privacy-protective adjustments to digital Fourth Amendment law have not been applied to people on probation and parole—ironically the exact group that is in fact wearing the ankle monitor invoked by Chief Justice Roberts in Carpenter, and is in fact routinely subject to the cell phone searches condemned in Riley. To be sure, Kerr proposes that the protections of Carpenter should apply when three requirements are met: (1) the records were made available because of “surveillance methods of the digital age”; (2) the records are not the “product of a user’s meaningful voluntary choice”; and (3) the records are of a type that “tends to reveal an intimate portrait of a person’s life beyond the legitimate interest of criminal investigations.” While these requirements would seem easily met by electronic surveillance of supervisees, the protections of Jones, Riley, and Carpenter have not been extended to people on probation and parole. For example, soon after CalECPA went into effect, San Diego judges began asking defendants to sign waivers allowing probation and police officers to search their electronic devices without a warrant or even any suspicion of wrongdoing. The state legislature soon followed suit. In 2017, CalECPA was amended to clarify that the new protections did not apply to someone who is on parole or “subject to an electronic device search as a clear and unambiguous condition of probation, mandatory supervision, or pretrial release.”

Courts have similarly refused to extend the holdings in Riley, Jones, and Carpenter to those on community supervision. The closest the Supreme
Court has come to addressing electronic searches was when it concluded that GPS monitoring of people convicted of certain sex offenses constituted a search under the Fourth Amendment and remanded the case to the lower court to determine if the search was reasonable.\textsuperscript{116} Similarly, a statute that barred those convicted of certain sex offenses from accessing social media was struck down as infringing on free speech. In doing so, the Court expressed the importance of the internet as the “vast democratic forum[]” and to “foreclose access to social media altogether is to prevent the user from engaging in the legitimate exercise of First Amendment rights.”\textsuperscript{117}

Traditionally, courts justified probation searches based on the “special government needs” exception to the warrant requirement. This exception applies when “special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.”\textsuperscript{118} The special needs exception consists of a two-part inquiry: first, whether the search is being conducted for a non-law enforcement purpose and, second, if there is a non-law enforcement purpose, whether the search is reasonable.\textsuperscript{119} Warrantless searches of public-school students\textsuperscript{120} and public employees,\textsuperscript{121} as well as sobriety check points,\textsuperscript{122} to name a few, have all been upheld pursuant to the special needs exception.

The “special needs” of Wisconsin’s probation department was what the Court relied on in upholding a warrantless search of a probationer in \textit{Griffin v. Wisconsin,}\textsuperscript{123} one of the first probation-search cases. The “special need[]” the Court referred to was probation's function as a “period of genuine rehabilitation and that the community is not harmed by the probationer’s being at large.”\textsuperscript{124} The Court concluded that this “regime” would be “unduly disrupted by a requirement of probable cause.”\textsuperscript{125} Still, the majority in \textit{Griffin} made clear that a warrantless probation search must be justified by “reasonable grounds” to

\begin{flushright}
\textsuperscript{116}\
\textsuperscript{117}\
\textsuperscript{118}\
\textsuperscript{119}\
\textsuperscript{120}\
\textsuperscript{121}\
\textsuperscript{122}\
\textsuperscript{123}\
\textsuperscript{124}\
\textsuperscript{125}
\end{flushright}
believe the area searched will contain contraband and that the ability to infringe on a probationer’s privacy is “not unlimited.”126

Even this qualified approach drew strong criticism from Justice Blackmun who, in his dissent, questioned the majority’s “curious assumption that the probationer will benefit by dispensing with the warrant requirement.”127 This criticism foreshadowed what would ultimately come to fruition: when it comes to probation and parole searches, the line between the “special” needs of community supervision and traditional law enforcement purposes is hard, if not impossible, to discern.128 For example, the D.C. Court of Appeals in the Jackson case upheld electronic monitoring of people on probation as a special needs search,129 while the Supreme Court of North Carolina found that electronic monitoring of people convicted of sex offenses was not a special needs search.130

Given these line-drawing problems, the special needs doctrine is not often relied on to justify electronic surveillance. Instead, courts most often invoke one or both of the following justifications for suspicionless and warrantless searches: consent and general “reasonableness.” In the next two parts, I address why the emergence of these two justifications is doctrinally concerning. Electronic surveillance, in particular, brings into sharp focus the deep fissures in the consent and “reasonableness” doctrines.

II. “CONSENSUAL” SURVEILLANCE SENTENCES

Perhaps because electronic searches are distinctively more invasive than an occasional physical search, courts—with more frequency—are now invoking consent as a justification, either by itself,131 or in combination with a relaxed totality-of-the-circumstances approach.132 Although many scholars and jurists

126. Id. at 875.
127. Id. at 886 (Blackmun J., dissenting).
128. Barry Friedman & Cynthia Benin Stein, Redefining What’s “Reasonable”: The Protections for Policing, 84 GEO. WASH. L. REV. 281, 294 (2016) (observing that “the special needs test has proven incapable of coherent application”).
131. See, e.g., United States v. McCoy, 847 F.3d 601, 605 (8th Cir. 2017) (upholding electronic search clause because defendant agreed to it as a condition of release); People v. Nachbar, 3 Cal. App. 5th 1122, 1129 (Cal. Ct. App. 2016) (upholding electronic search condition on grounds that defendant “accepted probation in lieu of additional punishment”); People v. Thornburg, 895 N.E.2d 13, 23–24 (Ill. App. Ct. 2008) (upholding computer search term based on defendant’s consent to the terms); State v. Gonzalez, 862 N.W.2d 535, 542 (N.D. 2015) (upholding computer search condition on the grounds that “the probationer consents to warrantless searches ... when he accepts the conditions of probation”).
132. See, e.g., United States v. Lambus, 897 F.3d 368, 412 (2d Cir. 2018); United States v. Bare, 806 F.3d 1011, 1018 n.5 (9th Cir. 2015); People v. Smith; 8 Cal. App. 5th 977, 986 (Cal. Ct. App. 2017); State v. White, 890 N.W.2d 825, 829 (N.D. 2017); State v. Keller, 893 N.W.2d 276, 278–79 (Wis. Ct. App. 2017).
have opined on the problems with consent-based searches,\textsuperscript{133} consensual electronic surveillance of people on community supervision brings to light additional concerns. This part of the Article charts the emergence of the consent justification for electronic surveillance of people on community supervision and then demonstrates why it developed in a way that is doctrinally unsound.

A. The Rise of Consent

Consent, either on its own or as a factor, has recently emerged as an oft invokes justification by government officials for imposing otherwise unconstitutional electronic searches or surveillance of people on community supervision.\textsuperscript{134} The consent is usually either explicit (for example, a defendant agrees to an electronic search condition as part of a plea agreement or condition of probation)\textsuperscript{135} or implicit (for example, a defendant agrees to a traditional search condition that is later determined to include electronic searches).\textsuperscript{136} Consent takes other forms as well. For example, people placed on electronic monitors are usually required to sign a contract or sign their initials, indicating that they agree to, or are at least aware of, the rules governing the monitoring program.\textsuperscript{137} These rules often include a provision that failure to comply or the decision to opt out of the program may result in incarceration.\textsuperscript{138}


\textsuperscript{134} See McCoy, 847 F.3d at 605 (upholding electronic search clause because defendant agreed to it as a condition of release); Nachbar, 3 Cal. App. 5th at 1129 (upholding electronic search condition on grounds that defendant “accepted probation in lieu of additional punishment”); Thornburg, 895 N.E.2d at 23–24 (upholding computer search term based on defendant’s consent to the terms); Gonzalez, 862 N.W.2d at 542 (upholding computer search condition on the grounds that “the probationer consents to warrantless searches . . . when he accepts the conditions of probation”); State v. Kane, 169 A.3d 762, 776 (Vt. 2017) (upholding electronic monitoring on grounds that defendant “agreed” to it as a condition of probation).

\textsuperscript{135} See, e.g., McCoy, 847 F.3d at 605.


\textsuperscript{138} See sources cited supra note 137.
Although lower courts increasingly rely on consent as a legal basis to impose probation and parole searches, the Supreme Court has declined to resolve the question of consent each of the two times it was given the opportunity to do so. United States v. Knights presented the first such opportunity. In that case, the Court granted certiorari on the precise question of whether Mr. Knights’s agreement to a probation condition allowing for warrantless searches constituted valid consent. And yet, the Court made a point to “not decide whether Knights’ acceptance of the search condition constituted consent” because it concluded that the search was reasonable under a “general Fourth Amendment approach of ‘examining the totality of the circumstances.’”

Despite the Court’s explicit decision not to address consent, it implicitly suggested that being “aware” of a search condition is relevant to the general reasonableness test. The Court focused on the fact that Mr. Knights was “unambiguously informed” of the search condition, the fact which “significantly diminished [his] reasonable expectation of privacy.” The Court observed that the “judge who sentenced Knights to probation determined that it was necessary to condition the probation on Knights’ acceptance of the search provision.”

Although simply being aware of a probation condition is not the same as consenting to it, the Court’s reasoning seems premised on the assumption that Mr. Knights could have—but did not—object to it. Being “informed of” and “accepting” terms are certainly species of consent.

Oral argument from Knights further reveals the Court’s concerns with consent in the context of probation. Justice Souter, for example, seemed to question the utility of labeling probation an “agreement” because in some cases a defendant is ineligible for a sentence of incarceration or has, in effect, been ordered onto probation, allowing no opportunity to actually “agree” to the individual terms of probation. Justices Ginsberg and Stevens also appeared to be concerned that consent in cases where a defendant could face jail time is coercive and may be an unconstitutional condition. These varied views may explain why the Court did not ultimately rule on consent grounds and instead relied on a general reasonableness standard.

The second time the Court addressed, but did not resolve, the question of consent-based community supervision searches was five years later in Samson v.
In Samson, the Court concluded that a parole search was reasonable even though there was no suspicion for the search. The Court’s focus this time was on the significantly diminished expectations of privacy for people on parole as compared to people on probation. Like in Knights, the Court did not explicitly resolve the question of consent but did focus on the fact that Mr. Samson “signed an order submitting” to the search condition and was thus “unambiguously’ aware of it.” Nonetheless, the Court made clear in a footnote that it was not invoking the special needs doctrine or consent because the search was deemed “reasonable” under a totality-of-circumstances test.

Despite the Court having yet to rule on the legality of consent-based searches, there is a near-perfect circuit split as to whether consent, and consent alone, is sufficient to justify a probation or parole search. On one side, many lower courts have found that explicit search conditions constitute a valid waiver of Fourth Amendment rights. And yet other courts have firmly rejected the notion that a warrantless search condition is “the price the government may exact in return for granting probation.” Courts have found, and judges have argued, that the search conditions were essentially nonconsensual, not that consent, if voluntary, is an insufficient justification.

The next section provides an argument that this reliance on consent is not only contrary to the realities on the ground, in terms of the voluntariness of the choice, but also—even assuming “knowing and voluntary” consent—is an illegitimate justification for such searches, outside a narrow subset of offenses.

B. Concerning Consent

The consent justification rests on the general premise that probation is “an act of clemency and grace” and that “[b]ecause a defendant has no right to probation, the trial court can impose probation conditions that it could not
otherwise impose.” The presumption is that “[i]f the defendant finds the conditions of probation more onerous than the sentence he would otherwise face, he may refuse probation.” Thus, otherwise onerous probation conditions have been upheld on the grounds that a probationer can always reject probation.

To date, both litigants and jurists have yet to focus on how consent is uniquely problematic in the context of electronic surveillance of people on community supervision. This section posits that blanket use of consent is troubling on two levels. First, many people’s decision to consent to search conditions or electronic monitoring cannot be said to be “knowing” or “voluntary” under even the most forgiving, government-friendly conceptions of those terms. Defendants, just like most people, underappreciate the risks of complex electronic searches, a concern that is ever-present in all criminal justice bargaining but heightened in the digital privacy arena. Second, electronic monitoring and search conditions are very often “add-ons” rather than bargained-for conditions in exchange for a real reduction in harshness of punishment.

1. The Lack of a “Knowing” and “Voluntary” Waiver

The first problem with consent is that a defendant’s acceptance of electronic surveillance as a condition of supervision may be neither knowing nor voluntary, even under traditional waiver doctrine, which generally defers to free market principles. It is axiomatic that the legal rights of the accused are “subject to waiver by voluntary agreement of the parties.”

Applying this doctrine, courts have accepted as valid the

153. People v. Anderson, 235 P.3d 11, 20 (Cal. 2010); see also People v. Ebertowski, 228 Cal. App. 4th 1170, 1175 (Cal. Ct. App. 2014) (upholding computer search term because “[a]dult probationers, in preference to incarceration, validly may consent to limitations upon their constitutional rights” (internal quotation omitted) (quoting People v. Olguin, 198 P.3d 1, 7 (Cal. 2008)).


155. See, e.g., United States v. Smith, 414 F.2d 630, 636 (5th Cir. 1969) (explaining that defendant “could have rejected probation and elected prison” and that, having "choose[n] to enjoy the benefits of probation," the defendant had to "endure its restrictions"); see also Andrew Horwitz, Coercion, Psychology, and Judicial Moralizing: Some Proposals for Curbing Judicial Abuse of Probation Conditions, 57 Wash. & Lee L. Rev. 75, 84–90 (2000) [hereinafter Horwitz, Coercion].


159. Bordenkircher v. Hayes, 434 U.S. 357, 363 (1978) (“[P]lea bargaining flows from ‘the mutuality of advantage’ to defendants and prosecutors, each with his own reasons for wanting to avoid trial” (quoting Brady v. United States, 397 U.S. 742, 752 (1970))).
waiver of a host of fundamental trial rights as a condition of pleas.¹⁶⁰ Yet even under traditional waiver doctrine, consent assumes transparency, equal access to knowledge, and opportunity for defendants to make a decision that is in their own best interest.¹⁶¹

However, some people subject to electronic surveillance never literally “choose” surveillance as an alternative to incarceration. For example, probation and parole are frequently part of mixed sentences—usually, a defendant will be sentenced to a jail or prison term, in addition to a term of probation or parole.¹⁶² In the federal system, as well as in some state systems, defendants cannot “opt out” of supervision; they are sentenced to a prison term followed by a mandatory term of supervised release.¹⁶³ In such cases, even though the defendant has not explicitly consented to the conditions of supervision, courts will often impose or uphold supervision terms as implicitly consensual in the sense that the defendant has acquiesced to a sentence that includes a term of supervision. Furthermore, the term of supervised release is on top of a period of incarceration and does not replace the prison sentence. In this way, supervised release is not an alternative to prison. And yet, the very term “search condition” linguistically reflects an assumption that community supervision is always a privilege because the alternative would be jail—even if the reality is that a defendant has no actual choice.¹⁶⁴

Even if a defendant chooses probation or parole as an alternative to incarceration, he might not have all of the information necessary to choose between supervision conditioned upon electronic surveillance and a prison sentence. The legal and practical implications of waiving Fourth Amendment rights are opaque and not obvious. For example, people contemplating plea offers are often unaware of the full collateral consequences of a conviction.¹⁶⁵ As in other contexts, such as Miranda warnings, waiver assumes an understanding of the benefits and risks.¹⁶⁶


¹⁶⁴ Several states (including New York and Illinois) follow the federal system in that defendants serve a portion of their sentence in prison and are then are ordered onto parole or supervised release. See, e.g., 730 ILL. COMP. STAT. ANN. 5/3-3-7 (Westlaw through P.A. 101-629); N.Y. PENAL LAW § 70.40 (McKinney 2009 & Supp. 2020).

¹⁶⁵ See generally Jenny Roberts, *Ignorance Is Effectively Bliss: Collateral Consequences, Silence, and Misinformation in the Guilty-Plea Process*, 95 IOWA L. REV. 120 (2009) (arguing that “only a constitutional mandate that requires a complete and full informational disclosure about the serious collateral consequences of guilty pleas will avoid the problematic incentive structures we have now”).

Moreover, in the context of conditions attached to plea offers, where the alternative is to go to trial and face a potentially harsher sentence, defendants rarely have access to all the pertinent facts about the evidence in their case or the likelihood of prevailing at trial. Indeed, in some jurisdictions, defendants accept guilty pleas (and the attendant conditions) without ever speaking to an attorney. And even if a lawyer is available, many court-appointed attorneys are underresourced and have little time to explain the consequences of various options. Indeed, the scene is a familiar one: a defendant speaks with his attorney in the hallway or in a holding cell, and a few minutes later, he pleads guilty. At sentencing the judge lists off the conditions of a plea, not further inquiring if the defendant understands such conditions. Although it is unknown how often electronic monitoring is part of a plea agreement, the rate of plea agreements is undisputedly high—roughly ninety percent of all criminal cases are resolved through plea agreements.

In short, few meaningful opportunities exist for defendants to gain the necessary information before waiving procedural rights as part of a plea or offer of a more lenient sentence. To state this proposition is not to suggest that defendants lack personal agency. Rather, the criminal legal system, arguably by design, provides limited opportunities for people to meaningfully exercise agency and make decisions that are in their own best interest. As other scholars have observed, the field upon which pleas and probation conditions are negotiated is rarely level and the bargaining power between prosecutor and defendant is rarely equal. While the appropriate response to these asymmetries of power is not necessarily to invalidate all plea agreements, a

167. For example, a plea offer with a condition of electronic surveillance might expire before a defendant has the chance to interview witnesses, conduct a preliminary hearing, wait to see if the grand jury indicts him, review prior statements of the government’s witnesses, wait for forensic testing results to come back, or try to interview and subpoena alibi or other defense witnesses.


recognition of such imbalances should loom large over any proposal upholding “consent” as a blanket justification without further scrutiny.

These ever-present concerns about ignorance, misinformation, and rationality in traditional plea bargaining are compounded in the context of electronic surveillance conditions. Professor Paul Schwartz has noted that “citizens are often unaware of, or unable to evaluate, the increasingly sophisticated methods devised to collect information about them.”

Appreciating the risks of electronic surveillance is uniquely challenging. And as Professor Daniel Solove has observed, “Despite the embrace of notice and choice, people do not seem to be engaging in much privacy self-management”; instead, people “routinely turn over their data for very small benefits.” One interpretation of such failure to self-protect might be that people do not care about privacy. But as Professors Solove, Chris Hoofnagle, Jan Whittington, and others have shown, poor privacy decisions are driven mostly by misinformation, misunderstanding, and underappreciation of downstream risks—not because people devalue privacy.

2. The Lack of a True Discount: Unconstitutional Conditions

a. The Failure To Focus on “Wrongful Coercion” in the Absence of a True Discount

Both sides of the recurring debate over criminal justice bargaining agree that deals are invalid unless they are knowing and voluntary. But once a decision to accept a deal meets these requirements, the sides diverge and take two paths of reasoning, both problematic. This section argues that both sides of the debate have incorrectly focused on whether a reasonable defendant feels free to say no to a condition that avoids incarceration. Instead, the correct focus should be on whether the condition offers a true discount off of the sentence that the defendant would have otherwise been entitled to receive.

One side of the existing debate over criminal justice bargaining—the winning side, thus far—views bargaining between the prosecution and a defendant as unproblematic so long as the defendant’s decision to accept a deal is “knowing” and “voluntary” in the sense that it is informed by accurate information and that the defendant has the ability to refuse the deal. Under this view, so long as a defendant has the ability to “refuse probation” if he “finds

175. Solove, Privacy Self-Management, supra note 156, at 1884, 1886.
the conditions of probation more onerous than the sentence he would otherwise face, the deal is unproblematic.

This logic, however, has a limit. In other contexts, the mere fact that a waiver of a right is knowing and voluntary does not render it legally unproblematic. If the bargain is not a true discount from what the bargainer should fairly expect otherwise, then the deal is still problematic, even if it is knowing and voluntary. This “unconstitutional conditions” doctrine “reflects the triumph of the view that government may not do indirectly what it may not do directly” and has been applied by courts in several contexts outside criminal law.

For example, imagine if the Governor of California decided to condition the granting of state park passes on California residents’ willingness to waive their Fourth Amendment rights and submit to routine continuous suspicionless electronic surveillance. The state park pass is clearly a privilege, not a right—the state of California could constitutionally decline to have parks at all or could constitutionally decline to allow human access to them, keeping them as wildlife refuges. But to condition such a privilege on the waiver of a constitutional right would presumably run afoul of the unconstitutional conditions doctrine. While the current doctrinal standard for what does and does not constitute such an unconstitutional condition remains infamously murky at best, the park pass example would surely be illegal under any conception of the test. The condition is not “related” to the state’s decision to grant a pass, and in a world where imposing electronic surveillance were not a possibility, the state would surely just grant the park passes unconditionally rather than withholding them.

There seems to be little reason, aside from inertia and tradition, not to recognize such wrongfully coercive conditions as invalid in the criminal justice context as well. While there may be difficult questions to address in terms of which deals run afoul of the doctrine and what the right baseline is, the idea that such reasonable limits on conditional offers would have no application in the criminal context makes little sense. While scholars such as Mitch Berman and Josh Bowers have persuasively argued that the doctrine is applicable in

180. Id. at 1415.
181. See Mazzone, supra note 158, at 805 (compiling examples of unconstitutional conditions doctrine applied in non-criminal settings).
183. See, e.g., South Dakota v. Dole, 483 U.S. 203, 207 (1987) (noting that “conditions on federal grants might be illegitimate if they are unrelated ‘to the federal interest in particular national projects or programs’” (quoting Massachusetts v. United States, 435 U.S. 444, 461 (1978))).
plea-bargaining context, the argument has gained little traction in challenging plea agreements in real criminal cases and has generated little scholarship outside of the plea-bargaining context.

On the other side of the debate, critics of criminal justice bargaining have equally failed to recognize that in some situations a plea offer may in fact reflect a "true discount" thus making the plea less coercive. Instead, critics and litigants have almost exclusively relied on the argument that a choice between “freedom and prison” is inherently coercive because the alternative of prison is so harsh that no defendant would ever refuse the deal. For example, in his dissent in Samson, Justice Stevens characterized the notion of a parolee’s consent to suspicionless physical searches as “sop histry” and that to speak of consent when the choice is freedom or prison is to “resort to a ‘manifest fiction.’”

This critique, though perhaps intuitive, is both over- and underinclusive and fails to recognize the crux of the problem. The mere fact that an offer is too good to refuse, given the “unpleasant alternative[,]” should be neither necessary nor sufficient to render a criminal justice bargaining process invalid. A plea deal that is the product of a fully informed choice and offers a true discount off a harsher sentence that a defendant would otherwise justifiably receive should not be condemned as inherently problematic simply because a reasonable defendant would find it difficult to refuse the deal. While it may be difficult to discern what constitutes a “justifiable” sentence, evidence such as sentencing guidelines and historical charging data could provide insight into what sentence a properly motivated prosecutor would have sought in a world without the condition at issue. If the deal really is a discount and accepting is a knowing and voluntary choice, then the only remaining reasons to disallow the deal would seem to be unconscionability or inherent objections to commodifying certain rights.

b. Why Electronic Surveillance May Not Be a True Discount

For most people on some form of community supervision, warrantless electronic searches and surveillance often offer no real discount. The baseline in

185. The one exception thus far appears to be the application of the doctrine to DNA sampling as a condition of dismissals and pleas. See Roth, Spit and Acquit, supra note 168, at 417.
188. Of course, the unconstitutional conditions doctrine is no panacea for the myriad of other concerns with plea bargaining in the criminal legal system, such as institutional racism, prosecutorial misconduct, and the politics of law-and-order policing. See, e.g., Michelle Alexander, Go to Trial: Crash the Justice System, N.Y. TIMES (Mar. 10, 2012), https://www.nytimes.com/2012/03/11/opinion/sunday/go-to-trial-crash-the-justice-system.html [https://perma.cc/F8WR-ZA4D (dark archive)].
many probation and parole cases—that is, the sentence the state would legitimately seek if electronic searches were not an option—is not prison. Instead, most supervisees would likely still receive probation or parole.\(^\text{189}\) In this way, people agreeing to an electronic search condition do not get any sentence “discount” because there is no actual benefit.\(^\text{190}\) The ostensible benefit—avoiding incarceration—places the defendant in no better stead than he would have been absent the state’s ability to condition release on accepting an electronic search condition.\(^\text{191}\) In turn, where the threatened penalty for rejecting the offer is as harsh as incarceration, most people—though technically able to reject the deal—are likely to accept the unconstitutional search condition.

Perhaps these concerns have motivated the few courts that have invoked the unconstitutional conditions doctrine to invalidate otherwise consensual searches of nonincarcerated defendants.\(^\text{192}\) For example, the Ninth Circuit determined that consent could not be the sole basis to uphold an otherwise unreasonable search conducted pursuant to a pretrial release agreement.\(^\text{193}\) In its opinion, the court cautioned that giving “the government free rein to grant conditional benefits creates the risk that the government will abuse its power by attaching strings strategically, striking lopsided deals and gradually eroding constitutional protections.”\(^\text{194}\) But these cases are outliers. In the end, if the unconstitutional conditions doctrine is not widely recognized as applicable to conditions imposing surveillance on the nonincarcerated, then there seems to be literally no limit to the state wielding consent to justify any surveillance measure.\(^\text{195}\)

Whatever doctrinal label one chooses—an unconstitutional condition, an unduly coercive “contract of adhesion,” or simply “involuntary”—electronic surveillance conditions should not be treated as a freely made choice simply because they are technically a condition on an offer of a nonprison sentence.

C. Should Privacy Be Subject To Bargaining?

It may also be that electronic surveillance should not be a bargaining chip to begin with. If one agrees with the premises underlying Carpenter, Riley, and

189. See Eisenberg, supra note 37, at 157 (noting the difficulty in assessing whether a defendant would have been placed on a monitor if “EM technology were not available”).


192. See, e.g., United States v. Scott, 450 F.3d 863, 866 (9th Cir. 2006); State v. Baldon, 829 N.W.2d 785, 802 (Iowa 2013).

193. Scott, 450 F.3d at 866.

194. Id.

195. See generally Kate Weisburd, Concerning Consent and Contracts: A Criminal Procedure Paradox (unpublished manuscript) (on file with author) (describing the broad reach of the state in justifying surveillance).
the California Electronic Communications Privacy Act, then electronic surveillance might be viewed as so unprecedented and invasive that to offer it up as something to be bargained away would be unconscionable.\footnote{196. See Roth, Spit and Acquit, supra note 168, at 444–46 (suggesting that DNA collection as a condition of a lenient sentence may raise bioethical concerns above and beyond traditional voluntariness concerns).} While limited surveillance in some particular subset of serious crimes might be appropriate, some may characterize a bargain that contracts away one’s right to be free of broad invasive surveillance of everyday communication as unconscionable.

The problem of forcing people to choose between privacy and everyday cell phone use was one of the key factors in the Court’s decision to limit the third-party doctrine in Carpenter. Chief Justice Roberts, in writing for the majority, focused on the pervasiveness of cell phones to conclude that there is no voluntary disclosure in a “meaningful sense” because cell phone use is so widespread and “there is no way to avoid leaving behind a trail of location data.”\footnote{197. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).} This concern with the lack of meaningful “choice” adds credence to the argument that perhaps privacy in one’s cell phone and own movements is not something that should be up for bargaining.\footnote{198. Although beyond the scope of this Article, there are contract-based arguments to be made about the legality of “bargaining” over Fourth Amendment privacy. See Wayne A. Logan & Jake Linford, Contracting for Fourth Amendment Privacy Online, 104 Minn. L. Rev. 101, 130 (2019).}

In both the commercial and criminal contexts, asymmetries abound “between data collectors and the individuals whose personal information is collected.”\footnote{199. Schwartz, supra note 174, at 2080.} When it comes to making a decision about sharing personal data, “people often favor immediate benefits even when there may be future determents . . . . [P]rivacy is an issue of long-term information management, while most decisions to consent to the collection, use, or disclosure of data are tied to a short-term benefit.”\footnote{200. Solove, Privacy Self-Management, supra note 156, at 1891.} The problem of short-term gain in exchange for potential long-term pain is analogous to defendants agreeing to invasive search conditions as a way to avoid a prison sentence.

These concerns have led privacy scholars to suggest ways of limiting the alienability of privacy rights while not completely eliminating the ability to bargain.\footnote{201. See Pamela Samuelson, Privacy as Intellectual Property?, 52 Stan. L. Rev. 1125, 1143 (2000); Schwartz, supra note 174, at 2106; Solove, Privacy Self-Management, supra note 156, at 1903.} These solutions include codifying basic privacy norms; invoking contract principles, such as default rules; establishing the right to exit; and creating institutions to monitor privacy violations.\footnote{202. Sonia K. Katyal, The New Surveillance, 54 Case W. Res. L. Rev. 297, 382 (2003); Schwartz, supra note 174, at 2106; Solove, Privacy Self-Management, supra note 156, at 1903.} It is not entirely clear how these solutions could map onto criminal justice bargaining, where defendants...
often have very little bargaining power to secure the most favorable outcome. While comprehensively applying the principles of property and privacy law to criminal justice bargaining is beyond the scope of this Article, much can be learned from examining the degree to which certain rights are considered alienable.

III. “Reasonable” Surveillance Sentences

Along with the rise of consent as a justification, the emergence of the general reasonableness standard reflects a trend toward state surveillance untethered from meaningful Fourth Amendment protections. This part explores the erosion of the special needs doctrine and how it has been replaced with the general reasonableness test. I then explain why this development is doctrinally unsound. Finally, I argue that, even under the ill-construed reasonableness test, electronic surveillance should be more often construed as unreasonable.

A. The Evolution of “Reasonable” Community Supervision Searches

The emergence of the general “reasonableness” justification for electronic surveillance reflects a significant shift in Fourth Amendment law that reverberates well beyond the situations at issue in *Knights* and *Samson*—the two cases that first articulated the reasonableness standard. As discussed in Part I, warrantless probation searches were initially justified under the special needs exception to the warrant requirement. Yet, most courts today do not invoke the special needs doctrine, and the last time the Supreme Court relied on the special needs doctrine in the context of community supervision was in 1987.

So, why did the Court abandon the special needs exception as the justification for probation and parole searches?

There is a two-part explanation for why the Supreme Court may have made such a sharp turn from special needs to reasonableness in justifying routine probation and parole searches. First, and perhaps most obvious, the searches in both *Knights* and *Samson* were carried out by law enforcement officers for purposes of crime solving, and, thus, it would have been disingenuous to label either search as being carried out as part of the probation or parole institution. Indeed, the government in *Knights* did not even argue that the search was justified on special needs grounds. From reviewing the pleadings and oral argument, it appears that the parties, as well as the Court, may have assumed that the special needs doctrine was beside the point precisely because

---

204. *Id.*
of the law-enforcement nature of the search. This conclusion makes sense as the special needs exception does not apply when “the immediate objective” of the search is “to generate evidence for law enforcement purposes,” even if the “ultimate goal” is to further a goal other than general crime control. What remains a puzzle is why the inquiry did not end there. If the searches in Knights and Samson were clearly for law enforcement purposes, why didn’t the Court simply conclude that they were “per se unreasonable under the Fourth Amendment”?  

The second part of the explanation may provide an answer: the shift to reasonableness was both piecemeal and, according to some scholars, doctrinally incoherent. In Knights, although the Court invoked a general reasonableness standard, the search was supported by reasonable suspicion and, therefore, the Court was not staking out dramatically new doctrinal territory. And in Samson, decided five years later, there was no suspicion to support the warrantless search, but the Court highlighted the unique status of parolees as having less liberty than those on probation. Although both holdings were intended to be limited (Samson was limited to parolees, and Knights was limited because there was reasonable suspicion in that case), together the cases are applied much more broadly. Today, most lower courts reviewing various forms of electronic surveillance do so on the Samson/Knights reasonableness test.

The emergence of a general reasonableness test is part of what Professor David Sklansky calls the Court’s “new Fourth Amendment originalism,” which focuses on what was considered unreasonable at the time the Fourth Amendment was adopted. The Court’s focus on reasonableness is also in accord with scholars, such as Akhil Reed Amar, who posit that the Fourth Amendment does not require warrants; on the contrary, the Framers were

205. See generally Transcript of Oral Argument, United States v. Knights, 534 U.S. 112 (2001) (No. 00-1260) (showing no argument of the special needs doctrine).


skeptical of general warrants. Instead, Amar argues, the Fourth Amendment’s chief concern is that searches be reasonable.

What does Samson mean for the future of warrantless searches and, in particular, electronic surveillance of people in the criminal legal system? As Cynthia Lee has observed, the “Court today stands at a crossroads” between adherence to the warrant requirement on the one hand and embracing a pure reasonableness standard on the other. While many jurists and scholars have challenged Amar’s view of the Fourth Amendment, these critiques have not yet been applied in the context of electronic surveillance of people on community supervision; that is the topic I turn to next.

B. Problematizing the “Reasonableness” of Surveillance Sentences

Electronic surveillance, in particular, reveals the degree to which the general reasonableness standard allows for “unbridled discretion” that has no natural limit. As pointed out by the dissent, Samson marked the first and only time the Supreme Court has upheld “an entirely suspicionless search unsupported by any special need.” Scholars have likewise noted that Samson removed any protection against “discretionary and suspicionless searches” of any subpopulation with reduced privacy rights.

Electronic surveillance reveals two additional and underappreciated concerns with the reasonableness standard. First, the reasonableness balancing test is “very deferential to the government, and the resulting searches are almost always deemed reasonable.” As Professors Barry Friedman and Cynthia Benin Stein have argued, “The Court’s idea of ‘balancing’ is illusory—the test is rigged such that the government almost always wins.” This is especially true when it comes to people on probation and parole: the government’s stated interest in preventing recidivism and protecting the community will almost always trump the privacy interest of people on community supervision—a group of people who already have diminished rights.

---

213. Id.
216. Id. at 860 (Stevens, J., dissenting).
218. Primus, supra note 208, at 256–57.
219. Friedman & Stein, supra note 128, at 297.
review—a level of scrutiny that has proven to be effectively no scrutiny at all.”

As a result, the reasonableness test “is a poor approach for protecting a constitutional right.”

This deference to government interests explains why, in post-Samson probation and parole search cases, the searches are almost universally upheld as “reasonable.” It is challenging to argue that “monumental interests of law enforcement” do not outweigh the already diminished privacy rights of people on community supervision. For example, courts post-Samson have upheld suspicionless DNA profiling of people on probation and parole as being reasonable, precisely because of the strong government interests in solving crime. As one judge cautioned in a dissent in one such case, by relying only on a reasonableness standard to justify suspicionless law enforcement searches, the Fourth Amendment becomes “little more than an afterthought as the government seeks to conduct more and more invasive general programs in the name of law enforcement.”

The second problem with the test is that when it comes to electronic surveillance, reasonableness is a “boundless” standard. In writing for the majority in Samson, Justice Thomas emphasized that California law forbidding “arbitrary, capricious or harassing” searches guarded against searches conducted “at the unchecked ‘whim’ of law enforcement.” And yet, the nature of expansive electronic surveillance of people on probation and parole is, in many ways, arbitrary and harassing. Unlike physical searches, electronic surveillance is invisible and people do not know when they are being searched or watched. Electronic surveillance also monitors not just those in the criminal legal system but everyone with whom they communicate or associate. And as discussed below, electronic monitoring allows for the perfect surveillance of inevitable imperfections with the many rules governing community supervision. Monitoring tracks not just compliance with the technical terms

---

221. Steiker, supra note 217, at 855; see also Thomas Y. Davies, Recovering the Original Fourth Amendment, 98 Mich. L. Rev. 547, 556 (1999) (arguing that the Framers intended for warrants to curb police power).
222. Primus, supra note 208, at 297.
225. See United States v. Kriesel, 508 F.3d 941, 947 (9th Cir. 2007); Banks v. United States, 490 F.3d 1178, 1185 (10th Cir. 2007); United States v. Weikert, 504 F.3d 1, 3 (1st Cir. 2007); United States v. Kraklio, 451 F.3d 922, 924–25 (8th Cir. 2006).
226. Kincade, 379 F.3d at 865 (Reinhardt, J., dissenting).
227. Id. at 866.
229. For additional discussion on the harassing nature of electronic surveillance, see infra Section III.C.
230. See infra Section III.C.
231. See infra Section III.C.2.
of release, it collects and stores a perfect digital trail—capturing data on people’s location that arguably has nothing to do with probation or parole. In these ways, electronic surveillance reflects a form of “arbitrary, capricious or harassing” searches that are nonetheless justified as “reasonable.”

The “opaque” and “malleable” nature of the reasonableness standard also offers little in terms of consistency or guidance to lower courts. This lack of guidance may explain why two lower courts came out differently on a nearly identical question: whether continuous GPS monitoring of parolees is reasonable. Although the Supreme Court recently found in Grady v. North Carolina that lifetime GPS monitoring constituted a search, it remanded the case on the question of whether the search was reasonable. On remand, the Supreme Court of North Carolina found that GPS monitoring was not reasonable because of the “State’s inability to produce evidence of the efficacy of the lifetime [monitoring] program in advancing any of its asserted legitimate State interests.” In contrast, the Seventh Circuit upheld GPS monitoring as reasonable because of the strong law enforcement interests. Perhaps the difference in case outcomes can be explained by the difference in facts, but it is also the case that a general reasonableness test lends itself to being applied inconsistently across jurisdictions. As Cynthia Lee points out, the lack of guidance is surprising given that “on numerous occasions the Court has spoken of the importance of having bright line rules.”

C. Applying Reasonableness

The above critiques notwithstanding, even under a general reasonableness test, courts should more often rule that blanket use of electronic search conditions and electronic monitoring is unreasonable. This section makes the case that Jones, Riley, and Carpenter should force a recalibration of evaluating the reasonableness of electronic surveillance of people on community supervision. Considering what is now known (and not known) about the capacity of digital surveillance, which is beyond what was possible with the physical searches at issue in Samson, the balance between government interests versus privacy intrusions now tips in favor of greater privacy protection.

232. Samson, 547 U.S. at 856.
234. Id.
235. Lee, supra note 214, at 1149.
237. Id. at 309–10.
239. Belleau v. Wall, 811 F.3d 929, 932 (7th Cir. 2016).
240. Lee, supra note 214, at 1149.
1. Significant Privacy Intrusion

One of the most common factors in evaluating the reasonableness of probation and parole searches, including electronic surveillance, is the fact that people on community supervision have a "significantly diminished" reasonable expectation of privacy. And yet, as any criminal procedure student knows, this logic is circular: People's expectations of privacy depend on expectations set, at least to some degree, by the government. As the late William Stuntz observed, "By altering its behavior, the government can change how people expect it to behave. Thus, if the government is bound only to respect people's expectations, it is not bound at all, for it can easily condition the citizenry to expect little or no privacy." This is especially true in the context of probation and parole, where the expectation of privacy is dictated by the official imposing the search condition or the GPS device. As Stuntz opines, the more important question—especially in the context of surveillance—is a normative one: What should a person's reasonable expectation of privacy be? In Carpenter, the Court began to answer that normative question: People should, in fact, enjoy a reasonable expectation of privacy in their digital trail. And yet, as noted in Part I, this change in the Court's conception of expectations of privacy has not been extended to those on probation and parole. But it should be.

a. Privacy as Refuge

As other scholars have observed, invasive electronic surveillance exemplifies Jeremy Bentham's vision of the modern panopticon in which the "fear of being watched inhibits transgression." Indeed, the "panoptic gaze" of constant government surveillance is arguably the most dangerous threat to personhood and citizenship in modern life. Continuous electronic surveillance of one's movements, as well as data and communications, however, takes the panopticon one step further: the government is not just watching or threatening to watch but is actually "analyzing and drawing connections..."
Electronic surveillance of people on community supervision is an unprecedented blow to privacy of the nonincarcerated. With respect to electronic searches, much of our private lives is lived online and smartphones create a record of everything. Cell phone use, as well as the amount of data stored on them, has risen dramatically. Cellphone ownership is no longer limited to the wealthy; cell phones are now used by over ninety percent of adults. For example, most Americans do their banking and manage health records online.

As the Riley Court observed, 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.”

These privacy concerns apply equally to GPS-equipped ankle monitors. In her concurrence in Jones, Justice Sotomayor cautioned against the extensive use of GPS surveillance because “it generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.” This, in turn, alters “the relationship between citizen and government in a way that is inimical to democratic society.”

The nature of electronic surveillance, as compared to physical searches, also demonstrates the uniquely invasive quality of electronic searches. In the Riley Court’s words, “Before cellphones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy.” With respect to a typical probation search of a house, or a drug test that is a condition of probation, a defendant knows when he is being searched, tested, or monitored. And because it is a physical impossibility for law enforcement to constantly conduct physical searches or follow someone around...
twenty-four hours a day, a natural limit exists on the amount of searching that occurs.

Electronic surveillance, in contrast, allows law enforcement, with the click of a mouse, to access immense amounts of personal, otherwise private, information at any time of day and without notice to the defendant.\textsuperscript{256} The search of a cell phone “would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form.”\textsuperscript{257} Texts to family, emails to friends, political posts on social media, and confidential communication with doctors, for example, are all viewable at all times. And unlike a physical search of a home, GPS-equipped electronic monitoring means that people’s movement “will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.”\textsuperscript{258} In short, “[r]ather than a targeted query for information,” electronic surveillance “is often akin to casting a giant net, which can ensnare a significant amount of data beyond that which was originally sought.”\textsuperscript{259}

While Jones, Riley, and Carpenter focused on the rights of suspects, nothing about the Court’s discussion of the unique attributes of cell phones or GPS tracking devices rested on the special status of arrestees. Instead, the privacy costs articulated by the Court apply equally to any user of personal electronic devices or any person forced to wear an electronic monitor. Regardless of the owner’s status as a suspect, arrestee, probationer, or parolee, cell phones and electronic monitors are rich with private information about nearly all aspects of life.

The electronic privacy concerns for people on probation and parole are also heightened because they are already, for the most part, subject to probation conditions that allow for unannounced warrantless searches of their home, property, and person.\textsuperscript{260} By virtue of being on probation or parole, they already live their lives under a microscope. Electronic surveillance means that people on probation or parole have little remaining sectors of their lives shielded from the government’s view.

Being on a GPS ankle monitor also triggers significant dignity costs. Many people who have been on an electronic monitor describe it as a “shackle” that is

\begin{footnotes}
\item[256] Solove, Reconstructing Electronic Surveillance Law, supra note 245, at 1269.
\item[257] Riley, 573 U.S. at 396–97.
\item[258] Jones, 565 U.S. at 416 (Sotomayor, J., concurring).
\item[259] Solove, Reconstructing Electronic Surveillance Law, supra note 245, at 1269.
\item[260] Doherty, supra note 39, at 317–18 (discussing the frequency of probation searches).
\end{footnotes}
suffocating. Federal District Court Judge Jack B. Weinstein referred to electronic monitoring as tracking a person as if he “were a feral animal.” As long as GPS devices remain the size they currently are, they also act as a “scarlet letter,” which, as one judge observed, “will undoubtedly cause panic, assaults, harassment, and humiliation.” Clothes do not completely hide the devices, “especially given the need to regularly recharge and maintain the device’s GPS connection.” One young person on a monitor complained that the device buzzed in class, prompting his teacher to ask him why he was wearing the monitor. Another young person was turned away from a charter school when the principal saw the GPS monitor on his ankle. And people on monitors report that potential employers see the monitor and tell them to reapply once the monitor is removed. 

The privacy implications are significant not just for people on probation and parole but for everyone with whom they communicate and associate. It is well documented that “permissive parole search jurisprudence” leads to more searches of parolees’ nonparolee neighbors, which means that entire neighborhoods have dramatically lessened Fourth Amendment rights. In many jurisdictions, police accompany probation officers doing probation searches precisely because the ability to search is so much greater in the probation context. Electronic surveillance amplifies the privacy intrusions for third parties. The search of a cell phone reveals potentially incriminating statements by the person subject to the search and by anyone with whom they communicate. Such a search is a powerful tool in a police officer’s toolbelt: more likely than not, more than one person may make incriminating statements that are then recorded on multiple phones. Similarly, electronic monitoring implicates not just the person wearing the device but the other people with whom they associate or visit with. As one woman who spent time on a monitor explained, the “people who have not done anything are constantly being incarcerated with


263. Doe v. Bredesen, 507 F.3d 998, 1012 (6th Cir. 2007) (Keith, J., concurring in part and dissenting in part).


265. Lerner, supra note 53.

266. Telephone Interview with Laurel Arroyo, Juvenile Pub. Def., Alameda Cty. (June 15, 2018).


268. See Jacob bi et al., supra note 220, at 908 (“Parole not only reduces the Fourth Amendment rights of individual parolees, but also it erodes the constitutional protections of anyone the parolee happens to live with.”).

269. Id. at 888.

270. See Doherty, supra note 39, at 322.
the person [wearing the monitor]. Whoever lives in that house is being policed in that jail."\footnote{271} Thus, courts and scholars should acknowledge the collateral damage to others’ privacy from broad electronic surveillance of supervisees.

Some might argue that those on community supervision are not akin to the arrestees and suspects in \textit{Jones}, Riley, and Carpenter, given that people on probation and parole have been convicted of crimes and suspects are still presumed innocent. However, this difference, without more, cannot logically justify a dramatically different level of Fourth Amendment protections. In fact, a suspect for whom police have probable cause to believe committed a crime should arguably have fewer privacy rights than a probationer or parolee who has been restored to the normalcy of living and working in the community and suspected of no new wrongdoing and is not in a custody situation where the search is necessary for officer safety.

\textbf{b. Discouraging Dissent}

Warrantless government surveillance of people on community supervision risks chilling speech, as well as freedom of association and movement. Constant monitoring of one’s digital life and communications constitutes what Neil Richards has termed “intellectual surveillance,” a species of monitoring that is “especially dangerous because it can cause people not to experiment with new, controversial, or deviant ideas.”\footnote{272} Because supervisees know they are being potentially searched at all times,\footnote{273} electronic surveillance—more than physical surveillance—“shapes and restricts behavior.”\footnote{274} And because the courage to dissent is often a challenge, “[d]issent’s fragile lifecycle—from formulation to ferment—requires privacy and often confidential association to flourish.”\footnote{275} Moreover, while monitoring by commercial entities is one thing, monitoring by the state of a supervisee, who already understands he is one step away from incarceration upon revocation, might presumably have an even more dramatic dampening effect on would-be dissent.

By further stripping those on community supervision of personal agency and voice, constant surveillance arguably hastens the “civil death” associated with criminal convictions.\footnote{276} To be this closely watched and, by extension, limited in what you say or do, is part of the “degradation ceremony”\footnote{277} associated

with a criminal conviction. This intellectual surveillance may also contribute to what Monica Bell has termed “legal estrangement,” in which communities of color experience detachment and alienation from the state, and ultimately exclusion from the legal protections of society. 278

Ultimately, government monitoring of speech and movement jeopardizes democracy and political discourse by discouraging free flow of ideas and, in particular, dissent. 279 Those being watched cannot as meaningfully participate in the “vast democratic forums of the [i]nternet,” 280 or really any form of democracy. 281 Thus, “the worth of information privacy accrues” not only to the individual but ultimately to society. 282 Taken to extremes, the stifling of dissent through surveillance can eventually sound the death knell for a democracy; in Justice Brennan’s phrasing, surveillance “makes the police omniscient; and police omniscience is one of the most effective tools of tyranny.” 283

To the extent that misdemeanor practice and community supervision of low-risk defendants are modern means of managing certain populations, 284 the stifling of dissent in this subpopulation is particularly concerning. 285 Many people on community supervision already have criminal records that, depending on the jurisdiction, preclude them from exercising their political voice through alternative means such as voting and jury service. Over six million Americans are currently disenfranchised because of a criminal record. 286 Roughly thirty percent of African American men are prohibited from jury service because of a criminal record. 287 Thus, it is precisely this population that may have the most to lose from the inability to speak freely and criticize the very government apparatus that arrested, charged, prosecuted, and now surveilles them.

---

278. See Monica Bell, Police Reform and the Dismantling of Legal Estrangement, 126 YALE L.J. 2054, 2054 (2017).


282. Schwartz, supra note 174, at 2087.


c. Racialized Intrusions

Because of the rehabilitative and probation-as-privilege rhetoric surrounding community supervision, the racial inequity reinforced by electronic surveillance may be more insidious than the inequity of mass incarceration, which has been more thoroughly documented.\(^\text{288}\) And yet, as a community activist J. Jhondi Harrell explains, an ankle monitor invokes the “sign of an old slave shackle” and a “throw-back to slavery.”\(^\text{290}\) In many ways, electronic searches and surveillance are another method of social control that, by design, exert supervision over portions of the population deemed in need of “correction.”\(^\text{290}\) In Jonathan Simon’s words, the “othering” of people in the criminal legal system is historically racialized,\(^\text{291}\) and warrantless electronic surveillance represents another method of controlling the “other.”

As with virtually every aspect of the criminal legal system, invasive electronic surveillance of supervisees disproportionately impacts communities of color.\(^\text{292}\) In some neighborhoods, more than half of Black men are under correctional control, many on some form of probation or parole.\(^\text{293}\) The history of surveillance is likewise racialized. From the FBI monitoring leaders of the Civil Rights Movement to the surveillance of Movement for Black Lives, “people of color have been the disproportionate victims of unjust surveillance.”\(^\text{294}\) The parallels between surveillance today and slavery are ever apparent, as “[m]onitoring the movement of slaves was a central concern for plantation masters and slave patrollers.”\(^\text{295}\) As activist and monitoring expert James Kilgore explains, “[T]he data points of a GPS map are the modern

---

288. See Malkia Amala Cyril, \textit{Black America’s State of Surveillance}, PROGRESSIVE (Mar. 30, 2015), https://progressive.org/magazine/black-america-s-state-surveillance-cyril/ [https://perma.cc/J7LE-ADLA] (“As surveillance technologies are increasingly adopted and integrated by law enforcement . . . racial disparities are being made invisible by a media environment that has failed to tell the story of surveillance in the context of structural racism.”).


290. \textit{See VICTOR RIOS, PUNISHED: POLICING THE LIVES OF BLACK AND LATINO BOYS,} at xiv (2011) (describing the “youth control complex,” a system of constant surveillance in which every day youthful behavior is viewed as potentially criminal).


equivalent of ‘lanterns law’ that forced Black and Indigenous people in New York to carry candles if they travelled after dark—only the lights of data points never really go out.\textsuperscript{296} In these ways, electronic surveillance represents one of the newest forms of crime management and social control.\textsuperscript{297} Such searches allow for “aggregate control and system management” not just of individuals but of entire groups and subpopulations.\textsuperscript{298}

Surveillance in the criminal legal system has always been, at least to some degree, racialized. The concept of needing to monitor so as to enable reentry assumes an “unruly” group that requires correction. This same “rabble management” approach\textsuperscript{299} gave rise to the “broken windows” theory of crime-control,\textsuperscript{300} as well as aggressive police tactics like stop-and-frisk and using misdemeanors as a form of social control.\textsuperscript{301} These practices were ostensibly race neutral, and some argued that these policies benefited communities of color, but the reality, as observed by scholars, was that these policies had the opposite impact.\textsuperscript{302} Instead of solving crime and aiding in rehabilitation, these search-and-apprehend approaches of crime control inflict a form of state-sanctioned violence on communities of color, further subordinating and disenfranchising historically oppressed groups.

The ways in which electronic surveillance chills speech and association might also be viewed as a form of racialized degradation.\textsuperscript{303} As Professors Devon Carbado and Mitu Gulati point out in their book, Acting White?, “as a matter of both socialization and formal or informal political advice, African Americans are encouraged to signal cooperation by giving up their privacy” when confronted by law enforcement.\textsuperscript{304} In this way, warrantless electronic searches are not just about the loss of control over private information but also the ways...
that these searches “can build habits of dehumanization and brutality in the
institutions and officials carrying” them out.305

It is worth asking whether the solution may be a more egalitarian
distribution of diminished privacy rights—“equitable surveillance”306—across
all racial groups, an extension of the “all of us or none of us” position recently
articulated by several scholars.307 This solution might look like more people, not
less, being subject to electronic search conditions and surveillance. Professor
Bennett Capers, for example, makes a compelling argument that expanding
“soft” police surveillance techniques308—such as public surveillance cameras and
more terahertz scanners—would help deracialize policing because this
technology is not prone to implicit bias or unconscious racism.309 It is less
obvious if this reasoning holds true when the surveillance technology is more
invasive, less “soft,” and depends on law enforcement to implement, enforce,
and interpret.

2. Limited Government Interests

Having revealed the significant privacy interests at stake, I turn next to
the purported government interests in electronic surveillance of people on
community supervision. The most commonly stated government interests are
rehabilitation and reducing recidivism. And yet, as a threshold matter, there is
virtually no empirical evidence that electronic surveillance furthers these
goals—if anything, there are reasons to believe that surveillance undermines
these otherwise noble goals.

a. Undermines Rehabilitation

Expansive and invasive electronic surveillance is part of an overall regime
shift in community supervision that prioritizes automated, hypertechnical
surveillance over more individualized and, in theory, rehabilitative approaches.310 While scholars have theorized about the ways that community
supervision results in net widening and undermines, rather than promotes,

305. David Alan Sklansky, Too Much Information: How Not To Think About Privacy and the Fourth
Amendment, 102 CALIF. L. REV. 1069, 1105 (2014) [hereinafter Sklansky, Too Much Information].
306. Andrea Roth, Trial by Machine, 104 GEO. L.J. 1245, 1304 (2016) [hereinafter Roth, Trial by
Machine].
307. See Capers, supra note 28, at 1273; Bernard E. Harcourt & Tracey L. Meares, Randomization
and the Fourth Amendment, 78 U. Chi. L. REV. 809, 873 (2011) (noting potential salutary effects of
randomized searches and surveillance on racial disparities in policing).
308. Capers, supra note 28, at 1244.
309. Id. at 1276.
310. See GARLAND, supra note 297, at 168–70; JONATHAN SIMON, POOR DISCIPLINE: PAROLE
supra note 284, at 688–89; Michelle Phelps, Mass Probation: Toward a More Robust Theory of State
successful societal reentry, these concerns are amplified when electronic surveillance becomes a convenient, omniscient, and perpetual means to monitor strict compliance with probation and parole terms.

To fully appreciate the impact of electronic surveillance on the efficacy of probation as a penal intervention, one should bear in mind three fundamental features of the modern probation and parole system. First, probation and parole departments are historically underfunded and have increasingly high caseloads. As previously noted, while the number of people on some form of community supervision has dramatically increased, the number of probation and parole officers has not. Probation and parole departments are being required to do more with less.

Second, at the same time, the number of conditions of probation and parole has significantly increased. Those on community supervision are now ordered to comply with dozens of rules as standard practice, some very detailed and some very broad. Standard conditions include regularly reporting for probation office visits, notifying officers of address or job changes, not associating with people who have been convicted of felonies, not using or possessing alcohol or drugs, working regularly or attending school, paying probation fees and fines, supporting dependents, not leaving the state or county without permission from probation, abiding by curfew, obeying orders to “stay away” from certain people or places, providing DNA samples, and participating in certain drug and alcohol treatments. While any one condition may seem reasonable, the cumulative effect “imposes a nearly impossible burden.” At any point, anyone on probation could be out of compliance with some of the conditions that prohibit both criminal and noncriminal behavior.


313. See id.


315. Id. at 1710.


318. See, e.g., SIMON, supra note 310, at 11–12; Horwitz, The Costs of Abusing, supra note 79, at 75.
Additional rules are imposed for people ordered to wear monitors. In many jurisdictions, people on electronic monitors are subject to house arrest and may need permission from their probation or parole officer before leaving their house or changing their schedule.\(^{319}\) Other jurisdictions require that people on monitors obtain permission before changing employment, “required treatment,” and/or residence; that they maintain a working landline; and that they regularly charge their monitoring device.\(^{320}\) The sheer number of distinct rules is also notable. In Alaska, St. Louis, and Seattle, for example, people on electronic monitoring are subject to over thirty separate rules governing electronic monitoring.\(^{321}\)

Third, many probation terms are so broadly or vaguely worded that what constitutes a violation is highly discretionary. For example, as Professor Fiona Doherty discovered, the jurisdictions with the largest probation populations—Georgia, Texas, and California—all have broad “good conduct” terms that include “[b]e of [g]eneral [g]ood [b]ehavior,” do not “become abandoned to a vicious life” and “[a]void injurious and/or vicious habits.”\(^{322}\) In addition to the general “be good” terms, several states prohibit people on probation from spending time with “persons having known criminal records” and require them to either work full time or be in school.\(^{323}\) These terms are sufficiently broad that any range of everyday noncriminal conduct could be construed as a violation. Whether certain conduct triggers a formal violation is left to the
discretion of individual probation officers with little guidance; and these "street-level" discretionary decisions often go unscrutinized.\textsuperscript{324}

Taken together, these features reveal a regime primed to prioritize supervision techniques that favor technical compliance over time-intensive human interaction. High caseloads and limited budgets, coupled with the discretion afforded to probation officers to document violations of increasingly harsh terms, have given rise to a new type of hypercompliance.\textsuperscript{325}

In the context of hypercompliance, electronic surveillance allows for perfect detection of inevitable imperfections. This type of surveillance is arguably analogous to red-light cameras, except that the penalty is often incarceration rather than a two hundred dollar ticket.\textsuperscript{326} In addition, unlike regulations against running red lights, the conditions of probation are so numerous and broadly worded that documenting a violation based on an electronic search or a GPS monitor is presumably like shooting fish in a barrel. As one probation expert observed: “If I have 100 percent surveillance capacity, I’m going to find problems, and then I’m going to have to respond to them.”\textsuperscript{327} Furthermore, an “agent conducting a search or seizure no longer need to be physically located in the same place as the target of the search or seizure.”\textsuperscript{328} As a result, expansive electronic surveillance tends to focus attention on the defendant’s rule compliance, obscuring or relegating to the background deficiencies within public institutions, such as schools, probation, and parole.

Expansive electronic surveillance, with its emphasis on strict rule compliance, exemplifies the way that the “rehabilitative functions associated with parole have atrophied.”\textsuperscript{329} Indeed, electronic searches and monitoring are not inherently rehabilitative in nature—they are merely tools that purport to facilitate supervision,\textsuperscript{330} giving probation officers and police “wide latitude in deciding how to press for compliance.”\textsuperscript{331} For example, people who have spent time on electronic monitoring report being arrested when they failed to get permission to leave their house to go to a last-minute doctor’s appointment or a

\begin{itemize}
  \item \textsuperscript{324} Klingele, supra note 317, at 1039.
  \item \textsuperscript{325} See Scott-Hayward, supra note 86, at 439 ("Parole officers today spend more time monitoring conditions than providing services. In how they carry out their jobs, parole officers look less like social workers and more like police officers.").
  \item \textsuperscript{326} See, e.g., Richard M. Re, Imagining Perfect Surveillance, 64 UCLA L. REV. DISCOURSE 264, 267 (2016) (imagining surveillance technology that could perfectly identify and report the perpetrator of every crime); Roth, Trial by Machine, supra note 306, at 1303 (discussing red-light cameras).
  \item \textsuperscript{328} Jennifer Daskal, The Un-Territoriality of Data, 125 YALE L.J. 326, 369–70 (2015).
  \item \textsuperscript{329} THOMPSON, supra note 31, at 143.
  \item \textsuperscript{330} See Eisenberg, supra note 37, at 144 (discussing the ways that electronic monitoring “is not inherently rehabilitative”).
  \item \textsuperscript{331} Doherty, supra note 39, at 313.
\end{itemize}
job interview. Ultimately, when parole or probation officers focus on managing through technical requirements, “[s]uch technocratic rationalization tends to insulate institutions from the messy, hard-to-control demands of the social world.”

The expanded search power that comes along with electronic surveillance further undermines what are often already strained relationships between probation and parole officers and their supervisees. In Griffin v. Wisconsin, decided long before the advent of cell phones, Justice Blackmun, in his dissent, observed the irony of using rehabilitation as the justification for removing the warrant requirement:

I fail to see how the role of the probation agent in “foster[ing] growth and development of the client” is enhanced the slightest bit by the ability to conduct a search without the checks provided by prior neutral review. If anything, the power to decide to search will prove a barrier to establishing any degree of trust between agent and “client.”

Justice Blackmun just as easily could have been referring to warrantless electronic surveillance. GPS-monitoring and electronic searches send the message to supervisees that their supervising officers are less focused on meaningful reentry and more focused on “closely monitoring offenders to catch them when they fail to meet all required conditions.” And from the officer’s perspective, this level of “intrusive surveillance” can cause the monitoring agent “to dehumanize and depersonalize the people they search or surveil.”

Intensive surveillance may also chill communication that would otherwise facilitate the rehabilitation process. People on community supervision rely on cell phones and other electronic devices as a lifeline to reentry and reintegration. More than ever before, it is through smart phones, computers, and the internet that people on probation and parole connect to jobs, social services, health care providers, education, and more. Indeed, social media and the internet offers a “relatively unlimited, low-cost capacity for communication of all kinds.” And yet, warrantless surveillance may undermine this otherwise healthy exchange of information.

332. Kilgore, You’re Still in Jail, supra note 261.
333. Feeley & Simon, supra note 298, at 456.
336. Id. at 886 (Blackmun, J., dissenting) (alteration in original) (internal citations omitted) (quoting Id. at 876 (majority opinion)).
338. See Sklansky, Too Much Information, supra note 305, at 1112.
b. \textit{Increases Recidivism}

Suspicionless electronic surveillance likely contributes to greater rates of rearrest and reincarceration, not necessarily for new criminal offenses, but for technical rule violations.\textsuperscript{340} Although the degree to which this happens has yet to be studied, and is beyond the scope of this Article, higher arrest rates based on expansive electronic surveillance are an example of what scholars warn about as a danger of piling on collateral consequences in addition to prison and jail sentences.\textsuperscript{341} When courts place numerous probation conditions and restrictions on low-risk defendants, the result is probation violations for minor infractions that are often unrelated to public safety.\textsuperscript{342} These violations are rarely attributed to the excessive “piling on” problem; instead the fault is placed on the defendant for not taking advantage of reentry services. And violations do not impact all people on probation and parole equally. Leading researchers have found that non-white people on probation are subjected to higher rates of probation revocation.\textsuperscript{343}

At the same time, resource-strapped probation and parole agencies are often ill-equipped to address violations through any consequence other than incarceration. On the front end, there are fewer resources and staff for meaningful and individualized support (such as treatment programs, educational opportunities, job training or counseling). According to one national study, for example, “over two-thirds of probationers reported using drugs in the past; nearly a third reported use in the month before” the conviction that lead to probation.\textsuperscript{344} And yet only seventeen percent of those respondents received any substance abuse treatment while on probation.\textsuperscript{345}

The consequence of more easily detected violations is often incarceration. On the back end, agencies are so underfunded that they cannot “respond to technical violations in a graduated or nuanced way.”\textsuperscript{346} Because there are so few


345. Id.

resources in the community, probation and parole officers “default to the most available option they have—the most expensive and punitive option—the formal violation process which often results in jail or prison.” In this way, electronic searches contribute to a catch-22: more is expected of people on community supervision; noncompliance is more easily detected; and at the same time, there are fewer resources to support those on community supervision, both to avoid a violation in the first place and as a response to a violation. As Professor Michelle Phelps’s research demonstrates, people on probation who have more resources and privilege tend to fare better while “their less advantaged counterparts are funneled deeper into the criminal justice system.”

In short, increased surveillance capabilities may contribute to increased recidivism rates, not for new criminal offenses but for rule violations that often have little to do with public safety. Indeed, it is well settled that probation and parole violations account for a large percentage of prison admissions. In some states, more than one in three people in prison are there for technical supervision violations, such as a failed drug test or failure to report to a probation appointment. These violations become a gateway to months (if not years) of cycling in and out of incarceration, reflecting a “closed circuit of perpetual marginality.”

c. Lack of Outcome Evidence

There is no evidence that more surveillance effectively addresses any of the underlying problems that may have triggered someone’s entry into the criminal legal system. There is also no data demonstrating that greater surveillance leads to greater public safety. If anything, most mainstream news stories about electronic monitoring focus on people who cut off the monitor before committing a new crime. Of the very few studies that do exist, some make claims about effectiveness, but these studies are small in scale and fail to compare outcomes between people on monitors and similarly situated groups not on monitors.

347. Id.
348. See Phelps, supra note 342, at 56.
350. Id.
351. Alexander, supra note 293, at 95.
353. See Eisenberg, supra note 37, at 176–77.
There is, however, emerging research concluding that electronic monitoring leads to worse outcomes. As two researchers from the Brookings Institute observed, “False positive alerts overwhelm corrections officials, ‘tamper-proof’ devices can be circumvented, and technical glitches interfere with users’ ability to hold down a job.” Similarly, a pilot project for monitoring court-involved youth in New York City was plagued with technical problems, including problems with battery life, the ability to charge the devices, and cell phone reception in a large urban area. The monitoring devices also alerted the young people through a beep that was so disruptive at school that one participant was asked to leave class. A recent study by the Illinois Sentencing Policy Advisory Council likewise found that the use of electronic monitoring “can increase the risk of technical violations and returns to prison, especially for low- or moderate-risk offenders.” People who have worn ankle monitors also worry that the devices will malfunction or prove unreliable.

There is also little evidence that placing more people on electronic monitors corresponds to less crowded jails and prisons. In San Francisco, for example, bail reform triggered an increase in the use of electronic monitoring, but there was no parallel dip in the jail population. While other factors may help explain this phenomenon, the data does not appear to support the proposition that more people on electronic monitors means fewer people in jail.

Part of the reason there is so little empirical evidence is that the use of electronic surveillance is opaque. The opacity of electronic surveillance flows from a few sources. First, there is no meaningful oversight, much less judicial review, of the processes that lead to electronic surveillance. For example,
prosecutors and judges are provided wide latitude in plea negotiations and setting terms of supervised release. In at least one jurisdiction, Washington, D.C., it is often probation officers—not judges—deciding who is placed on a monitor and for how long. No mechanism exists to track conditions of probation or the specific terms of the several thousand plea agreements that are processed in the United States each year.

Second, it is challenging to evaluate the full impact of electronic surveillance because implementation is left to the several thousand probation and parole agencies throughout the United States. The extent to which electronic surveillance mechanisms are relied on, and how, is the product of thousands of administrative decisions and exemplifies how the parameters of searches are increasingly “designed through administrative policies.”

Third, the expansion of the criminal legal system through private industry, rather than more transparent public decisionmaking processes, also frustrates any effort to collect and analyze data. Relatedly, with private industry driving reform, it is impossible to disaggregate whether it is profit motive or sound evidence-based policy behind the expansion of criminal justice surveillance technology. The advertising rhetoric (with services like PureTrack that are touted as “community-based” alternatives) further compound the opacity problem. It is challenging to discern the precise service being offered or how it is used in practice.

In sum, the effectiveness of electronic surveillance can only be evaluated once there are better data and a greater understanding of the technology and its potential flaws. Collecting and analyzing data is well within the capacity of government agencies that oversee community supervision. For example, in 2019, the Illinois General Assembly passed a bill that requires the state to collect and publish data on how electronic monitoring is used, including the demographics of who is placed on a monitor, the justifications for placing people


363. See Horwitz, Coercion, supra note 155, at 80–81 (describing wide discretion afforded to courts in imposing any probation condition).

364. See United States v. Jackson, 214 A.3d 464, 468 (D.C. 2019) (detailing the process of a detective asking the parole officer agency to have an individual electronically monitored).

365. See Doherty, supra note 39, at 344.

366. See Petersilia, supra note 73, at 153.


368. Feeley supra note 89, at 1; Roth, Spit and Acquit, supra note 168, at 436.


370. For a discussion of privatized policing technology, see Joh, Policing by Numbers, supra note 90, at 66.

371. See Eisenberg, supra note 37, at 176–77.
on monitors, and what happens to people once they are on monitors. This legislation has the potential to serve as a model for other states committed to better understanding how monitoring operates and if it leads to better outcomes.

IV. SUSPICION-BASED SURVEILLANCE: A PATH FORWARD

By every indication, electronic surveillance is now a permanent fixture in the criminal legal system. The more challenging question is how to limit and regulate its imposition. In this final part, I suggest a path forward that not only takes seriously public safety and the rehabilitative goals of supervision but also moves away from the unfettered use of both consent and reasonableness to justify otherwise unconstitutionally invasive conditions.

A. Require a Warrant

The doctrinal solution for limiting electronic surveillance of those on community supervision is straightforward: require a warrant. There are two primary reasons this solution is doctrinally sound. First, electronic surveillance of people on community supervision, at least as currently employed, is conducted for law enforcement purposes and cannot be—nor should be—construed as a “special needs” search. Unlike a physical search, where getting a warrant may be impractical, it is less clear that obtaining a warrant to search a cell phone or attach a GPS device to someone’s ankle is so impractical as to excuse the warrant requirement.

Furthermore, unlike the search at issue in Griffin, which was limited to a physical search by a probation officer to monitor compliance with probation, electronic surveillance is categorically different. The data obtained through electronic surveillance is routinely relied on by probation, parole, and police officers to make arrests for both new criminal offences and technical violations. For example, the International Association of Chiefs of Police extols GPS monitoring because it can help place an “offender at the scene of a crime, allowing an agency to identify potential suspects or witnesses” and “offender’s alibi maybe supported or discredited using GPS data.” According to the American Probation and Parole Association, “[m]any [probation and parole] agencies have implemented manual or automated crime scene correlation


373. Solove, Reconstructing Electronic Surveillance Law, supra note 245, at 1299 (“[F]or most uses of electronic surveillance, warrants supported by probable cause should be required.”)

374. Primus, supra note 208, at 310 (arguing that, in the context of special needs searches, courts should ask whether complying with the warrant and probable cause requirements is actually impractical).

systems that can identify tracked clients who were in the vicinity of a crime scene.\footnote{376} Similarly, some of the electronic monitoring contracts that people sign explain that police (not just probation and parole) officers may view and use the data as evidence against them,\footnote{377} and GPS data is often relied on in criminal prosecutions.\footnote{378} In these ways, electronic monitoring and surveillance of people on community supervision “is ultimately indistinguishable from the general interest in crime control.”\footnote{379}

Unlike other special needs searches conducted by people who are clearly not law enforcement (such as teachers or employers), there is little distinction between probation officers and traditional police officers.\footnote{380} On paper, parole and probation officers may have different missions as compared to traditional law enforcement officers, but in practice, their roles significantly overlap. Police officers routinely conduct probation and parole searches and through these searches discover evidence of new criminal offenses, technical violations, or both.\footnote{381} At the same time, parole and probation officers monitor supervisees’ compliance with probation and parole conditions, but in many states they also have authority to arrest people for new criminal offenses as well as technical violations.\footnote{382} In short, it is hard, if not impossible, to make the case that electronic surveillance is primarily imposed for non-law-enforcement purposes. Ironically, this conclusion is consistent with at least part of the Court’s reasoning in \emph{Knights} and \emph{Samson}: there was no dispute that the searches in those cases were not justified on special needs grounds.

Second, if electronic surveillance is not categorized as a special needs search, then it should follow that it is presumptively unconstitutional unless

\begin{footnotes}
\footnote{376} AM. PROB. & PAROLE ASS’N, INCORPORATING LOCATION TRACKING SYSTEMS INTO COMMUNITY SUPERVISION 7 (2019), \url{http://appa-net.org/eweb/docs/APPA/stances/ip_IL.pdf [https://perma.cc/HQ4Y-PRF3].}
\footnote{377} See COURT OF COMMON PLEAS PROB. DEP’T, CUYAHOGA CTY., OHIO, ELECTRONIC MONITORING/GPS TRACKING UNIT RULES (on file with author); KING CTY. WASH., DEP’T OF ADULT & JUVENILE DET., COMMUNITY CORRECTIONS PROGRAMS-ELECTRONIC HOME DETENTION (EHD) (on file with author); LCA ELEC. MONITORING PROGRAMS, SAN FRANCISCO SHERIFF DEPARTMENT CLIENT ENROLLMENT PACKET (2019) (on file with author).
\footnote{380} See, e.g., Minnesota v. Murphy, 465 U.S. 420, 432 (1984) (noting that a probation officer is considered a peace officer); see also Kimberlin v. U.S. Dep’t of Justice, 788 F.2d 434, 437 (7th Cir. 1986) (“A probation officer is clearly a law enforcement official as the term is ordinarily used. A probation officer, either under the direction of the court or the Parole Commission, performs law enforcement-related functions.”).
\footnote{381} See Jacobi et al., supra note 220, at 940.
\end{footnotes}
there is a warrant or an applicable exception. Requiring a warrant is not a particularly high bar. It requires only probable cause that the defendant either committed or is committing a new crime or violation of community supervision. This approach more likely ensures that electronic surveillance is imposed proportionally in a targeted and narrow way and not used as a bargaining chip. A warrant requirement also more closely guards against wrongful coercion and abuse and subjects the decision to appellate review.

Requiring a warrant for electronic surveillance is hardly uncharted territory. The Wiretap Act, for example, offers an instructive approach that “requires the government to meet very high standards.” Under that law, a court may issue an order authorizing electronic surveillance if it finds: (1) there is probable cause to believe that the individual is committing, has committed, or will commit an enumerated offense; (2) that no other investigative procedures are feasible; and (3) that the surveillance is conducted in a way to minimize the interception of irrelevant information. This approach is appealing not only because of the probable cause requirement but also because of the demand for proportional surveillance.

A warrant requirement also appropriately places those on probation and parole on similar footing as the arrested suspects in Riley and Carpenter. In particular, law enforcement may still search a probationer’s cell phone or rely on GPS monitoring, but they will need a warrant first. Given the availability of electronic communications with on-call trial judges, the warrant requirement does not pose an undue burden on law enforcement. As the Riley court explained, “Recent technological advances . . . have . . . made the process of obtaining a warrant itself more efficient.” Perhaps not surprisingly, since the Riley decision, there has been an uptick in warrants for cell phone searches—suggesting that obtaining a warrant is hardly a difficult hurdle to overcome.

383. See Primus, supra note 208, at 311 (2011) (“Wholly suspicionless searches, like the one upheld in Samson, should be impermissible.”); see also Friedman & Stein, supra note 128, at 351 (referring to the Samson decision as “shameful”).
384. Of course, the probable cause standard is not immune from criticism, but entrepreneurial scholars, such as Andrew Crespo, have proposed creative ways of fortifying the probable cause standard with data. See Andrew Manuel Crespo, Probable Cause Pluralism, 129 YALE L.J. (forthcoming 2020) (on file with the North Carolina Law Review).
386. See § 2518(3).
387. See, e.g., Missouri v. McNeely, 569 U.S. 141, 154 (2013) (“Well over a majority of States allow police officers or prosecutors to apply for search warrants remotely through various means, including telephonic or radio communication, electronic communication such as e-mail, and video conferencing.”).
Not only is obtaining a warrant increasingly straightforward, there may be other relevant warrant exceptions that could provide a legal basis for a cell phone search, such as exigency.

And even if expecting courts to require a warrant is unrealistic, at a minimum, courts should require some level of suspicion (either reasonable suspicion or probable cause) before subjecting someone to electronic surveillance. This approach accounts for the unique status of people on probation and parole and imposes minimal additional burdens on state actors. Additionally, it offers an important limitation on unfettered reliance on electronic surveillance.

Critics may argue that requiring a warrant or some level of suspicion means that new crimes or probation violations will go undetected. That may be true. But, as the Riley court noted, “privacy comes at a cost.” The possibility of crimes going undetected is the price to not live in an Orwellian and totalitarian society. Simply because the technological capacity to detect lawbreakers with perfect omniscience and enforcement exists does not mean that we should deploy it. It is true that if electronic search conditions were limited, a probation officer would have a more difficult time detecting a supervisee’s use of a certain word or picture on Facebook. But perhaps that potential technical violation is itself more an artifact of the move toward automated probation rather than a true indication of dangerous or otherwise criminal activity.

Additionally, requiring a higher threshold to conduct electronic surveillance does not alter the other traditional aspects of probation and parole. Even if there were a warrant requirement for electronic surveillance, people on community supervision would still be subject to physical searches, drug tests, meetings with probation officers, as well as all the other requirements that were in place—and relied on—before the advent of electronic surveillance technology. Whether these other requirements raise separate constitutional concerns is beyond the scope of this Article, but for now, those requirements provide additional avenues by which probation and parole officers may still monitor compliance.

Critics might also ask if the Fourth Amendment is even necessary if electronic surveillance is imposed as a punishment. If surveillance is truly

390. As Cynthia Lee and others have pointed out, it is unlikely that the Court will “jettison[] reasonableness as the cornerstone of its Fourth Amendment jurisprudence anytime soon.” Lee, supra note 214, at 1157.
391. See Woodrow Hartzog et al., Inefficiently Automated Law Enforcement, 2015 MICH. ST. L. REV. 1763, 1791 (“If perfect enforcement is possible, that is, an ex ante decision for zero tolerance for legal violations, the temptation to embrace perfection is strong.”).
392. Riley, 573 U.S. at 401.
imposed as part of a criminal sentence—just like imposing jail time—why must it pass Fourth Amendment muster? If other rights are diminished as part of a criminal sentence (like the right to vote, serve on a jury, or bear arms) why, then, can the government not limit privacy in the same way? The answer, at least in part, is that the Supreme Court has made it clear that the Bill of Rights limits what can be imposed in the name of “punishment.” Just as “prison[ers] are not beyond the reach of the Constitution”394 so too are those on community supervision.395 As Justice Stevens noted in his dissent in Samson, the Court has never imposed “any search as a punitive measure.”396 The justification for minimized privacy rights for those in prison, for example, is not punitive. In prison, the Court has found “[t]he curtailment of certain rights is necessary, as a practical matter, to accommodate a myriad of ‘institutional needs and objectives’ of prison facilities … chief among which is internal security.”397 Indeed, there is “nothing talismanic about labeling a search a ‘punishment’ that automatically diminishes the privacy interests of the person being searched.”398

B. **Limit Surveillance**

Requiring a warrant, or at least some level of suspicion, is a necessary but insufficient solution to the problems inherent with electronic surveillance. The other half of the solution involves two shifts in criminal policy. First, a shift away from relying on community supervision as a default sentence; and second, a shift away from relying on intensive surveillance as a necessary component of community supervision.

Simply because probation and parole exist as nonincarcерative sentences, this does not mean that they should be frequently imposed. In fact, less is often the best strategy. As other scholars have observed, community supervision results in net widening and is often imposed in cases when less intensive (or no) supervision could serve as an alternative.399 Moreover, despite the growing popularity of alternatives to incarceration, there is little empirical evidence that intensive community supervision furthers rehabilitation, reentry, or protects public safety.400

---

395. In a forthcoming article, I use electronic surveillance as a case study to examine how criminal punishment is deployed to justify limitations on otherwise constitutionally protected rights and activities. See Kate Weisburg, *Punishing Rights: The Constitutionality of Surveillance Sentences* (manuscript) (on file with author).
2020] Supervision by Surveillance 775

Given the critiques of community supervision, it should not be utilized as a presumptive sentence that is imposed instead of condition-free release.401 This view is shared by a growing number of current and former probation chiefs who recently released a joint statement calling for the reduction of probation and parole populations.402 In a related policy report, several leading probation experts called for reform focused on less intensive supervision and instead on reserving community supervision for those that truly need it.403 This same report also examined extensive data to disprove the notions that “more people have to be under criminal justice control for crime to decline” and for “prison populations to decrease.”404

Eliminating community supervision as a default sentence does not mean that low-level defendants will receive no sanction. Even without probation and parole, there remain responses to criminal conduct that further the deterrent, rehabilitative, and retributive theories of punishment. The process of facing criminal charges is in itself punitive.405 Pretrial detention, bail, administrative fees, restitution, and fine payments, as well as the burdens of attending multiple court dates, all add up to an ultimate de facto sanction. In many low-level or first-time offenses, a conviction is punishment enough, given the extensive collateral consequences of a criminal record. Even if not placed on probation or parole, defendants continue to be punished when their criminal record becomes a barrier to education, employment, and housing.406 In short, unconditional release should be considered more often.407

For the reasons detailed in this Article, the use of electronic surveillance as a tool of community supervision should be limited and proportional. While there may be a place for electronic surveillance in community supervision, it must be narrowly tailored to the specific needs of the individual and impose as little of a privacy burden as possible. Imposing surveillance in this limited way, however, requires greater understanding of how surveillance technology operates, and in particular, how it may be more precisely targeted to avoid overly invasive monitoring. It also requires “[s]trict oversight of private vendors” so as to ensure that electronic surveillance “does not become a tool for financial

401. See Horwitz, The Costs of Abusing, supra note 79, at 771 (“[A]s many as 80% of adult misdemeanor convictions result in sentences of probation.”).
403. JACOBSON ET AL., supra note 312, at 11; Scott-Hayward, supra note 86, at 460–61.
404. JACOBSON ET AL., supra note 312, at 7.
406. See generally LOVE ET AL., supra note 287, at § 1:2 (describing the range of legal collateral consequences).
407. See Klingele, supra note 317, at 1057.
enrichment of the private sector at the expense of both government and low-income individuals."408

There is also much to be learned from community organizers who have long been fighting back against the expansion of electronic surveillance in the criminal legal system. These grassroots organizations have proposed common-sense guidelines for respecting the rights of people on electronic monitors. These guidelines include increasing transparency, not using a one-size-fits-all set of rules, eliminating fees, increasing privacy protections, and ensuring due process.409 Perhaps most significantly, the guidelines also call for electronic monitoring to be the option of last resort.410 Although these guidelines focus on electronic monitoring, they could apply with equal force to any form of electronic surveillance.

As this Article sets out, electronic searches and surveillance may have reached a point in which the government "can replicate the surveillance conditions of incarceration without ever erecting a single wall."411 Therefore, electronic surveillance should be viewed for what it is both as a matter of law and as a matter of practice: punishment.412 To categorize electronic searches and surveillance as a form of punishment is not only more accurate, but also signals the need for closer judicial scrutiny, oversight, and restraint.413

CONCLUSION

Given the millions of people on some form of community supervision, the increased capacity of surveillance technology represents "a revolution of historic proportions."414 It is therefore imperative that invasive, and potentially abusive, forms of electronic surveillance be subject to constitutional scrutiny, policy analysis, and public debate.

The significance of searches "untethered" from any meaningful constitutional limitation extends beyond electronic surveillance. The emergence of suspicionless electronic searches represents a cautionary tale about the consequences of deploying "consent" and "reasonableness" to justify abusive practices that would otherwise be unconstitutional, unconscionable, or both. One could imagine a not-so-distant future when, as a matter of routine,

408. Eisenberg, supra note 37, at 173.
409. See generally LOVE ET AL., supra note 287, at § 1:2 (describing the range of legal collateral consequences).
410. Id.
412. See Eisenberg, supra note 37, at 128 (arguing that electronic GPS monitoring should be viewed as punishment).
413. See Doherty, supra note 39, at 354.
criminal defendants could be asked to “consent” to forced sterilization,\textsuperscript{415} lifetime GPS monitoring,\textsuperscript{416} forced participation in medical experiments,\textsuperscript{417} or other draconian measures. Further, the general “reasonableness” test has already been deployed by several lower courts to justify compulsory DNA profiling of people on probation and parole.\textsuperscript{418} As Judge Reinhardt noted in his dissent in one of the forced-DNA collection cases, “Privacy erodes first at the margins, but once eliminated, its protections are lost for good, and the resultant damage is rarely, if ever, undone.”\textsuperscript{419} While this Article focused on the abusive elements of electronic surveillance, these concerns about abusive tactics are not limited to electronic searches. More than ever, a new systematic and transparent approach for determining which rights can be diminished, and for whom, is needed.

\textsuperscript{415} This is not unprecedented. Courts have, in the past, upheld plea-deals requiring sterilization. See Rory Riley, Note, \textit{A Punishment That Does Not Fit the Crime: The Use of Judge-Ordered Sterilization as a Condition of Probation}, 20 QUINN. PROB. L.J. 72, 73 (2006); Sam P.K. Collins, \textit{Tennessee Prosecutor Insisted Woman Undergo Sterilization as Part of Plea Deal}, THINKPROGRESS (Mar. 30, 2015), https://thinkprogress.org/tennessee-prosecutor-insisted-woman-undergo-sterilization-as-part-of-plea-deal-
a1ad95a5e045/ [https://perma.cc/Y2JH-6K2E].

\textsuperscript{416} This practice is also not unprecedented. Although the Supreme Court in \textit{Grady} determined that lifetime GPS monitoring constitutes a search, lower courts are split on whether such a search is reasonable. See Belleau v. Wall, 811 F.3d 929, 937 (7th Cir. 2016).

\textsuperscript{417} This country has a long history of experimentation on prisoners. See Keranet Reiter, \textit{Experimentation on Prisoners: Persistent Dilemmas in Rights and Regulations}, 97 CALIF. L. REV. 501, 503 (2009).

\textsuperscript{418} See, e.g., United States v. Amerson, 483 F.3d 73, 75 (2d Cir. 2007) (holding that forced DNA collection from probationers is not unreasonable); United States v. Conley, 453 F.3d 674, 674 (6th Cir. 2006) (affirming the lower court’s holding requiring a DNA test from a bank fraud defendant); United States v. Szubelek, 402 F.3d 175, 177 (3d Cir. 2005) (“[W]e conclude that under Fourth Amendment reasonable standard for analyzing the constitutionality of government searches and seizures, the collection of DNA samples from individuals on supervised release is constitutional.”); United States v. Kincade, 379 F.3d 813, 871 (9th Cir. 2004) (Reinhardt, J., dissenting) (arguing for comprehensive DNA profiling of a defendant on supervised release).

\textsuperscript{419} \textit{Kincade}, 379 F.3d at 871 (Reinhardt, J., dissenting).