

PARADIGMS OF RESTRAINT

ERIN MURPHY[†]

ABSTRACT

Incapacitation of dangerous individuals has conventionally entailed the exercise of physical control over an actual body: the state confines the person in jail. But advances in technology have changed that convention. A variety of new technologies—such as GPS tracking bracelets, biometric scanners, online offender indexes, and DNA databases—give the government power to control dangerous persons without relying on any exertion of physical control. The government can track the location of a person in real time, receive remote notification that an individual has ingested alcohol, or electronically zone someone into a home or out of a public park. It can prove conclusively that a particular person wore a hat or took a sip from a discarded soda can, or identify a single face in a ten thousand-person crowd. In this day and age, restraint of the dangerous can be as much about keeping people out of a place as it used to be about locking them up in one.

But whereas physical incapacitation of dangerous persons has always invoked some measure of constitutional scrutiny, virtually no legal constraints circumscribe the use of its technological counterpart. Across legal doctrines, courts erroneously treat physical deprivations

Copyright © 2008 by Erin Murphy.

[†] Assistant Professor, University of California, Berkeley (Boalt Hall). I owe a debt of gratitude to Carol Steiker, who invited me to participate in the Conference on Criminal Procedure Stories at Harvard Law School at which a preliminary version of this work was given, and to Dan Richman, whose superb piece on *United States v. Salerno* first inspired me to think about these issues and who provided equally enriching comments on a subsequent draft. Thanks are also due for the generous attention given by KT Albiston, Ken Bamberger, Eric Biber, Goodwin Liu, Melissa Murray, Anne Joseph O'Connell, and Molly Van Houweling, and to my wonderful colleagues Paul Schwartz, Jonathan Simon, David Sklansky, and Frank Zimring. This work benefited tremendously from helpful comments by Chris Slobogin, Brandon Garrett, and Robert Weisberg, and by remarks made at the UCLA Junior Faculty Exchange workshop, particularly by Sharon Dolovich and Jennifer Mnookin. Finally, thanks are due to the participants in the junior criminal professor workshop hosted by Rachel Barkow, Jennifer Collins, Dan Solove, and Orin Kerr at George Washington University Law School for their contributions, and to Steven Sassaman, Ben Wolff, and Debbie Won who supplied invaluable research assistance.

as the archetypal “paradigm of restraint,” and thus largely overlook the significant threat to liberty posed by technological measures. Similarly, little academic attention has been paid to the state’s use of targeted forms of non-physical control. Much scholarly interest has focused on the increased use of physical incapacitation as a means of exerting regulatory control over, for example, illegal immigrants, pretrial detainees, or the mentally ill. And an equally vibrant debate surrounds the protection of information privacy in general society. Yet nearly no attention has been paid to the connection between these two developments.

This Article examines the generally unheeded intersection between two well-documented trends: the state’s increasing desire to preventively regulate targeted classes of individuals, and its increasing capacity to use innovative technologies, rather than physical incapacitation, to realize that desire. This Article identifies four loosely grouped emerging technologies of control: DNA databasing, electronic monitoring, electronic indexing, and biometric scanning. It then reviews the legal landscape on which they operate and demonstrates that, across the range of doctrines, courts unduly focus on the physical world as the relevant metric against which all restraints are judged. As a result, technologies of restraint are imposed without necessary procedural safeguards. This Article then outlines four concerns peculiar to these kinds of restraints and illustrates how significant concerns are wholly overlooked when the physical world is the determinant referent of comparison. The Article closes by urging greater judicial scrutiny of technological restraint and by laying out a series of potential inquiries that might aid in such an effort.

TABLE OF CONTENTS

Introduction.....	1323
I. Technologies of Control	1328
A. DNA Databasing.....	1329
B. Electronic Monitoring.....	1332
C. Electronic Indexing.....	1336
D. Biometric Scanning	1340

II.	Legal Constraints on the Regulation of the Dangerous	1345
A.	“Regulatory” versus “Punitive”.....	1347
B.	Due Process and “Liberty Interests”	1351
C.	“Reasonable Expectation of Privacy”	1358
D.	Equal Protection.....	1362
E.	Summary.....	1363
III.	Four Physics of the Nonphysical World.....	1364
A.	Proliferation	1365
B.	Accumulation.....	1376
C.	Unaccountability	1380
D.	Invisibility.....	1384
E.	Summary.....	1393
IV.	“Different Constitutional Principles”: New Paradigms of Liberty and Restraint.....	1393
A.	The Case for Constitutional Regulation.....	1394
B.	The Shape of Constitutional Regulation	1400
	Conclusion	1410

INTRODUCTION

Everybody understands, or at least has a glimmering understanding of, what it means to go to jail. Whether from popular media or personal experience, most people imagine imprisonment as the strongest and most singular instrument of state power. And who, accordingly, would not trade nearly anything to avoid incarceration? Faced with a choice between prison and house arrest, global positioning system (GPS) tracking, or even public humiliation, who would not choose any—or even all—of the latter? But reconsider that trade-off when detailed more precisely: for instance, one day in jail versus having to fill out a form at a government office downtown after every hairstyle change or car rental; one week in jail versus a lifetime of GPS tracking; or one month in jail versus never being able to reside in or visit—for any reason—any major American city. Suddenly prison may no longer seem the state’s only means of restricting liberty that merits serious consideration.

Physical incarceration has long served as the primary means of incapacitating persons found guilty of committing criminal offenses.¹

1. For an interesting history of the crime-tort distinction, see David J. Seipp, *The Distinction Between Crime and Tort in the Early Common Law*, 76 B.U. L. REV. 59, 83–87 (1996).

Not surprisingly then, it is a power checked and monitored in multifarious ways; a litany of enumerated, entrenched procedural rules circumscribes the use of incarceration as a punitive sanction for wrongdoing in the American legal system.² Of course, a criminal conviction is not the only lawful means by which the state imprisons individuals. The state also has at its disposal an array of civil measures for preventive incapacitation of “all of those whom we know (or think we know) to pose a danger of serious harm to others,”³ including

2. Before a person may be jailed for a criminal offense, the U.S. Constitution provides generally for “due process of law,” U.S. CONST. amend. V, including specific entitlements to “presentment or indictment,” *id.*, a “speedy and public trial,” an “impartial jury,” notice of the “nature and cause of the accusation,” a right to confront witnesses, compulsory process, and the assistance of counsel, *id.* amend. VI. The state cannot punish individuals for acts previously held lawful, impose duplicative penalties, *id.* amend. V, or impose sanctions considered cruel and unusual, *see id.* amend. VIII; *Bell v. Wolfish*, 441 U.S. 520, 535 & 535 n.16 (1979). The Cruel and Unusual Punishments Clause applies, as its title suggests, only to “punishments.” *Id.* at 535 n.16 (noting that the Eighth Amendment applies only after punishment is imposed, and thus concerns about the incarceration conditions of pretrial detainees are properly addressed as due process matters that ask whether the conditions have matured into “punishments” under a *Mendoza-Martinez* test). Moreover, criminal punishment can be meted out only after the government, bearing the burden of proof, overcomes the presumption of innocence and proves guilt beyond a reasonable doubt, the highest standard in the law. *In re Winship*, 397 U.S. 358, 364 (1970). Although it was not until the midcentury that many due process rights were formally incorporated against the states via the Due Process Clause, some scholars argue that incorporation had a less profound effect on states than commonly believed, because many states nonetheless provided for a range of procedural entitlements. *See, e.g.*, Kenneth Katkin, “Incorporation” of the Criminal Procedure Amendments: The View from the States, 84 NEB. L. REV. 397, 411–12 (2005) (cataloguing incorporated rights, comparing them to contemporary state constitutional practice, and concluding that “points of disagreement [were] often narrow and technical”).

3. Carol S. Steiker, *Punishment and Procedure: Punishment Theory and the Criminal-Civil Procedural Divide*, 85 GEO. L.J. 775, 819 (1997). *See generally* DAVID GARLAND, *THE CULTURE OF CONTROL* 128 (2001) (“The new criminologies tend to view crime *prospectively* and in *aggregate* terms, for the purpose of calculating risks and shaping preventative measures.”); JONATHAN SIMON, *POOR DISCIPLINE* 169 (1993) (discussing the “new control model around risk management” in parole supervision); Malcolm M. Feeley & Jonathan Simon, *The New Penology: Notes on the Emerging Strategy of Corrections and Its Implications*, 30 CRIMINOLOGY 449, 452 (1992) (describing the shift from an “old penology” founded in findings of “responsibility, fault, moral sensibility, diagnosis, or intervention and treatment of the individual offender” to a “new penology” based in efforts to “identify, classify, and manage groupings sorted by dangerousness”); Stephen J. Schulhofer, *Two Systems of Social Protection: Comments on the Civil-Criminal Distinction, with Particular Reference to Sexually Violent Predator Laws*, 7 J. CONTEMP. LEGAL ISSUES 69, 81–82 (1996) (analyzing and advocating for a distinction between civil and criminal processes); Christopher Slobogin, *The Civilization of the Criminal Law*, 58 VAND. L. REV. 121 (2005) [hereinafter Slobogin, *Civilization*] (arguing in favor of a shift from the corrective to the preventive model of criminal law); Christopher Slobogin, *Dangerousness and Expertise Redux*, 56 EMORY L.J. 275 (2006) (discussing the merits of predictive calculations of danger).

commitment of the mentally ill,⁴ certain illegal immigrants,⁵ pretrial defendants,⁶ violent sexual predators,⁷ and terrorist suspects.⁸ Although fewer rules circumscribe the “civil” or “regulatory” forms of physical incapacitation,⁹ in many cases the standards closely approximate those required for penal sanctions.

But if penal incapacitation constitutes the first system of social protection and civil regulatory incapacitation the second,¹⁰ then a third system is emerging—the preventive state has become a technological one. The dawn of the twenty-first century witnessed an explosion in technologies such as GPS tracking bracelets, biometric scanners, online offender indexes, and DNA databases—all adopted as a means of controlling and regulating a particular subset of the population without exerting physical control. Technology permits the government to physically track large numbers of persons in real

4. See *Addington v. Texas*, 441 U.S. 418, 428 (1979) (upholding a civil commitment statute and noting that the reasonable doubt standard is not constitutionally required).

5. The Supreme Court initially rejected the constitutionality of detaining all deportable aliens. See *Zadvydas v. Davis*, 533 U.S. 678, 690 (2001) (“A statute permitting indefinite detention of an alien would raise a serious constitutional problem.”). The Court, however, then upheld detention of a limited class of aliens without requiring individualized determinations of dangerousness. See *Demore v. Kim*, 538 U.S. 510, 557–58 (2003) (“Detention is not limited to dangerous criminal aliens or those found likely to flee, but applies to all aliens claimed to be deportable for criminal convictions, even where the underlying offenses are minor.”).

6. See, e.g., *United States v. Salerno*, 481 U.S. 739, 755 (1987) (upholding an act that allowed for the pretrial detention of “arrestees charged with serious felonies who are found after an adversary hearing to pose a threat to the safety of individuals or to the community”).

7. See, e.g., *Kansas v. Hendricks*, 521 U.S. 346, 368–69 (1997) (“When the State has ‘disavowed any punitive intent’; limited confinement to a small segment of particularly dangerous individuals; provided strict procedural safeguards; afforded the same status as others who have been civilly committed; recommended treatment if such is possible; and permitted immediate release upon a showing that the individual is no longer dangerous or mentally impaired, we cannot say that it acted with punitive intent.”).

8. See, e.g., *Hamdi v. Rumsfeld*, 542 U.S. 507, 509 (2004) (plurality opinion) (allowing detention of a citizen captured on foreign soil based on less than that which should be required for the pretrial detention of a criminal defendant).

9. See, e.g., Schulhofer, *supra* note 3, at 70–78 (describing different ways in which states have authorized the indefinite civil confinement of mentally ill and dangerous individuals upon fewer procedural protections than that required for criminal confinement); cf. Franklin E. Zimring, *The Multiple Middlegrounds Between Civil and Criminal Law*, 101 YALE L.J. 1901, 1903 (1992) (“Heightened protection in civil cases usually occurs in situations that involve the risk of secure confinement, such as juvenile court delinquency jurisdiction and involuntary civil commitment under the mental health powers, or the loss of personal associations, such as child custody.”).

10. Schulhofer, *supra* note 3, at 80.

time;¹¹ to prove conclusively which person wore a hat or took a sip from a discarded soda can;¹² to electronically zone an individual into or out of designated spaces,¹³ or perhaps even to isolate and identify a single face in a ten thousand-person crowd.¹⁴ Regulation of the dangerous, in a technologically advanced society, has become as much about keeping a person out of a place as it used to be about locking a person up in one.

But whereas a rich debate explores the potential for abuse of physical incapacitation, whether as a matter of criminal sanction or “regulatory” control,¹⁵ a corresponding dialogue surrounding the risks posed by nonphysical, technology-based means of control is conspicuously lacking. Essentially no legal structures superintend the use of noncorporeal means of incapacitation, even though their use raises many of the concerns manifest in the use of physical restraints, and even as the advent of technological alternatives has diminished the government’s need to rely on conventional forms of incapacitation.

The purpose of this Article is to examine the generally unheeded intersection of two well-documented trends: the state’s increasing desire to preventively regulate specified individuals and its increasing ability to use innovative technologies, rather than physical incapacitation, to realize that desire. Many scholars have observed that the government and private entities routinely collect and store

11. See, e.g., *United States v. Moran*, 349 F. Supp. 2d 425, 467–68 (N.D.N.Y. 2005) (upholding the warrantless use of GPS tracking devices).

12. See, e.g., *State v. Piro*, 112 P.3d 831, 834 (Idaho Ct. App. 2005) (upholding the DNA testing of a water bottle retained by officers after defendant was offered a drink while in custody).

13. See, e.g., Cara Buckley, *New York Plans Surveillance Veil for Downtown*, N.Y. TIMES, July 9, 2007, at A1 (describing a New York City plan to install cameras linked to license plate databases that could trigger barriers if cars banned from the area passed nearby).

14. See, e.g., *Eyeticor v. Unisys Corp.*, 155 F. Supp. 2d 527, 532–34 (E.D. Va. 2001) (describing potential uses of iris scanning technology); *People v. Johnson*, 43 Cal. Rptr. 3d 587, 597–98 (Cal. Ct. App. 2006) (discussing potential uses of facial recognition software); David Lamb, *One Last City is Scanning for Faces in the Crowd*, L.A. TIMES, Sept. 29, 2003, at A10 (reporting that Virginia Beach continues to use facial-recognition systems to scan for terrorists, felons with outstanding warrants, and missing children).

15. Compare Schulhofer, *supra* note 3, at 96 (arguing that civil commitment should serve only as a “gap-filler, to solve problems that the criminal process cannot address”), with Slobogin, *Civilization*, *supra* note 3, at 165 (arguing for a “preventive regime” of criminal law that would collapse the “artificial distinctions between civil and criminal dispositions” in appropriate cases).

large quantities of data about individuals in society.¹⁶ But none have focused on the concerns unique to the use of technological means of exercising control over *specified* persons or populations, in particular those deemed by the state to be “dangerous,”¹⁷ in order to regulate or control them. That is, this Article does not concentrate on “open systems” of technological surveillance that monitor generally or indiscriminately without focusing *ab initio* on particular suspects.¹⁸ Rather, this Article is concerned with “closed system[s]” of surveillance” that either specifically target a particular subject or else operate indiscriminately but with reference to “a relevant archive that can be searched.”¹⁹ In short, this Article focuses not on the intersection camera that catches anyone running a red light but rather on the intersection camera connected to a database of felon license plates that isolates and identifies only those particular cars.²⁰

In this respect, the literature surrounding general issues of privacy with regard to new technologies places into sharper relief the issues that nonphysical forms of surveillance and control bring to the fore. At the same time, the literature surrounding regulatory

16. See generally Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815 (2000) (arguing for more nuanced regulations of Internet privacy); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999) (detailing the extent to which personal information is collected online and proposing rules for fair practice); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002) (noting myriad ways in which the government can gather information without suspicion) [hereinafter Solove, *Digital Dossiers*]; Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001) (reconceptualizing the problem of Internet privacy in power and dignity terms rather than in embarrassment or self-censorship terms).

17. In particular, my concern is with the “reconfiguration of the practices that we most associate with disciplinary society—that is, panoptic surveillance aimed at intervening in the social world to provide an effective treatment for defective behaviour . . . to a type of surveillance which is essentially concerned with the ‘management’ of those already deemed criminal.” Robin Williams & Paul Johnson, *Circuits of Surveillance*, 2 SURVEILLANCE & SOC’Y 1, 11 (2004).

18. *Id.* at 5.

19. *Id.*

20. Many technologies indiscriminately amass or collate information—it is estimated, for example, that over five hundred thousand cameras monitor the streets of London, and one study suggested that a single person is filmed roughly three hundred times a day. Steve Stecklow, Jason Singer & Aaron O. Patrick, *Watch on the Thames: Surveillance Cameras Monitor Much of Daily Life in London, May Help Identify Bombers*, WALL ST. J., July 8, 2005, at B1. Such “open system” forms of technological surveillance monitor generally or indiscriminately, without focusing on particular suspects. Williams & Johnson, *supra* note 17, at 5. The emphasis of this article, however, is on “closed systems” that target suspects individually or by identifiable class.

incapacitation and the preventive state helps to refract those general concerns through the specific lens of state power when exercised outside the realm of formal criminal process.²¹

To be clear, this Article does not claim that nonphysical restraints are necessarily, or even ever, as severe an incursion into liberty as is full-fledged incarceration. It is difficult to imagine that even the most assiduous constellation of technological restraints, imposed under the same standards and for the same duration of time, could ever effectuate a deprivation of liberty equal to that caused by imprisonment. Rather, this Article essentially asks, if the government can replicate the surveillance conditions of incarceration without ever erecting a single wall, what procedures ought to govern the operation of these virtual prisons?

I proceed as follows. Part I provides a general sketch of a range of operable or plausible surveillance technologies that exercise control over allegedly dangerous persons or classes of persons. This Part claims neither to be comprehensive nor exhaustive, but rather sets up the canvas on which the concerns identified in the rest of this Article are drawn. Part II then maps the legal landscape surrounding the use of these technologies. It demonstrates that these technological restraints tend to evade serious procedural scrutiny of any kind and instead fall far off the constitutional radar. Part III argues that the unfettered operation of technological restraints raises grave concerns that are all too easily obscured by the dominant referent of physical incapacitation, the paradigmatic form of restraint. The final Part urges a richer understanding of the interests that technological regulations place in jeopardy and proposes the development of new legal constructs to regulate their use.

I. TECHNOLOGIES OF CONTROL

*Any sufficiently advanced technology is indistinguishable from magic.*²²

21. See generally Symposium, *The Civil-Criminal Distinction*, 7 J. CONTEMP. LEGAL ISSUES 1 (1996) (surveying the robustness of the civil-criminal distinction both as a descriptive and normative matter). A substantial literature also addresses punitive civil sanctions and explores the theoretical bases for distinguishing between civil and criminal penalties. E.g., Kenneth Mann, *Punitive Civil Sanctions: The Middleground Between Criminal and Civil Law*, 101 YALE L.J. 1795, 1844–61 (1992).

22. ARTHUR C. CLARKE, PROFILES OF THE FUTURE 21 n.1 (1973) (emphasis added).

A range of new technologies has greatly enhanced the state's ability to monitor large numbers of individuals. With the advent of surveillance methods less costly than physical restraint, the standard binary of incarceration and liberty has unfurled into a broad continuum on which those two choices mark only the extremes. This Part introduces four loosely grouped forms of technological surveillance and illustrates the ways in which law enforcement uses them to monitor or control allegedly dangerous persons. Rather than present an exhaustive catalog of restraints, or even a typology of such mechanisms, this Part aims mainly to sketch the varied terrain on which such methods operate. Specifically, this Part discusses DNA databasing, electronic location monitoring, online indexing, and biometric scanning and zoning restrictions.

A. DNA Databasing

The collection and retention of forensic DNA samples became commonplace in the mid-1990s.²³ The government routinely collects biological material from a variety of individuals and then tests, types, and uploads that information to state and national databases.²⁴ Most databases retain the typed genetic information indefinitely; currently no state provides for deletion of an otherwise lawfully retained sample.²⁵ All but one state, Wisconsin, also permit indefinite retention of the actual physical sample, which contains the individual's entire genetic code.²⁶

Initially, most mandatory DNA collection statutes applied only to those convicted of sexual offenses or violent felonies.²⁷ Then legislatures started extending the mandate to include all those convicted of any felony.²⁸ Next came statutes that required collection of DNA from all convicted persons, whether felons or

23. JOHN M. BUTLER, *FORENSIC DNA TYPING* 11–12 (2d ed. 2005) (charting timeline of forensic DNA development).

24. *Id.* at 440–41.

25. R.E. Gaensslen, *Should Biological Evidence or DNA Be Retained By Forensic Science Laboratories After Profiling? No, Except Under Narrow Legislatively-Stipulated Conditions*, 34 J.L. MED. & ETHICS 375, 376–77 (2006). Some states do require discarding of the genetic sample or removal of the digital profile if a conviction is expunged or overturned. *Id.* at 377.

26. *Id.*

27. See Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 CAL. L. REV. 721, 738 n.73 (2007).

28. BUTLER, *supra* note 23, at 438.

misdemeanants.²⁹ As of 2008, all fifty states, as well as the federal government, require the submission of DNA samples from convicted offenders according to a variety of categorical distinctions.³⁰ The federal government and seven states—California, Kansas, Louisiana, Minnesota, New Mexico, Texas, and Virginia—also require samples from arrestees,³¹ and other states have considered following suit.³² The federal government has also begun collecting DNA samples from detained illegal immigrants.³³ Although no such statutes exist, it is not difficult to imagine the passage of legislation requiring the collection of DNA samples from mentally ill persons or other such individuals—not on the basis of being arrested or convicted of a crime, but rather as a result of simply being labeled “dangerous.”

As collection standards have broadened, the databases have responded in kind. Initially, the federal government narrowly circumscribed the range of material eligible to be “uploaded” into the national database, providing among other things a statutory limit that restricted the database to convicted offenders. Congress then changed this requirement by enacting legislation to authorize the inclusion of any sample collected according to state law.³⁴ The federal database now contains the genetic profiles of 3.3 million offenders, and it is reportedly growing by roughly 80,000 individuals per month.³⁵

These growing databases are in turn powerful investigative tools. Using a database, law enforcement can make associations between known individuals and evidence collected at a scene, and among evidence in different cases with no known suspects. Creative innovations in DNA searching, along with rule changes initiated by

29. *Id.*

30. *Id.* (noting that some states limit collection to those convicted of specified sex offenses or violent crimes).

31. See 42 U.S.C. § 14132 (2000); CAL. PENAL CODE § 296 (West 2008); KAN. STAT. ANN. § 21-2511(e) (2006); LA. REV. STAT. ANN. § 15:609(A)(1) (2007); MINN. STAT. ANN. § 299C.105 (West 2007); N.M. STAT. § 29-3-10(A) (2007); TEX. GOV'T CODE ANN. § 411.1471 (Vernon 2007); VA. CODE ANN. § 19.2-310.2:1 (2007).

32. See, e.g., H.B. 4092, 94th Leg., 1st Reg. Sess. (Mich. 2007); A.B. 4108, 212th Leg., 2d Reg. Sess. (N.J. 2006); H.B. 779, 94th Gen. Assem., Reg. Sess. (Ill. 2005); S.B. 746, Gen. Assem., 2005 Sess. 2005 (N.C. 2005).

33. See 42 U.S.C.A. § 14135a(a)(1)(A) (West 2008); Julia Preston, *U.S. Set to Begin a Vast Expansion of DNA Sampling*, N.Y. TIMES, Feb. 5, 2007, at A1.

34. DNA Fingerprint Act of 2005, Pub. L. No. 109-162, tit. X, § 1002(1), 119 Stat. 2960 (codified at 42 U.S.C.A. § 14132(a)(1)(C) (West 2008)).

35. Rick Weiss, *Vast DNA Bank Pits Policing Vs. Privacy: Data Stored on 3 Million Americans*, WASH. POST, June 3, 2006, at A1.

the federal government, permit DNA-database searches aimed at finding nondatabased suspects via the profiles of relatives contained in the database,³⁶ or even to determine a likely surname given a particular genetic profile.³⁷ Cases in which the suspect was identified through a “trawl” of the database, and thus the only evidence is DNA evidence, have increasingly percolated in the courts; most courts have upheld such convictions as constitutional.³⁸

Notably, each of these provisions for mandatory collection applies categorically. None requires any findings of particularized need for collection—the onetime felonious bad-check writer convicted forty years ago must provide a sample alongside the incorrigible rapist. Moreover, most impose no limit on the retention of either the sample or profile; both can stay in the government’s possession even beyond the lifespan of the contributor.

Nearly every state court has endorsed DNA collection from convicted offenders.³⁹ Although the circuits have split on precisely which legal rubric should be applied, with some applying the “special needs” test and others using a general balancing inquiry,⁴⁰ every federal court to consider the issue has upheld contribution requirements.⁴¹ Arrestee statutes, which are of recent vintage, have yet to be aired fully as legal challenges.⁴² But by many accounts, the

36. Frederick H. Bieber, Charles H. Brenner & David Lazer, *Finding Criminals Through DNA of Their Relatives*, 312 SCIENCE 1315–16 (2006); Henry T. Greely et al., *Family Ties: The Use of DNA Offender Databases to Catch Offender’s Kin*, 34 J.L. MED. & ETHICS 248, 250 (2006).

37. Pilar N. Ossorio, *About Face: Forensic Genetic Testing for Race and Visible Traits*, 34 J.L. MED. & ETHICS 277, 278, 283 (2006).

38. See, e.g., *People v. Rush*, 672 N.Y.S.2d 362, 364 (App. Div. 2000); *Roberson v. Texas*, 16 S.W.3d 156, 172 (Tex. Ct. App. 2000).

39. See Ron Scherer, *Should DNA Be Collected from All Criminals?*, CHRISTIAN SCI. MONITOR, May 19, 2006, at 1, available at <http://www.csmonitor.com/2006/0519/p01s02-usju.html#> (outlining the breadth of collection in different states). But see *State v. Watkins*, Nos. 6805-12-04 et al., slip op. at 16–17 (Vt. Dist. Ct. Apr. 24, 2006) (holding that the state statute that allows DNA collection from nonviolent convicted felons violates the state constitution).

40. See *Nicholas v. Goord*, 430 F.3d 652, 658–59 (2d Cir. 2005) (summarizing such cases).

41. *Id.*

42. In the few instances where courts have considered these statutes, they have split on whether to uphold them. See, e.g., *In re Welfare of C.T.L.*, 722 N.W.2d 484, 491–92 (Minn. Ct. App. 2006) (holding that DNA collection from arrestees violates the Minnesota and U.S. constitutions); *Anderson v. Commonwealth*, 650 S.E.2d 702, 705 (Va. 2007) (likening DNA collection to fingerprinting and upholding a statute requiring DNA collection from persons arrested for certain offenses); see also, e.g., *State v. McKinney*, 730 N.W.2d 74, 87 (Neb. 2007) (allowing collection of a DNA sample upon a showing of probable cause that the individual

reasoning used to uphold convicted felon statutes applies equally to arrestees. As Judge Kozinski observed, dissenting in the Ninth Circuit case upholding the federal collection statute:

if the reason for taking [the defendant's] DNA while he's on supervised release is that it will help solve crimes later, it seems equally justifiable to take his blood after he comes off supervised release. . . . Which brings us to the people we really need to worry about, namely you and me. If collecting DNA fingerprints can be justified on the basis of the plurality's multi-factor, gestalt high-wire act, then it's hard to see how we can keep the database from expanding to include everybody.⁴³

Moreover, courts have routinely upheld collection of “abandoned” DNA evidence⁴⁴ and even surreptitious police methods of collection.⁴⁵ Thus, the constitutionality of arrestee statutes may have minimal impact if law enforcement officers may compose a list of “suspicious persons” and evade legal regulation by simply sending out mail-in prize-claim forms or sifting through the dumpster at Taco Bell.

B. Electronic Monitoring

Technologies for electronically tracking individuals fall into two general categories: electronic location monitors and chemical substance monitors. These technologies are most popularly used within the criminal justice system as a form of enhanced surveillance during probation or parole. But attention has increasingly turned to using these technologies outside of the formal criminal process.

Individual location monitoring programs vary greatly in the details—including how the systems operate, what class of individuals

committed the crime for which the DNA was sought, but rejecting the use of DNA when the DNA is not related to the probable cause).

43. *United States v. Kincade*, 379 F.3d 813, 872 (9th Cir. 2004) (en banc) (Kozinski, J., dissenting).

44. *See, e.g.,* *Murphy*, *supra* note 27, at 736.

45. Several news accounts describe a variety of methods of obtaining DNA, including taking samples of saliva after the suspect spit on the ground and sampling utensils and a glass after the suspect ate out with his wife. Richard Willing, *Police Dupe Suspects into Giving up DNA*, USA TODAY, Sept. 11, 2003, at A3; Carolyn Thompson, *Police DNA Collection Sparks Questions*, BOSTON.COM, Mar. 17, 2007, http://www.boston.com/news/science/articles/2007/03/17/police_get_creative_in_collecting_dna. At least one court has upheld such collection techniques in a case in which police officers posed as attorneys seeking information and took a sample of the saliva used by the suspect to close an envelope. *State v. Athan*, 158 P.3d 27, 31 (Wash. 2007).

they cover, and how long the monitoring remains in place. Some devices rely on transmitters that only relay whether the individual is within range of a preestablished point.⁴⁶ Active GPS systems relate the most precise information, including the exact location of the offender, whether through passive recordings that can later be reviewed or through active observation of real-time activities.⁴⁷

At least seventeen states have statutes in place that authorize some form of electronic location tracking for sexual offenders on supervised release.⁴⁸ Other states have pursued implementation of such programs through either legislative enactments or executive orders.⁴⁹ These provisions, like DNA-collection statutes, tend to be drawn on broad categorical grounds—such as specific classes of prior offenders—that provide for no individualized determination of dangerousness or likely recidivism. They apply equally to the sex offender in hospice care as to the predator on the street. Many of these statutes apply retroactively, so that an offender convicted years ago and long since disentangled from the criminal justice system must suddenly resume supervision via an electronic device.⁵⁰

The use of location tracking has in two respects already expanded beyond simple regulation of sexual offenders on formal release. First, tracking requirements no longer remain confined to imposition during periods of formal court or parole supervision. That is, several jurisdictions impose a lifetime monitoring requirement on

46. Cecil E. Greek, *Tracking Probationers in Space and Time: The Convergence of GIS and GPS Systems*, 66 FED. PROBATION 51, 51 (2002).

47. See, e.g., *Chism v. State*, 824 N.E.2d 334, 335 (Ind. 2005); Megan A. Janicki, *Better Seen than Heard: Residency Restrictions and Global Positioning Tracking Laws for Sex Offenders*, 16 B.U. PUB. INT. L.J. 285, 295–96 (2007).

48. These states include Alabama, Arizona, Arkansas, Colorado, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Michigan, Missouri, Oklahoma, South Carolina, Virginia, Washington, and Wisconsin. See ALA. CODE § 15-20-26.1 (LexisNexis 2007); ARIZ. REV. STAT. ANN. § 13-902(G) (2007); ARK. CODE ANN. § 12-12-923 (2007); COLO. REV. STAT. § 18-1.3-1005 et seq. (2007); FL. STAT. ANN. § 947.1405 (West 2008); GA. CODE ANN. § 42-1-14 (2007); 730 ILL. COMP. STAT. 5/5-8A-6 (2007); IND. CODE ANN. § 35-38-2.5-3 (LexisNexis 2007); IOWA CODE ANN. § 692A.4A (West 2007); KAN. STAT. ANN. § 74-9101(15) (2006); MICH. COMP. LAWS ANN. § 791.285 (West 2007); MO. REV. STAT. § 217.735 (West 2007); OKLA. STAT. tit. 57, § 510.10 (2008); S.C. CODE ANN. § 23-3-540 (2007); VA. CODE ANN. § 37.2-908(E) (2007); WASH. REV. CODE ANN. § 9.95.435 (West 2007); WIS. STAT. ANN. § 301.135 (West 2007).

49. For instance, California, Idaho, Minnesota, Montana, and North Dakota all apparently engage in some form of electronic monitoring, and Connecticut, Louisiana, Massachusetts, New Jersey, and Tennessee each have initiated pilot programs. New Hampshire, North Carolina, Rhode Island, and South Dakota are all considering legislation.

50. Bret R. Hobson, *Banishing Acts: How Far May States Go to Keep Convicted Offenders Away from Children?*, 40 GA. L. REV. 961, 964 & nn.21–22 (2006).

designated persons, either through independent statutory mandates or as a condition of specially concocted mandatory lifetime supervision terms.⁵¹

Second, the categories of persons subject to tracking requirements include persons other than just sex offenders. San Bernardino County, California, initiated a pilot project using GPS tracking to monitor alleged gang members on supervised release.⁵² Connecticut announced a program to fit all parolees on release for specified burglaries with GPS tracking devices.⁵³ Another jurisdiction is contemplating a bill to require tracking and registration of persons never convicted but who instead were declared sex offenders according to civil proceedings with lesser evidentiary and proof standards than that required for criminal conviction.⁵⁴ It is not difficult to imagine a legislature writing laws applying these devices to other purportedly high recidivist classes like drug dealers, prostitutes, perpetrators of domestic violence, or drunk drivers.

In fact, another technology is already available to address one of these categories—drunk drivers. In 2003, a private company first made available the secure continuous remote alcohol monitor (SCRAM), a bewitching device that attaches to the ankle and purports to test the alcohol concentration levels in natural daily perspiration on an hourly basis.⁵⁵ The device date- and time-stamps the data and stores it for transmission—typically to a probation officer—via the home phone of the individual.⁵⁶ Jurisdictions have

51. See, e.g., GA. CODE ANN. § 42-1-14 (2007); MICH. COMP. LAWS ANN. § 791.285 (West 2007); MO. ANN. STAT. § 217.735 (West 2007).

52. Press Release, Cal. Dep't of Corr. & Rehab., California Department of Corrections and Rehabilitation Announces GPS Partnership with the City of San Bernardino to Monitor High-Risk Gang Activity (Mar. 15, 2006), available at http://www.cdcr.ca.gov/News/2006_Press_Releases/press20060314.html.

53. Associated Press, *Paroled Burglars To Be Fitted with GPS Tracking Devices*, BOSTON.COM, Aug. 12, 2007, http://www.boston.com/news/local/connecticut/articles/2007/08/12/paroled_burglars_to_be_fitted_with_gps_tracking_devices/.

54. Blade Columbus Bureau, *Plan Gains to Publicly Identify Accused: Ohio Panel Backs Registry Proposal*, TOLEDO BLADE, Aug. 29, 2006, <http://www.toledoblade.com/apps/pbcs.dll/article?AID=/20060829/NEWS24/608290360/-1/NEWS>.

55. Alcohol Monitoring Systems, *The SCRAM Bracelet*, <http://alcoholmonitoring.com/index/scram/what-is-scram/scram-bracelet> (last visited Apr. 6, 2008).

56. *Id.* According to one report, the device is so sensitive that offenders are instructed not to wear cologne, rinse with mouthwash, or use any other products containing alcohol. *Keeping Watch: New Device Helping Court Monitor Those on Probation*, TIMES REP. (Dover-New Philadelphia, Ohio), Sept. 6, 2005, http://alcoholmonitoring.com/ams_files/pdf_articles/2005/090605_timesreporter.pdf.

adopted the devices to monitor offenders on release, especially those who have incurred multiple driving under the influence convictions.⁵⁷ According to company promotional materials, SCRAM programs are in place in “44 states and more than 1,500 courts and agencies, with SCRAM monitoring more than 50,000 alcohol offenders.”⁵⁸ Again, although this technology is commonly used for offenders under formal criminal supervision, it is easy to imagine the imposition of lifetime monitoring requirements on habitual drunk drivers or those prone to alcohol-related violence. Indeed, celebrity Lindsay Lohan voluntarily wore one as a means of “demonstrat[ing] her commitment to sobriety” after a DUI arrest.⁵⁹

Unlike challenges to DNA collection and online registration acts, challenges to requirements to wear electronic monitors do not appear to have yet been fully litigated. As the next Part explains, however, the Court’s reasoning with regard to sexual predator commitment statutes⁶⁰ and sexual offender registration acts⁶¹ gives some indication that such programs would likely withstand constitutional challenge on the grounds that they impinge on no cognizable “liberty interest” or

57. See, e.g., Tony Bizjak, *Bracelet Monitors Human Drunkenness*, SACRAMENTO BEE, Sept. 23, 2006, at 2 (reporting on the use of the device and on a California Assembly bill that urges the county to consider using bracelets); Associated Press, *N.C. Courts Test Alcohol-Detecting Bracelet*, WINSTON-SALEM J., July 22, 2005, http://alcoholmonitoring.com/ams_files/pdf_articles/2005/072205_winstonsalemjournal.pdf.

58. Alcohol Monitoring Systems, About Alcohol Monitoring Systems, <http://www.alcoholmonitoring.com/about/index.html> (last visited Apr. 6, 2008). There are also mobile drug-detection scanners that purport to reveal traces of illegal substances. See, e.g., Smiths Detection, http://www.smithsdetection.com/eng/narcotics_detection.php (last visited Apr. 6, 2008) (listing devices). Such devices have become increasingly popular as a means of screening visitors to prison facilities. See, e.g., Press Release, Commonwealth of Pa. Dep’t of Corr., National Study Reveals Ridge Administration Crackdown Has Made Pennsylvania Prisons Nearly 99 Percent Drug Free (Jan. 22, 1999), available at <http://www.correctionsdrugtesting.com/pennstudy.htm> (detailing efficacy of three ion scanners, among other tools, in lowering rates of drug use in Pennsylvania correctional facilities); Associated Press, *Devices Linked to Decreased Drug Use in Tucson Area Prisons*, ARIZ. DAILY, Mar. 6, 2001, http://wc.arizona.edu/papers/94/113/01_92_m.html.

59. See Joshua Zumbrun, *Celebs Put Their Best Foot Forward*, WASH. POST, July 18, 2007, at C1.

60. See discussion *infra* Part II; see also *Seling v. Young*, 531 U.S. 250, 267 (2001) (finding a sexual predator commitment statute “civil” and thus upholding it against ex post facto and double jeopardy challenges); *Kansas v. Hendricks*, 521 U.S. 346, 350 (1997) (upholding commitment of a sexual predator against due process challenge). *But see* *Kansas v. Crane*, 534 U.S. 407, 409 (2002) (finding a constitutional requirement that there be some inability to control behavior before civil commitment of sexual predator).

61. See discussion *infra* Part II; *Smith v. Doe*, 538 U.S. 84, 105–06 (2003); *Conn. Dep’t of Pub. Safety v. Doe*, 538 U.S. 1, 4 (2003).

suspect class. Moreover, routine drug and alcohol monitoring, typically done by collecting urine specimens, is familiar in the criminal adjudicatory process.⁶² As of yet, there have been only limited efforts to undertake broad, categorical testing outside the strictures of the criminal justice processes⁶³—such as testing of high school students⁶⁴ and employees in sensitive positions.⁶⁵ Given that courts have largely upheld those efforts, however, it is not difficult to imagine that courts might view a similar intrusion as lawful against a status population like former felons, habitual drunk drivers, or domestic abusers.

C. *Electronic Indexing*

A third, increasingly popular tool for regulating “dangerous” persons is the creation and publication of indexes of such persons. The most common type of online index is the sex offender registry, which swept the nation in the wake of federal legislation that reduced grant funding to states without such mandatory registration statutes.⁶⁶ Every state has such an act, and in July 2006, Congress passed and President Bush signed into law a bill authorizing the creation of a national federal database of convicted sex offenders.⁶⁷ Although the statutes vary in specific terms, all require online publication of certain sex offenders’ biographical information and charge of conviction.⁶⁸

62. SIMON, *supra* note 3, at 170–71.

63. Of course, wide latitude has long been granted such monitoring with regard to conditional releases like probationers and parolees. *See* Samson v. California, 126 S. Ct. 2193, 2196 (2006) (upholding the random, suspicionless search of a parolee).

64. *See, e.g.*, Bd. of Educ. v. Earls, 536 U.S. 822, 825 (2002) (upholding the random, suspicionless drug testing of students involved in extracurricular activities); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 665–66 (1995) (upholding the random, suspicionless testing of school athletes); New Jersey v. T.L.O., 469 U.S. 325, 328–29 (1985) (upholding the warrantless search of student purses).

65. *See, e.g.*, Nat’l Treasury Employees Union v. Von Raab, 489 U.S. 656, 677 (1989) (upholding drug testing of customs employees); Skinner v. Ry. Labor Executives’ Ass’n, 489 U.S. 602, 634–35 (1989) (upholding drug testing of railway employees involved in accidents).

66. Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Program, 42 U.S.C. § 14071 (2000) (reducing federal grants to states that fail to enact registration statutes).

67. Adam Walsh Child Protection and Safety Act of 2006, Pub. L. No. 109-248, 120 Stat. 587 (to be codified in scattered sections of 18 and 42 U.S.C.) (creating a national database and also granting money for GPS tracking programs).

68. *See* FBI, U.S. Dep’t of Justice, National/State Sex Offender Registry, <http://www.fbi.gov/hq/cid/cac/registry.htm> (last visited Apr. 6, 2008) (including links to all states’ sites, as well as the national registry); Klaaskids—Megan’s Law Legislation in All 50 States,

Most websites publicly display a home and work address, date of birth, physical characteristics, or other identifying information.⁶⁹ There are also websites that allow an individual to input an address, which in turn generates a map of nearby listed offenders.⁷⁰ Four states have also passed laws requiring real estate agents to provide information on sex offender registries to all homebuyers.⁷¹

Like DNA collection statutes, electronic monitoring requirements tend to be triggered by broad categorical classifications based on prior conviction without regard to present status within the criminal justice system.⁷² Most statutes impose on individuals the obligation to submit regular updates to the government—typically every ninety days—and to actively notify the registry if they relocate, use automobiles not registered to them, or change their appearance in any way.⁷³ These data collection and dissemination provisions apply without regard to any term of supervision or formal entanglement with criminal process, and some require registration and regular updating for the entire lifetime of the individual.⁷⁴ One Ohio legislative panel even moved to enact a law that requires registration of persons alleged to have propensities toward sex offenses, even if the individual has never been convicted of a crime.⁷⁵

These statutes have largely withstood legal challenges of various kinds in state and federal courts. In 2003, the Supreme Court

<http://www.klaaskids.org/pg-legmeg.htm> (last visited Apr. 6, 2008); *see also* DEVON B. ADAMS, U.S. DEP'T OF JUSTICE, SUMMARY OF STATE SEX OFFENDER REGISTRIES, 2001, at 1, 3 (2002), available at <http://www.ojp.usdoj.gov/bjs/pub/pdf/sssor01.pdf> (detailing the development of and information available on state sex offender registries). Since issuance of this 2001 report, the twenty-one states that did not have public online registries have launched such sites.

69. *See, e.g.*, Delaware Sex Offender Central Registry, <http://sexoffender.dsp.delaware.gov> (last visited Apr. 6, 2008); Oregon Sex Offender Inquiry System, <http://sexoffenders.oregon.gov> (last visited Apr. 6, 2008).

70. *See, e.g.*, National Sex Offender Registry, <http://www.familywatchdog.us> (last visited Apr. 6, 2008). On many websites, the user can input an address and then see a map with small flags designating the location of nearby offenders. Clicking on the flags then reveals the offender's photo, name, and address, as well as a hyperlink to the sex offender registry site for the state.

71. *E.g.*, CAL. CIVIL CODE § 2079.10a (West 2008). One major real estate search engine added sex offender registries to its online search terms. Press Release, PropertyMaps.com, PropertyMaps.com Adds Sex Offender Registries to Real Estate Search (July 26, 2007), available at http://www.propertymaps.com/corporate/press/media/2007_07_26_a.pdf.

72. Of course, DNA databases are in fact a form of electronic indexes of "dangerous" persons.

73. *See, e.g.*, *Smith v. Doe*, 538 U.S. 84, 89–91, 101–02 (2003).

74. *See id.* at 90.

75. *Blade Columbus Bureau, supra* note 54.

examined both the onerous Alaska Sex Offender Registration Act⁷⁶ and the Connecticut registration act⁷⁷ in light of claims that such enactments violated the procedural component of the Due Process Clause and the Ex Post Facto Clause. The Court upheld the statutes in both cases.⁷⁸ State courts have proven equally receptive toward such statutes,⁷⁹ although some have made efforts to narrow their reach.⁸⁰

The story of indexing, similar to that of other technological restraints, does not stop with its deployment against sex offenders. The New York City Council passed the Gun Offender Registration Act,⁸¹ modeled on sex offender acts, which requires individuals convicted of a gun offense to register for four years.⁸² Like the sex offender registries on which it was modeled, the Act requires eligible persons to submit personal information and a photograph and to appear in person to update or confirm such information every six months or within ten days of changing residences.⁸³ Other jurisdictions have expressed interest in creating registries of alleged gang members⁸⁴ or those convicted of making or selling methamphetamine⁸⁵ or operating illegal drug laboratories.⁸⁶

Online indexes are not limited just to official registries. Many jurisdictions, no doubt in response to the proliferation of online private companies that offer online instant background checks for an

76. *Smith*, 538 U.S. at 89.

77. *Conn. Dep't of Pub. Safety v. Doe*, 538 U.S. 1, 4 (2003).

78. *See* discussion *infra* Part II.

79. *See, e.g., Doe v. Poritz*, 662 A.2d 367, 422–23 (N.J. 1995) (rejecting numerous constitutional challenges to New Jersey's sex offender registry).

80. *See, e.g., Doe v. Phillips*, 194 S.W.3d 833, 852 (Mo. 2006) (en banc) (finding the application of a registration provision to sex offender defendants invalid under the Missouri constitution's prohibition on retrospective laws).

81. N.Y. CITY, N.Y., ADMIN. CODE tit. 10, ch. 6, §§ 10-601 to -608 (2006).

82. *Id.* § 10-604.

83. *Id.* § 10-603.

84. Andrew Glazer, *Despite Risk, L.A. Names Its Most Violent Gangs: Authorities Change Tactics After Surge in Bloodshed Among City's 400 Gangs*, MSNBC.COM, Feb. 8, 2007, <http://www.msnbc.msn.com/id/17054161/> (reporting on the Los Angeles Police Department's compilation of a list of notorious gangs and the ten most wanted gang members).

85. *E.g., Methamphetamine Manufacturer Registry Act*, 730 ILL. COMP. STAT. 180/1-99 (2006).

86. Donna Leinwand, *States List Meth Offenders on Web*, USA TODAY, Aug. 23, 2006, at 1A.

affordable price,⁸⁷ have begun placing criminal records online.⁸⁸ Postings can include not just the judgments of conviction, but also arrest records and dates of court proceedings.⁸⁹ Legislators have also floated proposals to place all court records and documents in an openly accessible, online format,⁹⁰ or to broadcast all court proceedings on television.⁹¹ One particularly creative sheriff in Arizona even hooked up a live video streaming webcam at the county jail, so that people around the world could log on and “[w]atch what’s happening in the Madison Street Jail NOW.”⁹² Although the Ninth Circuit ultimately ruled the webcam unconstitutional (for a while it was pointed at the toilet area of the jail), the county website retained a “Techno-Cops” link that allowed users to search by name for outstanding arrest warrants and had a “Crime of the Week” feature that displayed full arrest information and mug shots upon selection of an offense from a drop-down menu.⁹³

Finally, the use of indexes and registries has also included public–private partnerships in certain limited contexts. For instance, the Transportation Security Administration has engaged in a constant process of refining its airline security surveillance program.⁹⁴ Much

87. For example, BackgroundChecks.com offers a series of background check packages, ranging from \$19.95 for either a nationwide search of sex offender registries or a single state criminal history search to \$44.95 for the “Comprehensive Background Report,” which includes a national search for the addresses, neighbors, family members, single-state criminal history, and real property of any person of interest. BackgroundChecks.com, <https://www.backgroundchecks.com> (last visited Apr. 6, 2008).

88. For example, one may visit the website of Washington Access to Criminal History (WATCH) and, upon paying ten dollars, search for Washington State records of arrests less than one year old with dispositions pending, dependency proceedings, conviction history, and information regarding registered sex and kidnap offenders. Washington Access to Criminal History, <https://watch.wsp.wa.gov/> (last visited Apr. 6, 2008). Florida and Indiana are among other states with such systems.

89. *Id.*

90. See, e.g., Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 MINN. L. REV. 1137, 1153 (2002).

91. See, e.g., Jessica Brown, *Live TV Comes to Mason Court*, CINCINNATI ENQUIRER, Feb. 22, 2007, at 1C.

92. *Demery v. Arpaio*, 378 F.3d 1020, 1025 (9th Cir. 2004). For a critical discussion of the implications of jail cameras, see generally Mona Lynch, *Punishing Images: Jail Cam and the Changing Penal Enterprise*, 6 PUNISHMENT & SOC’Y 255 (2004).

93. Maricopa County Sheriff’s Office, <http://www.mcso.org/> (last visited Apr. 6, 2008).

94. Stephen W. Dummer, *False Positives and Secure Flight Using Dataveillance When Viewed Through the Ever Increasing Likelihood of Identity Theft*, 11 J. TECH. L. & POL’Y 259, 263–66 (2006) (surveying the history of federal data mining programs in the airline industry).

attention has popularly been paid to the compilation of “no-fly” lists composed of the names of suspected terrorists.⁹⁵

The “Secure Flight” program, for example, relies on “data mining and computer algorithms taken from governmental databases of known terrorists compared against huge commercial databases containing private information” to identify prospective threats.⁹⁶ Famously, one iteration of the no-fly system marked Senator Ted Kennedy as a hazard and prevented him from boarding his intended flights.⁹⁷

D. Biometric Scanning

The least developed and utilized of the four general technologies explored here are those related to biometric techniques such as facial recognition software or iris scanning.⁹⁸ Various pilot programs have been instituted throughout the country, although most have met with only limited success.⁹⁹ Perhaps the most famous use of facial recognition technology occurred in 2001, when law enforcement scanned the faces of seventy thousand people attending the Super Bowl in Tampa yielding nineteen “hits” to faces of known terrorists, none of which ultimately proved legitimate.¹⁰⁰ In December 2007,

95. See, e.g., Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1136–37 (2006) (discussing the federal government’s creation of lists forbidding or limiting airline travel by certain individuals but without developing any procedural safeguards to ensure the accuracy of the lists).

96. *Id.* at 265–66.

97. Bob Barr, *Post-9/11 Electronic Surveillance Severely Undermining Freedom*, 41 VAL. U. L. REV. 1383, 1406 (2007); Justin Florence, Note, *Making the No Fly List Fly: A Due Process Model for Terrorist Watchlists*, 115 YALE L.J. 2148, 2150 (2006).

98. Although DNA and fingerprint typing and indexing also constitute “biometric technologies,” I separate them into another category largely to distinguish the use of technology to identify an unknown sample from the use of technology to identify an unknown person. Thus, for instance, a fingerprint database might allow the government either to identify the probable source of fingerprints found at a crime scene or to identify an individual purporting to be another person. The first use is addressed *infra* Part I.A, whereas this Section deals with the latter kind of usage. Of course, the same basic technology—fingerprint identification, in this case—is used in both instances.

99. Ellen Nakashima, *FBI Prepares Vast Database of Biometrics*, WASH. POST, Dec. 22, 2007, at A1 (reporting a German study on facial recognition technique that had a 60 percent success rate during daylight, but only a 10 percent to 20 percent rate at night).

100. Barnaby J. Feder, *Technology Strains to Find Menace in the Crowd*, N.Y. TIMES, May 31, 2004, at C1. Dutch researchers recently tested the efficacy of biometric fingerprint scanners by conducting 6400 checks of fans at European football games in an effort to identify “blacklisted” volunteer fans. The system failed to identify 15 to 20 percent of those listed when kept to a 0.1 percent false positive rate. Jurgen den Hartog & Ruud van Munster, *How To*

however, the Federal Bureau of Investigation announced a one billion dollar plan to compile a vast database of biometric information, including digital face images, fingerprints, palm patterns, iris scans, and perhaps even voice and gait recognition material.¹⁰¹

Local reports about uses of these technologies are piecemeal and anecdotal. According to one report, a Los Angeles Police Department street officer used a handheld device to scan the face of a man “illegally riding double on a bicycle,” who then came up as “94 percent likely to be a match” to a gang member.¹⁰² The individual did turn out to be the alleged gang member and was arrested on suspicion of violating an antiloitering gang injunction and of possessing illegal drugs.¹⁰³ Several commercial airports, including those in Boston, Tampa, and Virginia Beach, have attempted to implement facial scanning programs at security checkpoints, although again each program met with only limited success.¹⁰⁴ One Florida county installed technology in police cars that allows officers to take a digital photo of a suspect, scan it into a computer, and compare it to a national database of fugitives with outstanding warrants.¹⁰⁵ Another pilot program used technology to scan crowds in a downtown district to find felons and runaways, but met with no success.¹⁰⁶

Finally, New York City announced an intention to install one hundred cameras in downtown Manhattan and to have three

Dodge the Red Card, INFO SECURITY, Nov./Dec. 2007, <http://www.infosecurity-magazine.com/features/novdec07/football.html> (“Ideally, false accusation should be less than 0.01%, but not more than 0.1%. The chance of missing a hooligans [*sic*] on the other hand, should be 1% or less.”).

101. Nakashima, *supra* note 99.

102. Associated Press, *LAPD Experimenting with Facial-Recognition Software*, SIGNONSANDIEGO.COM, Dec. 26, 2004, http://www.signonsandiego.com/uniontrib/20041226/news_1n26lapd.html.

103. *Id.*

104. *See* Lamb, *supra* note 14 (reporting that a Boston airport program recognized the faces of 153 volunteer “terrorists,” but failed to identify 96 others, and that Tampa stopped its program after repeated failures, although Virginia Beach continued to use the system). German researchers examining the efficacy rates of facial recognition in a crowd achieved, in a four-month study of a Mainz train station that saw 23,000 daily passengers and tolerated a 0.1 percent false positive rate, roughly a 60 percent success rate during the day, which fell to 10 to 20 percent at night. Nakashima, *supra* note 99.

105. *Facial ID Technology Makes Gains in Florida*, ORGANIZED CRIME DIG., May 4, 2005, http://findarticles.com/p/articles/mi_qa4441/is_200505/ai_n16058151 (reporting that use of technology has led to forty-five arrests since implementation nine months earlier).

106. Lamb, *supra* note 14; *see also* *Chambers v. Commonwealth*, No. 2005-CA-000815-MR, 2006 WL 1451566, at *1 (Ky. Ct. App. May 26, 2006) (noting that the defendant, who gave a false name on arrest, was identified through an iris scan at the jail).

thousand such cameras blanketing the area in an effort to increase public safety.¹⁰⁷ The intention is to link these cameras to license plate readers able to “send out alerts if suspect vehicles [are] detected,” and to install remote-controlled gates or barriers that could “block traffic or a suspect car.”¹⁰⁸ The police department is reportedly contemplating using “face-recognition technology” as well¹⁰⁹ and six other states are purportedly compiling “enormous databases of driver’s license photographs” to use “as a resource for law enforcement agencies.”¹¹⁰

Iris scanning initiatives have also gained ground. According to one report, a county in North Carolina implemented a database to store the biometric images of the iris scans of sex offenders.¹¹¹ Deputies also receive handheld PDA devices that allow them to scan irises in the field that then upload remotely for comparison to the database.¹¹² Federal customs officials are moving toward iris scanning and digital fingerprinting to document all those who enter the country, and U.S. passports already encode biometric information in an effort to integrate scanning systems.¹¹³ Finally, research is underway to develop devices capable of long-range iris scanning, which are perceived to have a higher accuracy rate than traditional facial recognition programs.¹¹⁴

Because biometric technologies are still in development, few legal challenges have been documented and therefore little information exists about biometric databases or what images they might contain. Regardless, it seems likely that biometric technologies

107. Buckley, *supra* note 13.

108. *Id.*

109. *Id.* One New England state in the 1990s reportedly checked cars at the turnpike tollbooth for warrants. SIMON, *supra* note 3, at 199.

110. Adam Liptak, *Driver's License Emerges as Crime-Fighting Tool, but Privacy Advocates Worry*, N.Y. TIMES, Feb. 17, 2007, at A10. States have sought to introduce facial recognition software at state motor vehicle offices to combat identity theft and the fraudulent acquisition of state identification cards. *See, e.g.*, Mark Brunswick, *State Seeks to Get in the Face of ID Theft*, STAR TRIB. (Minneapolis, Minn.), Jan. 6, 2006, at 1B.

111. Lynn Waddell & Arian Campo-Flores, *Iris Scans: Keeping an Eye on Sex Offenders*, NEWSWEEK, July 24, 2006, at 8.

112. *Id.*

113. *See* Embassy Visa & Passport Services, <http://www.passportsrus.com/services.php> (last visited Apr. 6, 2008) (stating that the “proposed U.S. Electronic Passport” contains an embedded computer chip that will “securely store” a “digital photograph” to “enable biometric comparison, through the use of facial recognition technology”).

114. Lynda Hurst, *Bio-Security Still a Fantasy*, TORONTO STAR, Jan. 24, 2004, at A1.

will be the method least likely to encounter any procedural impediments. Nothing prohibits law enforcement from snapping an image of an individual in public (or even via a long-range iris scan).¹¹⁵ The Supreme Court has held that facial features, voice tone, and other identifying public characteristics raise no Fourth Amendment interest.¹¹⁶

There also appears to be no constitutional bar to assembling those images in any particular form. In *Whalen v. Roe*¹¹⁷ the Supreme Court found that no constitutional violation occurs simply because the state amasses private information—there, a list of names and addresses of all those prescribed certain prescription drugs—into a computerized database.¹¹⁸ And very few restrictions limit when or where the government may use such technologies to scan public crowds for matches to its databases once it has amassed enough images to make such efforts worthwhile. Supreme Court doctrine suggests that the only likely limit on such technologies would be if they penetrate the four walls of a private home.¹¹⁹

Finally, it is important to note that biometric technologies (and the electronic location devices discussed in Section C), dovetail nicely with the burgeoning popularity of residency and movement restrictions that declare certain areas off limits to particular individuals.¹²⁰ Injunctions, stay-away orders,¹²¹ and “barring notices”¹²² are a familiar condition of release in an ongoing criminal case, parole

115. See Nakashima, *supra* note 99 (reporting that researchers are working on “capturing images of people’s irises at distances of up to 15 feet, and of faces from as far away as 200 yards,” which may be “several years away”).

116. *United States v. Dionisio*, 410 U.S. 1, 14 (1972); see also *United States v. Karo*, 468 U.S. 705, 730–31 (1984) (finding no expectation of privacy in what is exposed to the public).

117. *Whalen v. Roe*, 429 U.S. 589 (1977).

118. *Id.* at 605–06. The reasoning of lower court opinions upholding DNA databases similarly underscores the likelihood of a biometric analogue being judged constitutional.

119. *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (requiring a warrant for the use of a thermal imager to determine heat radiating from inside of a home). *But cf.* *Minnesota v. Carter*, 525 U.S. 83, 85 (1998) (upholding the warrantless peeking through a slit in the closed blinds of a ground-level apartment).

120. See, e.g., Chiraag Bains, *Next-Generation Sex Offender Statutes: Constitutional Challenges to Residency, Work, and Loitering Restrictions*, 42 HARV. C.R.-C.L. L. REV. 483, 483 n.5 (2007) (cataloguing sex offender statutes).

121. Jeannie Suk, *Criminal Law Comes Home*, 116 YALE L.J. 2, 48 & n.197 (2006) (describing a request for a stay-away order as standard protocol in domestic violence cases).

122. *Id.* at 22 n.66 (enumerating drug-related barring orders); Gregory A. Beck, Note, *Ban Lists: Can Public Housing Authorities Have Unwanted Visitors Arrested?*, 2004 U. ILL. L. REV. 1223, 1234–39 (2004) (describing the operation of “no-trespass lists” or “ban lists”).

or probation, but residence and zoning restrictions apply to persons otherwise free of state supervision. States and municipalities have imposed such restrictions as a means of controlling certain status-based classes of individuals like gang members,¹²³ sex offenders,¹²⁴ or the generally undesirable.¹²⁵ When coupled with electronic tracking devices or biometric imaging machines, however, these restrictions serve as powerful means of monitoring and controlling certain classes of persons.¹²⁶

These mandates typically carry little to no procedural safeguards and are applied categorically rather than individually, in contrast to barring notices and stay-away orders. Most require that certain classes of offenders, typically sex offenders, not live, work, or travel within certain distances of schools, parks, or other places children congregate.¹²⁷ Legal challenges to such ordinances and statutes are still percolating in the courts, but have thus far generally been upheld against various constitutional attacks.¹²⁸

123. Stephanie Smith, Comment, *Civil Banishment of Gang Members: Circumventing Due Process Requirements?*, 67 U. CHI. L. REV. 1461, 1464–68 (2000) (surveying civil responses to gang violence).

124. Corey Rayburn Yung, *Banishment by a Thousand Laws: Residency Restrictions on Sex Offenders*, 85 WASH. U. L. REV. 101, 103–05 (2007). Californians approved a ballot initiative for Proposition 83 that imposed strict residency requirements for certain categories of convicted offenders, although a district judge then blocked its retroactive enforcement. Jennifer Warren, *Judge Blocks Part of Sex Offender Law*, L.A. TIMES, Nov. 8, 2006, at A32. Then-Attorney General Bill Lockyer later announced that his office would interpret the law to be nonretroactive. Bob Egelko, *New Stance on Sex-Offender Law*, S.F. CHRON., Nov. 28, 2006, at A1.

125. STEVE HERBERT & KATHERINE BECKETT, *Zoning Out Disorder: Assessing Contemporary Practices of Urban Social Control*, in STUDIES IN LAW, POLITICS AND SOCIETY 8–11 (forthcoming 2008) (cataloguing techniques of urban control).

126. See Wendy Koch, *More Sex Offenders Tracked by Satellite*, USA TODAY, June 7, 2006, at 3A (describing how “[i]f the offender enters a restricted area, such as a playground, the receiver immediately alerts a data center, which notifies officials via cellphone, e-mail, or fax”).

127. See *supra* note 120 and accompanying text.

128. See, e.g., *Doe v. Miller*, 405 F.3d 700, 705, 709–16 (8th Cir. 2005) (upholding residency restriction); *People v. Leroy*, 828 N.E.2d 769, 775 (Ill. App. Ct. 2005) (same); *ACLU v. City of Albuquerque*, 137 P.3d 1215, 1228 (N.M. Ct. App. 2006) (upholding residency restriction as modified by district court to apply only to newly acquired residences, and not to homes previously owned or second mortgages).

II. LEGAL CONSTRAINTS ON THE REGULATION OF THE DANGEROUS

The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. . . . Can it be that the Constitution affords no protection against such invasions . . . ?¹²⁹

New technologies have been harnessed to control or monitor allegedly dangerous individuals without relying on their physical incapacitation in a wide range of ways. But of course, vast differences exist in their actual operation and practice, both across technologies and even within a particular technology. Consider electronic location monitoring (such as GPS tracking). It might be ordered to monitor pretrial a suspect in a specific criminal case, or imposed as a sentencing condition, or required as a freestanding rule for anyone previously convicted of a certain offense. It might be used prospectively, for instance to alert authorities if an individual enters into a forbidden area, or retrospectively, for example to prove that a person was in a particular place. It might be used with prior notice to the tracked individual or, conceivably, without alerting the individual in advance that all movement will be monitored.

Each variation obviously evokes distinct sets of questions and concerns. Moreover, although some of those concerns might be common to the variety of technologies discussed above, not every one overlaps. Not all surveillance technologies are created equal, nor ought they all share the same permissible scope of implementation. Indeed, this Article claims precisely that the wide variation and nuance in the manner in which these techniques operate calls for careful, sensitized attention to how they might be deployed in any particular situation.

Unfortunately, the existing legal scrutiny of technological restraints lacks the necessary degree of care and sensitivity. Across doctrines, and with regard to a range of technologies, nonphysical methods of incapacitation and control have been approved with

129. *Olmstead v. United States*, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) (emphasis added).

minimal, or in many cases no, judicial scrutiny of any kind. In fact, many methods have been implemented without any meaningful effort to analyze, much less differentiate, their appropriate scope of application.

All of the technologies outlined in Part I apply in a broad-brush, categorical manner, with few, if any, tailored inquiries into necessity or possible harm. Courts have upheld most as constitutional even when imposed retroactively or in duplicate to another form of restraint. Few set any expiration date or temporal limit on the period of use. For example, electronic location monitoring and sex registry requirements all tend to be triggered by a categorical status—typically prior conviction—apply retroactively and alongside other forms of restraint (including one another), and remain in place for decades or even life.¹³⁰ Government databases of biometric images or genetic material—say of purported gang members or drug dealers—can be secretly constructed, eternally maintained, and freely searched without any limiting restrictions on their contents.¹³¹

One possible explanation for the conspicuous absence of meaningful judicial scrutiny may be that many technologies of restraint first emerged within the procedural edifice of the criminal justice system, in which established and rigorous legal standards already governed their implementation. For instance, tracking systems were first deployed as alternatives to otherwise authorized, more restrictive forms of supervision—whether pre- or post-trial physical incarceration. Thus, before the state attached a GPS bracelet to an individual, it first had to lay charges, provide counsel, and meet the standard of proof beyond a reasonable doubt or demonstrate by clear and convincing evidence that an individual posed a danger if released pretrial. The alternatives, then, were equivalent: qualify for detention and await trial either in jail or wearing a GPS bracelet. Similarly, biometric techniques like DNA typing or iris scans naturally inherit the legacy of their more rudimentary ancestor, fingerprinting, which longstanding practice has allowed on a showing of probable cause at the time of arrest.

But, as Part I illustrates, these technologies ensnare individuals otherwise outside of any formal control of the state. GPS bracelets have been affixed, whether by statute or executive order, on

130. See *supra* Part I.

131. See *supra* Part I.D.

individuals who have long since finished any sentence or term of supervision. DNA is likewise taken and stored from those in no way subject to any special state authority or supervision. Persons long since through with probation or parole must nonetheless report trimonthly to an agent of the state for purposes of sex offender registries. In these cases, then, the familiar limitations of criminal process fall away, leaving nothing but a void.

This Part, accordingly, examines how extant constitutional doctrines regulate the use of technological restraints against targeted “dangerous” populations otherwise outside of the control of the criminal justice system. Analysis reveals that such restraints evade scrutiny in part because, across a range of claims, the notion of the value at stake—liberty—is typically viewed through the lens of physical incapacitation as the archetypal “paradigm of restraint.” In short, physical deprivations serve as the touchstone of constitutional scrutiny. But wearing an electronic bracelet, giving a DNA sample, submitting to a facial scan, or complying with indexing requirements only minimally impact physical liberty. Accordingly, such analysis rarely generates cause for concern or, correspondingly, judicial attention.

A. “Regulatory” versus “Punitive”

Physical incapacitation virtually always triggers some degree of serious procedural scrutiny.¹³² The Constitution spells out a long litany of entitlements that must be granted before a criminal “punishment” may be imposed. Full criminal process, along with its individualized proceedings for finding guilt, its high standard and burden of proof, and the full range of Fifth and Sixth Amendment rights, must precede all “punishment.”¹³³ A punishment cannot be retroactive,¹³⁴ cannot be imposed in duplicate,¹³⁵ and certain categories and kinds of punishments such as those that are cruel and unusual are forbidden altogether.¹³⁶

In contrast, “regulatory” restraints operate almost entirely unfettered. A “civil” or “regulatory” restriction can apply

132. Even the government’s recent attempts to push the limit of this principle were met with resistance. *See, e.g., Hamdan v. Rumsfeld*, 126 S. Ct. 2749 (2006).

133. U.S. CONST. amends. V, VI, VIII.

134. *See, e.g., Kansas v. Hendricks*, 521 U.S. 346, 371 (1997).

135. *See, e.g., United States v. Ursery*, 518 U.S. 267, 273 (1996).

136. *See Bell v. Wolfish*, 441 U.S. 520, 535 & n.16 (1979).

retroactively and can duplicate other measures, including punitive ones. It need not meet the strict procedural standards of criminal process. Indeed, it may not receive constitutional scrutiny of any kind. In sum, whereas “punitive” measures receive the protections of constitutional criminal process, “regulatory” measures receive only that scrutiny available to any ordinary civil enactment under the Constitution.

What then differentiates “punitive” from “regulatory” measures? Across a range of doctrines and over a broad span of time, the answer has turned on the application of a multifactor test first outlined in *Kennedy v. Mendoza-Martinez*.¹³⁷ In the years since its articulation, *Mendoza-Martinez* has emerged as the standard “in various constitutional contexts,”¹³⁸ including in assessing rights related to substantive due process,¹³⁹ procedural due process,¹⁴⁰ self-incrimination,¹⁴¹ ex post facto,¹⁴² double jeopardy,¹⁴³ and cruel and unusual punishment.¹⁴⁴ Nevertheless, it remains a largely under-the-radar test that garners little scholarly attention.¹⁴⁵

Mendoza-Martinez involved a statute that automatically revoked the citizenship of those who left the country to evade military service.¹⁴⁶ Finding the law “punitive” and thus violative of the Fifth and Sixth Amendments, the Court undertook to distinguish between

137. *Kennedy v. Mendoza-Martinez*, 372 U.S. 144, 168–69 (1963).

138. *Smith v. Doe*, 538 U.S. 84, 97 (2003). This approach has also been used to determine cases under the Bill of Attainder Clause. *See, e.g., De Veau v. Braistead*, 363 U.S. 144, 160 (1960).

139. *United States v. Salerno*, 481 U.S. 739, 746–47 (1987) (finding that pretrial detention was “regulatory” and not “punitive,” and therefore did not violate substantive due process); *Bell*, 441 U.S. at 534 (rejecting prison conditions case raised by pretrial inmates on substantive due process grounds because alleged discomfort was not punishment and did not otherwise “rise to the level of [a] fundamental liberty interest[]”).

140. *Mendoza-Martinez*, 372 U.S. at 165–66 (holding that due process prohibited imposition of the “punishment” of deprivation of nationality in the absence of full criminal process).

141. *Allen v. Illinois*, 478 U.S. 364, 375 (1986) (finding that the Illinois Sexually Dangerous Persons Act requirement that defendants answer questions about their acts did not violate the Fifth Amendment self-incrimination clause because the proceeding was civil and not criminal in nature); *United States v. Ward*, 448 U.S. 242, 249–55 (1980).

142. *Kansas v. Hendricks*, 521 U.S. 346, 362, 371 (1997).

143. *Id.*; *United States v. One Assortment of 89 Firearms*, 465 U.S. 354, 365–66 (1984).

144. *See supra* note 136 and accompanying text.

145. Although hardly empirical proof, it is nonetheless revealing that a search in the “JLR” database of Westlaw for “*Kennedy v. Mendoza-Martinez*” yields only 819 hits, whereas “*Katz v. United States*” yields 3510, “*Mathews v. Eldridge*” turns up 2994, and “*Terry v. Ohio*” returns 3,276.

146. *Kennedy v. Mendoza-Martinez*, 372 U.S. 144, 147 (1963).

punitive and regulatory enactments.¹⁴⁷ The Court explained that it first inquires into the legislature's intent, noting that the legislature's failure to provide the procedural safeguards associated with criminal procedure constitutes evidence that a particular measure was intended to be civil and regulatory in nature.¹⁴⁸

If the statute appears to be civil in nature, then only the "clearest proof" that the effects of the regulation are punitive "will suffice to override legislative intent."¹⁴⁹ Such proof is derived from an examination of the effects of the measure, according to the Court's articulation of an oft-quoted, seven-part test that asks:

Whether the sanction involves an affirmative disability or restraint, whether it has historically been regarded as a punishment, whether it comes into play only on a finding of scienter, whether its operation will promote the traditional aims of punishment—retribution and deterrence, whether the behavior to which it applies is already a crime, whether an alternative purpose to which it may rationally be connected is assignable for it, and whether it appears excessive in relation to the alternative purpose assigned¹⁵⁰

This test is not applied according to any precise mathematical formulation, however, and at various times the courts have emphasized particular factors over others.

In operation, the *Mendoza-Martinez* factors have fixed the line between regulatory and punitive measures as a function of the jailhouse door. For instance, in *Smith v. Doe*,¹⁵¹ the Supreme Court confronted an ex post facto claim regarding a sex offender registration statute's retroactive application. Applying the *Mendoza-Martinez* test, the Supreme Court looked to the "affirmative disability or restraint" factor and observed that the "Act imposes no *physical* restraint, and so does not resemble the punishment of *imprisonment*,

147. *Id.* at 165–66.

148. *Smith v. Doe*, 538 U.S. 84, 96 (2003) ("The Act itself does not require the procedures adopted to contain any safeguards associated with the criminal process. That leads us to infer that the legislature envisioned the Act's implementation to be civil and administrative."). Even the inclusion of such safeguards, however, does not necessarily render it punitive. *Allen v. Illinois*, 478 U.S. 364, 371–72 (1986).

149. *Smith*, 538 U.S. at 92.

150. *Mendoza-Martinez*, 372 U.S. at 168–69 (footnotes omitted).

151. *Smith v. Doe*, 538 U.S. 84 (2003).

which is the paradigmatic affirmative disability or restraint.”¹⁵² The Court even dismissed the import of the physical restrictions that the statute did impose—such as the “requirement of periodic updates”¹⁵³ or the fact that “registrants must inform the authorities after they change their facial features (such as growing a beard), borrow a car, or seek psychiatric treatment”¹⁵⁴—and noted that “minor and indirect” restraints are “unlikely to be punitive.”¹⁵⁵

The D.C. Circuit likewise relied upon the “paradigm” of incarceration in *Johnson v. Quander*,¹⁵⁶ which upheld the retroactive application of a DNA collection statute against an ex post facto claim. Asking whether DNA collection imposed an “affirmative disability,” the court concluded that the “DNA Act ‘imposes no physical restraint, and so does not resemble the punishment of imprisonment.’”¹⁵⁷ As a result, the measure was not punitive. Similar reasoning could easily apply to statutes mandating electronic location tracking or collecting biometric images for use in databases. Image collection entails no physical restraint of any kind, and electronic location tracking at best involves only a minor physical inconvenience in the form of a bracelet or other device.

Courts have also applied the remaining *Mendoza-Martinez* factors by referencing the physical world while simultaneously dismissing its virtual counterpart. For example, in *Smith v. Doe*, a lower court had applied the “history and tradition” of punishment factor and concluded that an online index was “of fairly recent origin” and thus could not qualify as “punishment.”¹⁵⁸ On appeal to the Supreme Court, the litigants countered that the online index resembled the shaming and banishments punishments of yore.¹⁵⁹ Rebuking the analogy, the Court observed that historical punishments “staged a direct confrontation between the offender and the public” and “either held the person up before his fellow citizens

152. *Id.* at 99–100 (emphasis added); see also *Hudson v. United States*, 522 U.S. 93, 104 (1997) (finding that bar from working in banking industry is “certainly nothing approaching the ‘infamous punishment’ of imprisonment”).

153. *Smith*, 538 U.S. at 101.

154. *Id.*

155. *Id.*

156. *Johnson v. Quander*, 440 F.3d 489 (D.C. Cir. 2006).

157. *Id.* at 502 (quoting *Smith*, 538 U.S. at 100).

158. *Smith*, 538 U.S. at 97.

159. *Id.*

for face-to-face shaming or expelled him from the community.”¹⁶⁰ The registries, in contrast, merely disseminated information with a purpose to “inform the public for its own safety, not to humiliate the offender.”¹⁶¹ Because the confrontation took place in virtual rather than physical space and the purpose was framed as informational rather than experiential, the Court concluded that the measure was not punitive.¹⁶²

In sum, technological restraints—which impose harm in predominantly nonphysical forms—are rarely found to constitute punitive restraints. Of course, the mere designation of a measure as regulatory need not necessarily foreclose a finding that additional procedural protections are nonetheless warranted. But whereas the punitive label brings with it the constellation of constitutional criminal entitlements,¹⁶³ the regulatory classification carries no clear next procedural step. Typically, a measure judged “civil” under *Mendoza-Martinez* only triggers procedural scrutiny if it also implicates a “liberty interest” founded in state law or the Constitution.¹⁶⁴

B. Due Process and “Liberty Interests”

The rubric of procedural due process arguably constitutes the most natural vehicle for a procedure-based challenge to a technological restraint. But when it comes to these regulatory restraints, it is unclear what constitutional standard should apply. Courts typically ask first whether a measure is in fact punitive, applying the *Mendoza-Martinez* test outlined in Section A.¹⁶⁵ If punitive, then the necessary procedural requirements are those dictated by the strict constitutional requirements for criminal process.

160. *Id.* at 98.

161. *Id.* at 99.

162. *Id.*

163. *See, e.g.,* Commonwealth v. Lee, 935 A.2d 865, 880 (Pa. 2007) (“The number of arguments raised by Appellees tends to obscure that Appellees succeed only if we accept the premise, which we have all but categorically rejected in our prior cases, that the registration, notification, and counseling provisions of Megan’s Law II are punitive in the constitutional sense, thus requiring observance of all the due process protections that attend criminal prosecution, especially those identified by the United States Supreme Court’s decision in *Apprendi*.”).

164. *See infra* Part II.B.

165. *See supra* Part II.A.

If characterized as regulatory, however, the inquiry becomes clouded. Courts tend to resort to the conventional test of procedural due process, which first asks whether the measure infringes a cognizable “liberty interest.”¹⁶⁶ But as the Supreme Court has repeatedly stated, such “liberty interests” must materialize either in positive state law or as the fundamental rights enshrined in the Constitution.¹⁶⁷ Yet here again, as in the punitive–regulatory distinction, such “liberty interests” tend to begin only at the jailhouse door.

No one doubts that the government infringes liberty when it physically incarcerates individuals. Freedom from “physical detention by one’s own government” has been described as “the most elemental of liberty interests.”¹⁶⁸ Even in a criminal case, a due process right to counsel has been “recognized to exist only where the litigant may lose his physical liberty if he loses the litigation.”¹⁶⁹ To be sure, the Supreme Court has acknowledged that “‘liberty’ . . . is not confined to mere freedom from bodily restraint,”¹⁷⁰ but at the same time, it has

166. Ky. Dep’t of Corr. v. Thompson, 490 U.S. 454, 460 (1989); see also Doe v. Miller, 405 F.3d 700, 709 (8th Cir. 2005).

167. See *Thompson*, 490 U.S. at 460. See generally Jane Rutherford, *The Myth of Due Process*, 72 B.U. L. REV. 1, 44–45 & nn.242–44 (describing the Court’s approach to liberty and summarizing popular critiques).

168. Hamdi v. Rumsfeld, 542 U.S. 507, 529 (2004) (plurality opinion) (citing *Foucha v. Louisiana*, 504 U.S. 71, 80 (1992)). In *Foucha* the Court held that “[f]reedom from bodily restraint has always been at the core of the liberty protected by the Due Process Clause from arbitrary governmental action.” *Foucha*, 504 U.S. at 80. The Supreme Court in *McKune v. Lile*, 536 U.S. 24 (2002), addressed a prison rehabilitation program that required inmates to confess to prior crimes without a promise of immunity, or else have their housing transferred to a far more restrictive block. *Id.* at 30–31. Noting that a refusal to participate “did not extend [the defendant’s] term of incarceration,” or “affect his eligibility for good-time credits or parole,” the Court found no due process liberty interest—or even a lesser interest relevant for a Fifth Amendment compulsion analysis—in remaining in medium, rather than maximum, security. *Id.* at 38–39. This simply underscores the degree to which the Court views the deprivation determination as zero-sum; the relevant inquiry is whether the state has taken physical liberty or not, not to what degree such deprivation is effectuated.

169. *Lassiter v. Dep’t of Soc. Servs.*, 452 U.S. 18, 25 (1981). The Court has held that such loss of liberty includes the possible loss of liberty should a suspended sentence be executed. *Alabama v. Shelton*, 535 U.S. 654, 675 (2002).

170. *Bolling v. Sharpe*, 347 U.S. 497, 499 (1954). Indeed, the Court has held:

[liberty is] not merely freedom from bodily restraint but also the right of the individual to contract, to engage in any of the common occupations of life, to acquire useful knowledge, to marry, establish a home and bring up children, to worship God according to the dictates of his own conscience, and generally to enjoy those privileges long recognized . . . as essential to the orderly pursuit of happiness by free men.

failed to define the notion of “liberty” with “any great precision.”¹⁷¹ Generally speaking, the “liberty interests” defined by deprivations of privacy¹⁷² or impediments to work,¹⁷³ housing,¹⁷⁴ or bodily autonomy¹⁷⁵ stand on far shakier footing than the right to be free of corporeal restraint.¹⁷⁶ Accordingly, technological regulations, which again rarely

Conn v. Gabbert, 526 U.S. 286, 291 (1999) (quoting *Bd. of Regents v. Roth*, 408 U.S. 564, 572 (1972)); *see also* *Washington v. Glucksberg*, 521 U.S. 702, 719 (1997) (“The Due Process Clause guarantees more than fair process, and the ‘liberty’ it protects includes more than the absence of physical restraint.”).

171. *Bolling*, 347 U.S. at 499.

172. In *Paul v. Davis*, 424 U.S. 693 (1976), the Court observed that “[w]hile there is no ‘right to privacy’ found in any specific guarantee of the Constitution, the Court has recognized that ‘zones of privacy’ may be created by more specific constitutional guarantees and thereby impose limits upon government power,” *id.* at 712–13. It also noted, however, that “‘right of privacy’ cases, while defying categorical description, deal generally with substantive aspects of the Fourteenth Amendment.” *Id.* at 713; *see also* *Planned Parenthood of Se. Pa. v. Casey*, 505 U.S. 833, 851 (1992) (“[M]atters[] involving the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy, are central to the liberty protected by the Fourteenth Amendment.”). The Court rejected the defendant’s claim, which was based on the sheriff’s public posting of the defendant’s name and picture on an “Active Shoplifters” flyer, noting that “[t]he activities detailed as being within this definition were ones very different from that for which respondent claims constitutional protection—matters relating to marriage, procreation, contraception, family relationships, and child rearing and education.” *Paul*, 424 U.S. at 713.

173. For instance, the Court has held that a state may clearly enact a general scheme of legislation that inhibits individuals’ economic liberties by foreclosing their ability to pursue a lawful occupation. *See* *New Motor Vehicle Bd. v. Orrin W. Fox Co.*, 439 U.S. 96, 106–08 (1978) (upholding a California statute regulating the grant of franchises in the auto industry and comparing cases); *Williamson v. Lee Optical Co.*, 348 U.S. 483, 491 (1955) (upholding an Oklahoma law prohibiting the fitting or duplication of eyeglasses without a written prescription from an ophthalmologist). Rejecting the notion that a search of an attorney’s office infringed upon the right to freely exercise of a profession, the Court stated that although there might exist a liberty interest in “choos[ing] one’s field of private employment,” such a right “is nevertheless subject to reasonable government regulation.” *Conn*, 526 U.S. at 292.

174. Courts have rejected a constitutional right to housing in a variety of contexts. *See, e.g.*, *Lindsey v. Normet*, 405 U.S. 56, 73–74 (1972) (rejecting the claim that the “‘need for decent shelter’ and the ‘right to retain peaceful possession of one’s home’ are fundamental interests” because there is no “constitutional guarantee of access to dwellings of a particular quality, or any recognition of the right of a tenant to occupy” property outside of a contractual situation); *Royer ex rel. Estate of Royer v. City of Oak Grove*, 374 F.3d 685, 689 (8th Cir. 2004) (finding “no property interest in having unlimited access to a public building”).

175. *Kelley v. Johnson*, 425 U.S. 238, 244 (1976) (assuming liberty interest in “matters of personal appearance” but finding no infringement in law that dictated permissible hair lengths for local police officers). *But see* *Washington v. Harper*, 494 U.S. 210, 221–22 (1990) (finding a “significant liberty interest in avoiding the unwanted administration of antipsychotic drugs under the Due Process Clause of the Fourteenth Amendment,” but finding it commensurate with the right as established in positive state law).

176. *But see* *Youngberg v. Romeo*, 457 U.S. 307, 309 (1982). *Youngberg* addressed a due process claim by an institutionalized, mentally retarded person that his conditions of

impinge physical freedom in any meaningful way, can thus easily escape constitutional attention.

For example, in *Connecticut Department of Public Safety v. Doe*,¹⁷⁷ the Supreme Court addressed a procedural due process challenge to the Connecticut law creating a state sex offender registry.¹⁷⁸ The law required every eligible offender to provide the state with personal information including a name, current address of residence, photograph, and DNA sample.¹⁷⁹ Offenders then had to verify the accuracy of this information every ninety days (or notify the agency upon change) for a period of ten years or, for certain offenders, life.¹⁸⁰ The act applied without any individual determination of dangerousness and its scope included nonviolent offenders.¹⁸¹ There was no allowance for any tailored formal or informal process or an individualized showing of danger. The state published this information on a public website that could be searched by zip code or town name.¹⁸²

Eight of nine Justices, in addressing a procedural due process claim, agreed that these reporting requirements likely invoked no cognizable liberty interest of any kind.¹⁸³ Of course, the statute contained at least one express, recurring deprivation of the defendant's physical liberty: defendants had to check in at a government office every ninety days for the rest of their lives. Yet because the reporting obligation was framed in informational terms, it did not register with the Court as an infringement deserving of any scrutiny or procedural oversight.¹⁸⁴ Equally as importantly, the Court

confinement were both unsafe and unnecessarily restrictive. Finding liberty interests in both concerns, the Court found a duty to provide the claimant with "reasonably nonrestrictive confinement conditions," among other things. *Id.* at 324.

177. *Conn. Dep't of Pub. Safety v. Doe*, 538 U.S. 1 (2003).

178. *Id.* at 4–6.

179. *Id.* at 4–5.

180. *Id.*

181. *Id.* at 7.

182. *Id.* at 5.

183. *Id.* at 6–7.

184. Of course, it still might have found that no process was necessary to prevent its erroneous deprivation. *See Mathews v. Eldridge*, 424 U.S. 319, 335 (1976) (outlining a three-part inquiry triggered by a liberty interest that weighs the private interest affected, the risk of erroneous deprivation using the procedures in place, and the value of any additional procedures).

expressly rejected an interest in not having to report every change of hair color or address to the government.¹⁸⁵

Indeed, the closest the *Connecticut Department of Public Safety* Court could come to recognizing an interest implicated by the mandatory registration and dissemination regime was a nod to a foggy, trivial interest in “reputation” that was deemed noncognizable.¹⁸⁶ Even Justice Stevens, the sole member of the Court to acknowledge an impinged liberty interest, could define that interest only in conclusory terms, stating summarily in the companion case, *Smith v. Doe*, that “these statutes unquestionably affect a constitutionally protected interest in liberty.”¹⁸⁷

Procedural due process challenges to DNA collection statutes have likewise faltered on the ground that the interest intruded upon does not rise to a constitutionally cognizable level. As the Ninth Circuit succinctly held, “[t]he extraction of blood from an individual in a simple, medically acceptable manner, despite the individual’s lack of an opportunity to object to the procedure, does not implicate the Due Process Clause.”¹⁸⁸ Framed this way, no general interest in “genetic privacy” could apparently generate the requisite “liberty” interest. From this reasoning the government arguably need not infringe on a cognizable liberty interest when it captures and stores a biometric image of an individual in a database

Even affixing a location-tracking device could quite readily be viewed as no meaningful deprivation of liberty under the current conception of the term. Such devices impose only the slightest

185. *Conn. Dep’t of Pub. Safety*, 538 U.S. at 7–8.

186. *Id.* at 6. Regardless, the Court held that, to the extent that a cognizable interest existed, the offenders’ requests for individualized determinations of dangerousness were not warranted because the statutory regime drew no distinctions nor worked any deprivations on that basis. *Id.* at 7–8. Justices Souter and Ginsburg wrote separately to note that the Court’s holding did not foreclose a substantive due process claim, and also to underscore that the statute’s provisions allowing exemptions for certain sex offenders might raise equal protection problems. *Id.* at 9 (Souter, J., concurring).

187. *Smith v. Doe*, 538 U.S. 84, 112 (Stevens, J., joined by Ginsburg, J., dissenting).

188. *Rise v. Oregon*, 59 F.3d 1556, 1562–63 (9th Cir. 1995); *see also Doe v. Moore*, 410 F.3d 1337, 1350 (11th Cir. 2005) (rejecting a procedural due process challenge to a DNA-collection statute due to the lack of a cognizable liberty interest); *Johnson v. Quander*, 370 F. Supp. 2d 79, 92–93 (D.D.C. 2005) (noting the decreased expectation of privacy for convicts on probation, the compelling state interest of identification, and the limited uses for the DNA samples). A Kansas federal district court reached the same conclusion, adding that “even if [the] challenge is to the enactment of the law, rather than the method of the blood draw, his argument fails. When legislation affects a general class, the legislative process satisfies due process requirements.” *Miller v. U.S. Parole Comm’n*, 259 F. Supp. 2d 1166, 1169–70 (D. Kan. 2003).

physical discomfort and will become even less intrusive over time. To the extent that they impose any physical harm, it is at best “minor and indirect,” and thus “unlikely to be punitive.”¹⁸⁹ The Supreme Court has, in fact, found no property interest affected by the affixing of a tracking device on personal property, because even the “technical trespass” did not interfere with the defendant’s interest in “a meaningful way.”¹⁹⁰ Moreover, tracking devices do not impede individuals from moving freely in society, but simply watch them as they do; so long as such watching is outside of the home,¹⁹¹ then no constitutional concerns are raised.

The Court employed this very line of reasoning in the sex registry cases: whereas “liberty” might be infringed if the state refused to *allow* an individual to borrow a car or cut one’s beard, no liberty interest at all is affected so long as the government requires merely that the individual *report* having done so.¹⁹² Given this proclivity toward conceiving “liberty interests” as founded predominantly in physical terms, rather than in privacy or autonomy, it is hard to imagine that location monitoring—much less DNA typing, biometric imaging, or online indexing—would infringe any recognized interest.

To the extent that no cognizable “liberty interest” is likely to be found for purposes of procedural due process, it remains even less likely that an interest will be recognized under substantive due process—an even more parsimoniously applied doctrine.¹⁹³ In contrast, a state would be hard-pressed to physically restrain an individual without infringing a constitutionally recognized right

189. *Smith*, 538 U.S. at 100.

190. *United States v. Karo*, 468 U.S. 705, 712 (1984) (finding, *inter alia*, that the surreptitious installation of an electronic tracking device in a drum sold to the defendant did not interfere with any cognizable “possessory interest”); *United States v. Knotts*, 460 U.S. 276, 284–85 (1983).

191. *Karo*, 468 U.S. at 718 (requiring a warrant only for police monitoring of a beeper inside a home); *see also* *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (finding the warrantless use of a thermal imager to detect heat emanating from inside a home to be an unlawful search).

192. *Smith*, 538 U.S. at 101; *see also id.* at 100 (stating that “[t]he Act does not restrain activities sex offenders may pursue but leaves them free to change jobs or residences,” and noting only that while they “must inform the authorities after they change their facial features (such as growing a beard), borrow a car, or seek psychiatric treatment, they are not required to seek permission to do so”).

193. *Collins v. City of Harker Heights*, 503 U.S. 115, 125 (1992) (“As a general matter, the Court has always been reluctant to expand the concept of substantive due process because guideposts for responsible decisionmaking in this unchartered area are scarce and open-ended.”).

worthy of substantive due process scrutiny.¹⁹⁴ Indeed, from the series of cases involving civil physical incapacitation, it is evident that procedural safeguards play a critical role in determining the constitutionality of the incapacitation regime.

For example, in *United States v. Salerno*,¹⁹⁵ which upheld “regulatory” pretrial detention of certain criminal suspects, the Court specifically cited the elaborate procedural safeguards of the Bail Reform Act and remarked that a “scattershot attempt to incapacitate those who are merely suspected . . . of crime[]”¹⁹⁶ would not have stood. Similarly, in the sexual predator cases, the Court has specifically required that such statutes entail “proper procedures or evidentiary standards,” for instance, “a finding of dangerousness either to one’s self or to others,” and a “plus” factor such as mental illness or disease.¹⁹⁷ The Court has even specifically found unconstitutional the commitment of sexual offenders “without *any* lack-of-control determination.”¹⁹⁸ In cases of regulatory physical incapacitation, then, the degree of process appears mainly to either bolster the regime against substantive due process attack, or else serve as a basis for wholesale invalidating it.

But the courts have been far less demanding in dealing with “regulatory” measures. In addressing sex offender registries, courts have shied away from finding a cognizable interest of any kind, noting that “the Court has always been reluctant to expand the concept of substantive due process.”¹⁹⁹ In fact, even those few courts that have invalidated provisions of such acts using a substantive due process rationale have done so applying rational basis review rather than any heightened type of scrutiny.²⁰⁰

194. See *Bell v. Wolfish*, 441 U.S. 520, 535 & n.16 (1979) (noting that concerns about the incarceration conditions of pretrial detainees are properly addressed as due process matters).

195. *United States v. Salerno*, 481 U.S. 739 (1987).

196. *Id.* Moreover, the Court observed, the category of those even deemed eligible for detention was limited to individuals charged with serious offenses, and detention was permitted only for the limited, pretrial period. *Id.*

197. *Kansas v. Hendricks*, 521 U.S. 346, 357 (1997) (rejecting substantive due process, ex post facto, and double jeopardy challenges); see also *Seling v. Young*, 531 U.S. 250, 254 (2001) (noting a “panoply of protections,” including the proof beyond a reasonable doubt standard).

198. *Kansas v. Crane*, 534 U.S. 407, 412 (2002) (invalidating a provision, apparently on substantive due process grounds).

199. *Doe v. Phillips*, 194 S.W.3d 833, 842–43 (Mo. 2006) (en banc).

200. *ACLU v. City of Albuquerque*, 137 P.3d 1215, 1226 (N.M. Ct. App. 2006) (invalidating a registration provision for offenders convicted of crimes lacking a specific sexual component); *State v. Small*, 833 N.E.2d 774, 782–83 (Ohio Ct. App. 2005) (invalidating a registration

Regulatory measures that do *not* deprive physical liberty, however, seem capable of being crafted in the crudest procedural terms yet nonetheless survive constitutional scrutiny.²⁰¹ The *Smith v. Doe* Court ratified this stance, differentiating the ex post facto challenge to the physical confinement of sexual predators as requiring “individual assessment” due to the “magnitude of the restraint,” whereas such an assessment was unnecessary as regards to online indexing because the “[a]ct . . . imposes the more minor condition of registration.”²⁰²

C. “Reasonable Expectation of Privacy”

The Fourth Amendment provides another possible candidate for constitutional scrutiny of technological restraints on liberty. Interestingly, although Fourth Amendment litigation has dominated some of the new technologies, challenges regarding others have largely overlooked or ignored such claims.²⁰³ Thus, early litigation about the constitutionality of DNA collection statutes focused largely upon search and seizure arguments, whereas sex offender registration acts tended to be framed as equal protection or due process problems rather than as repeated, suspicionless, and intrusive seizures or searches for information in violation of the Fourth Amendment.

It is well established that to trigger Fourth Amendment scrutiny, a police practice must constitute an intrusion on “an actual (subjective) expectation of privacy . . . that society is prepared to recognize as ‘reasonable.’”²⁰⁴ Here again, however, the courts have tended to define such expectations with reference to the physical world, notwithstanding the promise long ago that the amendment

provision as violating substantive due process when it did not specify that conviction be based on sexual acts).

201. One aspect of the *Mendoza-Martinez* test—whether the restraint is “excessive” in relation to its purpose—can singularly transform a measure from regulatory to punitive. Probably because of this potency, however, it is rarely invoked. *But see* *Smith v. Doe*, 538 U.S. 84, 116–17 (2003) (Ginsburg, J., dissenting) (finding Alaskan registration act “excessive[] in relation to its nonpunitive purpose” because it “applies to all convicted sex offenders, without regard to their future dangerousness” and carries “exorbitant” duration and reporting requirements without any reference to the possibility of rehabilitation).

202. *Id.* at 104 (majority opinion).

203. The Court has held, however, that if a specific constitutional provision governs the government action in question, then that provision should guide the relevant constitutional inquiry as opposed to more nebulous provisions such as the Due Process Clause. *County of Sacramento v. Lewis*, 523 U.S. 833, 842 (1998).

204. *Katz v. United States*, 389 U.S. 347, 361 (1967).

would protect “people, not places.”²⁰⁵ Thus, the home remains a citadel²⁰⁶ or the slightest movement of a stereo creates a constitutional moment,²⁰⁷ even though the garbage on the street, the dialed numbers on a phone or the records at the bank receive no constitutional protection at all.²⁰⁸ The test relies upon the public–private distinction as drawn by the physical world; “the police can infringe privacy in ways that anyone else might infringe it,”²⁰⁹ even if no one else is likely to do so.

Technologies of restraint, however, tend to operate in a manner that entails minimal formal physical intrusion into the private sphere. A DNA sample can be collected, typed, and placed in a database by simply swabbing a cheek or even picking up a discarded straw. A GPS bracelet generally reveals no more information than would an alert, round-the-clock surveillance team. Biometric images can be collected without even informing the target, as can public scanning equipment be deployed without any physical interference with movement or traffic. And apart from a reporting burden placed on those required to comply with indexes, the information collected is often that which can be readily obtained from third-party or public sources. In sum, because the privacy interests most gravely affected by technologies of restraint do not take the form of physical intrusions on sacred spaces or bodily integrity, courts are apt to disregard them as viable interests at all.

For example, in *United States v. Kincade*,²¹⁰ the Ninth Circuit reviewed the compulsory DNA testing requirement for certain federal offenders.²¹¹ Applying a totality of the circumstances balancing test, the court began by assessing the burden the statute placed on the offenders.²¹² The primary approach looked to the *physical* intrusion that a blood test imposes and concluded that the intrusion was minimal.²¹³ The court easily concluded that blood tests are in fact

205. *Id.* at 351.

206. *Kyllo v. United States*, 533 U.S. 27, 31 (2001).

207. *Arizona v. Hicks*, 480 U.S. 321, 324–25 (1987).

208. *California v. Greenwood*, 486 U.S. 35, 40 (1988); *Smith v. Maryland*, 442 U.S. 735, 744 (1979); *United States v. Miller*, 425 U.S. 435, 443 (1976).

209. William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265, 1269 (1999).

210. *United States v. Kincade*, 379 F.3d 813 (9th Cir. 2004) (en banc).

211. *Id.* at 816.

212. *Id.* at 836.

213. *Id.*

“routine” and certainly far less intrusive than the body cavity searches and other physical indignities to which federal offenders are routinely subjected.²¹⁴ Concerns of a less corporeal variety, such as those regarding privacy and misuse of information, were readily disregarded.²¹⁵ Because the typed genetic profile constituted only “a record of the defendant’s identity,”²¹⁶ the retention of both that information and, more problematically, the entire biological sample, was deemed inconsequential.²¹⁷

The Second Circuit’s analysis of the impact of the New York DNA database law was similarly dismissive of noncorporeal interests.²¹⁸ The inquiry began with the physical intrusion, which the court easily immediately discarded as *de minimis*.²¹⁹ To its credit, the court then did expressly acknowledge a second, “potentially . . . far greater intrusion than the initial extraction of DNA,”²²⁰ namely the analysis and indefinite maintenance of the profile in a database. But the court observed that the statute “provides only for the analysis of identifying markers,”²²¹ ignoring that the statutes also sanctioned government retention of the entire DNA sample for no apparent purpose. The closest the court came to acknowledging less corporeal concerns, such as the significance of the unrestricted police possession of an individual’s entire genomic code,²²² was to observe that evidence of abuse of samples was “not present here”²²³ and that a range of

214. *Id.* at 836–37.

215. *Id.* at 837–38.

216. *Id.* at 837.

217. *Id.* at 837–38.

218. *See* *Nicholas v. Goord*, 430 F.3d 652, 671 (2d Cir. 2005) (“We therefore conclude that New York’s statute, which serves a special need beyond the normal need for law enforcement, is supported by strong government interests that outweigh the relatively minimal intrusion on plaintiffs’ expectation of privacy.”).

219. *Id.* at 669.

220. *Id.* at 670.

221. *Id.*

222. *See* N.Y. EXEC. LAW § 995-c(5) (McKinney 2007) (“The sample shall be collected, stored and forwarded to any forensic DNA laboratory which has been authorized by the commission to perform forensic DNA testing and analysis for inclusion in the state DNA identification index.”). There is no persuasive argument for retaining samples. Once a sample is typed and entered into the database, it is thenceforth associated with the individual and their identifying information. In the event that the sample should later be shown to match a crime scene, the individual would be arrested and typed again for confirmatory purposes. Thus, retention of the physical specimen—and the wealth of intimate information it contains—is unjustified.

223. *Nicholas*, 430 F.3d at 670.

statutes prohibited the intentional disclosure or misuse of “DNA records”²²⁴ (although notably, not *samples*).

Similarly, although challenges to devices tracking humans have yet to fully be aired, there are some indications of how the Supreme Court has viewed the privacy expectations involved in tracking generally. In *United States v. Karo*²²⁵ and *United States v. Knotts*,²²⁶ the Supreme Court found that the Fourth Amendment was not implicated by the surreptitious planting of electronic tracking devices on moving vehicles to ascertain publicly available knowledge such as the movement of a vehicle on a public street.²²⁷ This reasoning stood even when the obtained information necessarily relied upon the tracking device’s technology—because, for instance, officers had lost sight of the car—so long as the car itself remained in public space.²²⁸ By analogy, it would be easy to argue that the physical intrusion of a monitoring bracelet invades no cognizable expectation of privacy, at least as regards any information other than what individuals are doing within their own homes. Indeed, it is not a stretch to conceive that even the relatively painless implantation of a chip the size of a grain of rice is more akin to a routine DNA blood extraction than an intrusive surgery²²⁹ and likewise permit it without finding any privacy interest infringed.

Finally, an easy case can be made that the capture and storage of facial or other biometric images of an individual similarly compromises no cognizable interest, and therefore does not invoke Fourth Amendment scrutiny at all. That which is “knowingly expose[d] to the public,”²³⁰ like a face or even an iris, receives no Fourth Amendment protection. Indeed, given the degree to which DNA is shed or “abandoned” daily,²³¹ an individual’s entire genetic

224. *Id.* (citing N.Y. EXEC. LAW §§ 995-d(1) to -f) (emphasis added).

225. *United States v. Karo*, 468 U.S. 705 (1984).

226. *United States v. Knotts*, 460 U.S. 276 (1983).

227. *Karo*, 468 U.S. at 711–13; *Knotts*, 460 U.S. at 282–85.

228. *Knotts*, 460 U.S. at 285.

229. *See Schmerber v. California*, 384 U.S. 757, 772 (1966).

230. *Katz v. United States*, 389 U.S. 347, 351 (1967).

231. For instance, in a high-profile Durham, North Carolina, murder case, the prosecution presented evidence of the defendant’s DNA on a Diet Coke can found at the crime scene. John Springer, *Witness Juggling Puts Trial on Hold*, COURT TV NEWS, July 30, 2003, http://www.courtvtv.com/trials/novelist/073003_ctv.html; *see also* David H. Kaye, *Science Fiction and Shed DNA*, 101 NW. U. L. REV. COLLOQUY 62 (2006), <http://www.law.northwestern.edu/lawreview/colloquy/2006/7> (“Shed DNA is a real issue.”).

code is routinely on public display, and courts have held accordingly.²³²

D. Equal Protection

Lastly, it bears mention that the Equal Protection Clause might also be a vehicle for regulating technological restraints on liberty. For instance, Justice Souter, writing separately in *Connecticut Department of Public Safety* and joined by Justice Ginsburg, observed that the registration act's provisions allowing exemptions for certain sex offenders but not others might raise equal protection problems.²³³ Yet numerous obstacles preclude wholesale reliance on equal protection claims.

First, equal protection jurisprudence applies searching scrutiny only to government actions that impinge upon either "fundamental rights" or certain "suspect or semi-suspect" classes like race or gender.²³⁴ Most technological restraints, however, are not expressly imposed along those suspect categorical lines, but rather tie to a status such as prior conviction or allegedly dangerous proclivities. Accordingly, such techniques may likely receive only rational basis review, which tends to grant great deference to government authority.²³⁵

Second, to the extent that the imposition of technologies of restraint does receive closer scrutiny, even under rational basis review, the tools of the Equal Protection Clause have been used to cut more crudely than constructively. Equal protection review tends to be zero-sum, carving out statutory provisions or eliminating a statutory provision altogether. Courts that have invalidated portions of sex offender regulations under rational basis review have effectively excised whole categories of offenders—for instance, by

232. Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment & Genetic Privacy*, 100 NW. U. L. REV. 857, 865–66 & nn.43–45 (2006). For an argument that First Amendment values ought to shape and inform Fourth Amendment inquiries, see Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 151–54 (2007).

233. *Conn. Dep't of Pub. Safety v. Doe*, 538 U.S. 1, 9 (2003) (Souter, J., concurring).

234. Michael C. Dorf, *Equal Protection Incorporation*, 88 VA. L. REV. 951, 962–63 (2002).

235. *Doe v. Phillips*, 194 S.W.3d 833, 844–45 (Mo. 2006) (en banc). *But see* *People v. Kail*, 501 N.E.2d 979, 982 (Ill. App. Ct. 1986) (finding the prosecution of a prostitute under an obscure ordinance requiring bells on bicycles to violate the Equal Protection Clause, even under rational basis review); *ACLU v. City of Albuquerque*, 137 P.3d 1215, 1225–26 (N.M. Ct. App. 2006) (finding sex offender registration not to implicate "fundamental rights" but nonetheless invalidating some of the law's provisions under rational basis review).

excluding individuals required to register because they have prior kidnapping convictions when the conviction contains no sexual coercion component.²³⁶ Equal protection alone, as generally conceived, is an inadequate tool for conducting a more sensitive inquiry, which might find a particular restraint appropriate with the addition of some procedural safeguards or limits on the scope of application (for example, in terms of duration or retroactivity).

E. Summary

In sum, noncorporeal restraints on liberty are currently implemented without any meaningful scrutiny because courts apply an unduly rigid notion of what justifies legitimate procedural and constitutional concern. They fall outside the conventional boundaries of constitutional criminal process because they are not considered “punishment.” They evade scrutiny under either procedural or substantive due process because they do not affect a cognizable “fundamental right” or “liberty interest.” They are not captured by the Fourth Amendment because, despite the promise that the Amendment is about “people, not places,” the physical realm still largely governs the standards for “reasonable expectation of privacy.” And they receive the most deferential scrutiny under the Equal Protection Clause because they do not impinge a fundamental right or regulate a suspect class. In short, as “regulatory” measures not affecting physical liberty, these techniques avoid meaningful scrutiny aimed at delimiting their permissible application.

The *why* of this condition is of less concern than the fact that it exists. That is, it matters not whether the attachment to the physical paradigm stems from a vestigial familiarity with the physical world as the framework through which human beings experience virtual space and identity or whether it derives from a deliberate evaluation of physical restraints as meaningfully different in kind from noncorporeal ones.²³⁷ It is interesting to observe, by comparison, that

236. See, e.g., *Doe v. Moore*, 410 F.3d 1337, 1340 n.1 (11th Cir. 2005) (finding that certain crimes also require a nexus to the sexual offense); *ACLU*, 137 P.3d at 1226 (invalidating registration based on kidnapping and false imprisonment convictions); *State v. Small*, 833 N.E.2d 774, 782–83 (Ohio Ct. App. 2005) (invalidating a provision as applied to a defendant convicted of kidnapping if no sexual motivation were shown).

237. Indeed, as technology continues to bestow a range of options for engaging virtually in the world, questions of space and identity become increasingly complex. A virtual self may have as much dimension and depth as an actual one—perhaps even more. Yet at the same time, no matter how robustly realized the virtual person may be, it is hard to deny the persistent truth of

the Court has hesitated less in recognizing the significance of nonphysical deprivations of property rights; the constitutional protections of the takings clause, for instance, protect both physical and regulatory takings.²³⁸ But whatever the reason for the reluctance to scrutinize regulatory deprivations of liberty, what matters for the purposes of this Article is that, as Part III explains, such techniques can and do effectuate significant harms that merit closer examination.

III. FOUR PHYSICS OF THE NONPHYSICAL WORLD

*These examples and many others demonstrate an alarming trend whereby the privacy and dignity of our citizens is being whittled away by sometimes imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen—a society in which government may intrude into the secret regions of man's life at will.*²³⁹

Across doctrines, judicial supervision of state-imposed restraints on liberty consists primarily, if not exclusively, of appraisals measured in physical terms. An insignificant deprivation of physical liberty triggers constitutional scrutiny, even though extremely burdensome noncorporeal restraints receive little to no scrutiny at all. But phrasing inquiries into the impact of new technologies in outmoded concepts of physical liberty wrongly frames the question. The nature of the burden placed on the individual by the state cannot be captured simply by determining how painful is the blood sampling, how cumbersome is the GPS bracelet, or whether one can feel a face

the physical being. I am reminded of the scene in David Henry Hwang's reinterpretation of *Madame Butterfly*, in which the civil servant Gallimard—having learned that the opera diva with whom he has fallen in love is in fact a man, and not a woman—commits suicide because he cannot overcome the physical sexual identity of his lover, notwithstanding her pleas that “[i]t's the same skin you've worshipped for years. Touch it.” DAVID HENRY HWANG, *M. BUTTERFLY* act 3, sc. 2.

238. Penn. Cent. Transp. Co. v. City of New York, 438 U.S. 104, 124–25 (1978) (setting forth a balancing test for determining what constitutes a regulatory taking). In struggling to define what constitutes a taking, however, the Court has similarly privileged physical deprivations. *Id.* at 125 (“A ‘taking’ may more readily be found when the interference with property can be characterized as a physical invasion by government than when interference arises from some public program adjusting the benefits and burdens of economic life to promote the common good.”). I thank Professor Ron Wright for suggesting this analogy.

239. *Osborn v. United States*, 385 U.S. 329, 343 (1966) (Douglas, J., dissenting) (emphasis added).

scan. Many people would likely agree that a lifetime of electronic monitoring impinges liberty far more severely than one night in jail.

This Part argues that physical deprivation is not the most, and certainly not the only, pertinent referent for understanding the impact and effect of technological restraints. In fact, reliance upon a physical paradigm actively obscures four concerns raised by the use of technological restraints: the ease with which they proliferate, the manner in which they can cumulate, the degree to which they operate without accountability, and the extent to which the harms they impose are invisible. First, whereas technological restraints superficially appear as simply less invasive alternatives to physical restraints, in reality they enhance and increase state power rather than substitute for the exercise of physical control. Second, whereas physical restraints visibly constrain the body, technological restraints cumulate less visibly, exacerbating the threat to liberty in a manner evident only when considered in aggregate. Third, whereas the power of physical restraint rests exclusively in the state, and therefore the state can be held directly accountable for its consequences, technological restraints are wielded by potentially unruly and less readily accountable third parties. Lastly, whereas the harm of physical restraint is manifest and acute, the harms of technological restraints are often contingent and protracted, and therefore are both less visible and less manageable. What follows is an examination of each of these issues in turn.

A. Proliferation

Technological restraints on liberty characteristically present as substitutes for their physical world counterparts. A typical assessment is that technological advances simply hone otherwise ordinary physical mechanisms and thereby render them more efficient, more accurate, and less intrusive. In this view, the electronic bracelet is the less restrictive alternative to the jail cell or on-site surveillance, the DNA sample or biometric scan a more accurate alternative to the fingerprint or eyewitness, and the online record the more efficient alternative to its paper and file counterpart. Rather than question every fan at the ballpark, officers can sit unobtrusively on the sidelines with their facial scanner or DNA swab. Rather than go downtown to retrieve cumbersome paper documents, an officer can just scan an image remotely or a suspicious neighbor can simply run a web search online.

But technologies of restraint do not simply provide more efficient means to the same end. Technology alters—rather than just mechanizes—the relationship between the individual and the state. By way of illustration, consider a recent study of toll rate changes on the interstate highway system. The researcher found that toll rates increased 20–40 percent on thoroughfares that have adopted electronic toll collection systems, like FasTrak or E-ZPass, when compared to those that still relied on manual collection.²⁴⁰ She offered the simple explanation that hidden costs are easily hiked costs—automating the activity of toll collection rendered it not just quicker and more efficient, but in fact changed the nature and salience of the tax imposed.²⁴¹ Anecdotal observations provide additional support for the idea that technology changes, rather than simply optimizes, such relationships. In San Francisco, FasTrak users have specially designated lanes that allow them to pass through timed traffic lights (aimed at regulating signals) at a more rapid pace.²⁴² In central Florida, new highway construction presumes that drivers have Sun Pass systems and relies upon sensors on a bar over the highway to collect tolls; to pass through an actual toll booth to pay with cash, drivers must exit into lanes alongside the regular travel lanes (akin to rest stops).²⁴³ Technology, then, does more than just make traveling with FasTrak more efficient—it also makes traveling without it more cumbersome. By comparison, a no-fly database and iris scanning device may mean that some innocent persons will never be intrusively searched at the airport again, but it also may mean that other innocent persons will *always* be subjected to such searches.

240. Amy Finkelstein, *E-ZTax: Tax Salience and Tax Rates* 34 (Nat'l Bureau of Econ. Research, Working Paper No. 12924, 2007), available at http://www.nber.org/~afinkels/papers/EZTax_Finkelstein_February_07.pdf; see also David Leonhardt, *Technology Eases the Ride to Higher Tolls*, N.Y. TIMES, July 4, 2007, at C1 (“A decade after one [tollbooth] gets electronic tolls, it will be about 30 percent more expensive on average than a similar tollbooth without it. There [is] no shortage of examples: the Golden Gate Bridge, the George Washington Bridge and the Tappan Zee Bridge, among them.”).

241. Finkelstein, *supra* note 240, at 34–35.

242. See Michael Cabanatuan, *FasTrak Bridge Traffic Speedier, Thanks to Faster Metering Lights*, S.F. CHRON., Nov. 7, 2007, at B2 (noting that the highway authority gave “FasTrak users a 10-to-15 percent shorter wait, while delaying cash-payers by a similar amount” and citing a study by the toll authority that FasTrak users on certain highways move faster than cash payers).

243. Associated Press, *SunPass Drivers Will Whiz by New Florida Turnpike Booths*, ST. PETERSBURG TIMES, Jan. 22, 2007, http://www.sptimes.com/2007/01/22/State/SunPass_ldrivers_will_.shtml.

These dynamics of highway travel may very well provide insights into the dynamics of noncorporeal incapacitation of dangerous persons. The constraints of the physical world serve as a major curb on the power of the punitive state. A police department faces a wide range of enforcement options and cannot pursue them all; it must task its officers to those assignments perceived most critical. The same limitations confront the correctional system; already the jails and prisons are bursting at the seams.²⁴⁴ Most ordinary citizens do not worry about the police tailing them or sifting through their curbside trash or peering in their windows—not because the law prevents the police from engaging in such activity, but because simple economics prohibit it from occurring on a wide scale. Resource constraints impose priorities on the exercise of the police power, which in turn curbs excess and abuse.²⁴⁵ The same constraints restrain private acts of vigilance: many people may have an interest in the criminal histories of all their neighbors, but absent some certain benefit in making the task a priority, they simply will not expend the time and energy necessary to figure it out.

The efficiency gains of technological restraints upset these expectations. The economics of the virtual world, although not cost free, are far less prohibitive. Fewer choices must be made. A GPS tag can generate more information about identity or location on far more individuals than a fleet of officers on the beat. It is much simpler to run DNA samples in a database than to pound the pavement looking for witnesses. A camera affixed near a government landmark can generate far more hits when linked to a database than can a police officer monitoring the same traffic by sight. An online web search or registry can offer up more information in a couple hours than could be obtained the old-fashioned way in a couple weeks.

In short, the economics of technological control enable the regulation of greater numbers of persons under less stringent conditions for a longer period of time and to a greater degree than an

244. See SIMON, *supra* note 3, at 2 (“Corrections has become the Pentagon of the state budgets, pushing other service priorities to the side and sending ostensibly conservative governments into a massive buildup of debt.”).

245. A long literature documents and discusses the degree to which municipal and individual decisionmaking is made with biased, racist, or improper motives. See, e.g., DAVID COLE, *NO EQUAL JUSTICE: RACE AND CLASS IN THE AMERICAN CRIMINAL JUSTICE SYSTEM* 16–55 (2005) (detailing examples of biased policing); Alexandra Natapoff, *Underenforcement*, 75 *FORDHAM L. REV.* 1715, 1722–44 (2006) (noting inequalities in the lack of enforcement). But even biased decision making is resource constrained.

equivalent physical intrusion. Even setting aside the capacity to cumulate restraints, which will be addressed in Section B, any single technique of restraint can operate far more pervasively, and reach far more extensively, than its physical-world analogue.

Yet because courts ignore the impediments of the physical world, they likewise ignore the “net widening” that is enabled when its constraints are lifted.²⁴⁶ Appraising the impact of a technological restraint by comparing it to a physical analogue, when the physical world does not dictate the economies of its use, undervalues its potential effect on liberty.²⁴⁷ To return to the examples given at the start of this Section: the face-scanned ballpark attendees could not all have been individually interrogated—they would have been left undisturbed unless they aroused some suspicion. The net-savvy neighbor never would have gotten around to going downtown to check the records in the first place. The crime scene eyewitness would not have been able to identify every cup from which the suspect sipped or the names of family members, including the suspect’s previously unknown biological father. The GPS-tracked individual would not have otherwise gone to jail, but rather would have remained wholly free.

Compare, however, the Supreme Court’s assessment of the harm wrought by the online posting of sex offenders’ biographical information. The Court, analyzing the intrusiveness of the posting, declared that “[t]he record in this case contains no evidence that the Act has led to substantial occupation or housing disadvantages . . . *that would not have otherwise occurred* through the use of routine background checks.”²⁴⁸ The Court further reasoned that the process of searching online “is more analogous to a visit to an official archive of criminal records than it is to a scheme forcing an offender to appear

246. STANLEY COHEN, VISIONS OF SOCIAL CONTROL: CRIME, PUNISHMENT AND CLASSIFICATION 43 (1985). Relatedly, scholars have also reported on the effect of “destructuring movements . . . aimed at decreasing the size, scope and intensity of the formal deviancy control system,” such as diversion and deinstitutionalization programs. *Id.* Rather than shrink the system, however, empirical study demonstrates that “the use of community alternatives actually causes an overall system expansion which might not otherwise have occurred.” *Id.* at 49.

247. Professor Lawrence Lessig has made the same observation with regard to cyberlaw generally: “When the ability to search without burden increases, does the government’s power to search increase as well?” LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 17 (1999).

248. *Smith v. Doe*, 538 U.S. 84, 100 (2003) (emphasis added).

in public with some visible badge of past criminality.”²⁴⁹ In assessing the harm, therefore, the Court dismissed as insignificant the possibility of any change in the likelihood or frequency of intrusion; the analysis centered instead upon whether the intrusion could have occurred in the absence of the technology. In the Court’s own words, online registration simply “makes the document search more efficient, cost effective, and convenient”,²⁵⁰ it did not affect the very meaning of the act of retaining a criminal record.

Yet reducing the difficulty of obtaining such records by placing them online dramatically increases the likelihood, frequency, and scope of their access, and in turn dramatically alters their impact.²⁵¹ The Internet is open twenty-four hours. It requires no bus fare, no plane ticket, no copy card. It has no lines, or clerks on lunch break. A virtual file cannot be checked out or lost as readily as it can in the real world. And a database can be “trolled” and “fished” for information interminably, whereas the same fishing expedition done in person would likely incur the wrath of everyone else in line as well as the staff.

The “visit to an official archive,” in contrast, would likely include all of these impediments. The sheer inconvenience of obtaining paper records thus imposes a de facto screening mechanism: only those individuals deeply invested in obtaining particular information in fact gain access to it. In removing these impediments, the government changes the very meaning of its record keeping. A technically “public record,” filed away in a drawer in a clerk’s office, is simply not identical to the same record—in terms of its publicity—posted online. Whether a record is kept in a drawer at a registry, posted all over town on billboards, or placed on a website largely dictates its publicity—not the label placed on it by law.

The Court’s own analogy in *Smith* reveals as much: one cannot plausibly equate a website with an archive when, for instance, a website might get hundreds of thousands of visitors a day, but the

249. *Id.* at 99 (rejecting the notion that any special significance should be accorded to the fact that online publication magnified the harm by making readily available information that was otherwise cumbersome to obtain).

250. *Id.*

251. For instance, sex offenders in Maine were killed by a Canadian who traveled from Nova Scotia and had used the Internet to identify potential victims in Vermont, New Hampshire, Massachusetts, and Maine. David Hench, *Sex Offender Registries Offer Insight*, PORTLAND PRESS HERALD, Apr. 30, 2006, at A1 (describing how the killer compiled a list before leaving his home in Nova Scotia).

typical county archive might not manage that many in a year. In this respect, the claim that the website simply replicates the archive is demonstrably false. Indeed, the Court itself has previously recognized as much, noting that “[p]lainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.”²⁵²

This disjunction between the realities of the physical world and those of the virtual world are evident across all technologies of control. In the words of one commentator, “[t]echnical developments drastically alter the economics of surveillance such that it becomes much less expensive per unit watched.”²⁵³ Websites cost little to maintain. DNA collection, storage, and processing are becoming less expensive every day, and with automation the expense will continue to drop precipitously. The eyes of biometric technologies can watch far more cheaply than their human counterparts. GPS monitoring costs as little as eight to twelve dollars a day;²⁵⁴ for the cost of one incarcerated body, the government can track six people electronically.²⁵⁵

Moreover, the computerization of information into databases—whether genetic, biometric, biographical or geographical—activates previously passive collections of acquired knowledge. Historically, to say that a record was indefinitely retained did not mean that it was nevertheless instantly available. The file went into the archives to be stored in case it was needed in the future. But computerized methods

252. U.S. Dep’t of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 764 (1989).

253. Ronald Corbett & Gary T. Marx, *Critique: No Soul in the New Machine: Technofallacies in the Electronic Monitoring Movement*, 8 JUST. Q. 399, 400 (1991).

254. William Saletan, *Call My Cell: Why GPS Tracking Is Good News for Inmates*, SLATE, May 7, 2005, <http://www.slate.com/id/2118117>. This sum compares to the estimated sixty-two dollars per inmate daily it requires to incarcerate someone. JAMES J. STEPHAN, U.S. DEP’T OF JUSTICE, STATE PRISON EXPENDITURES, 2001, at 1 (2004), available at <http://www.ojp.usdoj.gov/bjs/pub/pdf/spe01.pdf>. As such requirements have swept the nation, however, questions about the cost of effective implementation have been raised. See, e.g., Michael Rothfeld, *Viability of Sex-Offender Law in Doubt*, L.A. TIMES, Nov. 27, 2007, at A1 (detailing the dispute within California over which agencies must shoulder the significant costs of voter-enacted GPS-tracking laws).

255. Corbett & Marx, *supra* note 254, at 403 (noting that “[p]risons are very expensive institutions, averaging (in 1987 dollars) between \$50,000 and \$75,000 per new cell for construction and \$14,000 for imprisoning one offender for a year”); STEPHAN, *supra* note 253, at 1 (reporting annual operating costs of state prisons at \$22,650 per year per inmate).

of record retention facilitate information exchange and transfer: the file goes in the database, which can then easily be accessed, searched, and shared. As the Supreme Court acknowledged in another context, a significant change occurs when “scattered . . . bits of information” are collected into a “compilation of otherwise hard-to-obtain information.”²⁵⁶ Instead of deploying its scarce resources to canvass for suspects or interview witnesses in one case, the government can run a biometric image or DNA sample and turn up a range of likely candidates in an array of cases.

Indeed, unlike the level or even escalating costs of physical forms of incapacitation, the cost of imposing a technological restraint may decrease over its period of use. Although difficult to quantify, it may be that the costs of technological restraints peak at implementation, both structurally and individually, and then level off or even decline after the initial capital outlay. For instance, although establishing a national DNA database incurs significant costs, fewer expenditures are required to maintain and operate it.²⁵⁷ Similarly, collecting and testing a DNA sample requires funding, but once processed, only minimal costs are necessary to store the sample and profile.²⁵⁸ Many technologies even have built-in mechanisms for recouping their expense: jurisdictions increasingly require solvent defendants to pay for their own electronic tracking devices²⁵⁹ and DNA tests,²⁶⁰ or charge a nominal fee for records searched online.²⁶¹

256. *Reporters Comm.*, 489 U.S. at 764 (finding privacy implicated in the FBI’s dissemination of a rap sheet, which collected publicly available but dispersed conviction and arrestee information into a single document).

257. *See BUTLER, supra* note 23, at 436, 442 (describing the high costs of clearing the backlog of untested DNA and setting up databases, but noting the benefits of making that investment).

258. *See id.* at 442–43 (describing Virginia’s initial need to rely on outsourcing to process its samples until it cleared a backlog and “built . . . capacity”).

259. A number of states require tracked individuals to pay for their tracking. *E.g.*, ALA. CODE § 15-20-26.1 (LexisNexis 2007); ARK. CODE ANN. § 12-12-923 (2007); GA. CODE ANN. § 42-1-14 (2007); MICH. COMP. LAWS ANN. § 791.285 (West 2007); S.C. CODE ANN. § 23-3-540 (2007). The same is true of many SCRAM programs. *See Keeping Watch, supra* note 56 (noting that the “offender must pay the entire cost of participating in the [SCRAM] program, which includes a refundable deposit of \$100, a \$75 installation fee and a daily fee of \$12 for the service”).

260. N.C. OFFICE OF STATE BUDGET & MGMT., N.C. DEP’T OF JUSTICE, COST STUDY OF DNA TESTING AND ANALYSIS 12 (2006) (reporting on various ways in which states recoup costs by imposing surcharges on convicted offenders or court penalties).

261. *See supra* Part I.C.

This myth that technological restraints simply optimize the conditions of the physical world, rather than enable greater degrees of intrusion, in turn often serves to legitimize a second misconception—that technological restraints are always preferable to physical ones. That is, even assuming that technological restraints did apply only in circumstances identical to a physical-world counterpart, they still would not necessarily effectuate an equal, much less smaller, deprivation. Naturally, if asked which is worse, targeted technological surveillance or full-fledged incarceration, few would dispute that surveillance presents the less offensive option. Many people may prefer a year under electronic monitoring to a year in jail, or providing a DNA sample or biometric image for search and storage in a national database to being brought in for questioning.

Rephrase the question as a choice between one day of incarceration and a year of intensive technological surveillance, however, and choosing the least offensive option may appear more complicated. Many people would likely trade a year in jail to avoid a lifetime ban from their hometown or the indelible stigma of public registration. And most people would likely accept the possibility that the police may confront them if there is an individualized suspicion of involvement in criminal activity rather than voluntarily contribute their biological and biometric samples to a government database so that they can be routinely ruled out as a suspect. There is a value in not having to engage with government officials on a prolonged or regular basis that may, in certain circumstances, transcend even the value of personal physical liberty. Indeed, it is not for nothing that some defendants actually prefer a jail term to probation,²⁶² or that most people dread engaging government bureaucracies over even the most rudimentary of tasks such as securing a driver's license or picking up a package at the post office.

262. See *State v. Cooley*, 587 N.W.2d 752, 753 (Iowa 1998) (reporting that defendant Michael Cooley did not desire the “problems and harassment” accompanying any form of probation and therefore “would rather serve his [*sic*] whatever time he gets rather than being put on probation for this”); Lawrence Van Gelder, *Arts, Briefly*, N.Y. TIMES, Apr. 27, 2006, at E2 (reporting that actress Michelle Rodriguez, faced with the choice of going to jail for five days or paying a \$500 fine and spending 240 hours performing community service for a drunk driving charge, chose jail saying “I kind of have to get back to my life”). Another celebrity, Kiefer Sutherland, prioritized his ability to work over his personal freedom: he elected to serve a forty-eight-day jail sentence in two stints that would not conflict with the filming of his popular television show, rather than a shorter period of time that would have interrupted the schedule. Associated Press, *‘24’ Star Pleads No Contest in DUI Case, To Serve 48 Days*, CNN.COM, Oct. 10, 2007, <http://www.cnn.com/2007/SHOWBIZ/TV/10/10/sutherland.arrested.ap>.

But the very same courts that use incarceration as the point of comparison in assessing the harm wrought by a particular technology in turn neglect to ask whether the technology was imposed with the specificity or procedural protection remotely approximating that required for the purportedly comparable physical deprivation. For example, in *In re Commitment of William P. Browning*,²⁶³ a Texas Court of Appeals addressed that state's sexual predator commitment act, which allowed for "outpatient" commitment using electronic surveillance.²⁶⁴ The court compared the restrictions imposed—GPS tracking, residence in a specific county, and treatment—to the incarceration upheld by the Supreme Court in *Kansas v. Hendricks*.²⁶⁵ Observing that "the intrusion is far less restrictive than if he were confined in a secure facility,"²⁶⁶ the court upheld the requirements as "nonpunitive," but it never considered whether the qualifying processes for outpatient commitment were likewise identical to involuntary inpatient commitment.²⁶⁷ Similarly, the large number of sexual offenders currently required to submit to ten-year to lifetime terms of GPS monitoring almost certainly could not all have been, pursuant to the procedural standards imposed by the Supreme Court, physically incarcerated.²⁶⁸

The same logic is evident with regard to online index cases. In *E.B. v. Verniero*,²⁶⁹ for instance, the Third Circuit upheld a sex offender registry, noting that dangerous sex offenders can be detained both pretrial and postsentence through civil commitment procedures.²⁷⁰ The court commented that, in contrast, "[a]ll Megan's Law mandates is registration and notification"²⁷¹ and "[c]ertainly, in terms of the impact on the everyday lives of registrants, the burden of

263. *In re Commitment of William P. Browning*, 113 S.W.3d 851 (Tex. App. 2003).

264. *Id.* at 857.

265. *Kansas v. Hendricks*, 521 U.S. 346 (1997).

266. *In re Commitment of Browning*, 113 S.W.3d at 859.

267. *Id.* at 858.

268. Physical commitment has been held constitutional if accompanied by fairly elaborate procedural safeguards approximating those available in a criminal trial. *Kansas v. Crane*, 534 U.S. 407, 409 (2002); *Seling v. Young*, 531 U.S. 250, 267 (2001); *Hendricks*, 521 U.S. at 366. But the persons subject to technological surveillance are not necessarily limited to only those adjudicated eligible for physical commitment. *See supra* Part I.

269. *E.B. v. Verniero*, 119 F.3d 1077 (3d Cir. 1997). This case focused on the original "Megan's Law," named after a child who was brutally raped and murdered by a convicted sex offender.

270. *Id.* at 1104–05.

271. *Id.* at 1102.

this aspect of Megan's Law pales by comparison to the civil commitment of sex offenders.²⁷² Other courts have followed similar reasoning, concluding that "[a]lthough we recognize that the duty to register in person every 90 days for a minimum of ten years is onerous, we do not believe that this burden is sufficiently severe to transform an otherwise nonpunitive measure into a punitive one," because "the Supreme Court has consistently upheld far heavier burdens . . . including deportation, termination of financial support, and loss of livelihood."²⁷³ Yet no court acknowledged that, the higher burdens of the analogous condition also carried more stringent procedural safeguards. Such protections, not the least of which is individualized process—restrict the power of civil commitment or deportation, whereas no such limitations circumscribed the application of registration statutes, which generally apply indefinitely and on the basis of categorical membership.

Conversely, courts have also failed to appraise the additional burdens imposed by technological restraints that are lacking in the case of their physical counterparts and which therefore might warrant additional procedural protections. For instance, the Supreme Court in addressing sex registries in *Connecticut Department of Public Safety* specifically rejected the need for individualized assessments of eligibility for regulatory registration statutes because the Court claimed that, to the extent that any process was necessary, it had already been provided in the criminal trial at which the defendant was adjudicated guilty of an offense.²⁷⁴ Publication of an already public offense, by itself, did not occasion any need for additional procedural safeguards.²⁷⁵

Yet the Court's logic overlooks the fact that in enacting the registry, the state is both demanding more and doing more than is possible in the physical world. Online registries contain more information, and saddle registrants with a greater burden, than the

272. *Id.* at 1105.

273. *Doe v. Pataki*, 120 F.3d 1263, 1285 (2d Cir. 1997). Several courts have drawn the same analogy. *See, e.g., Doe v. Sex Offender Registry Bd.*, 697 N.E.2d 512, 519 (Mass. 1998) ("The offenders in these cases do not face a potential loss of liberty . . ."); *Commonwealth v. Williams*, 832 A.2d 962, 982 (Pa. 2003) ("[T]he duties imposed . . . are not in themselves sufficiently onerous to qualify as punishment.").

274. *Conn. Dep't of Pub. Safety v. Doe*, 538 U.S. 1, 7 (2003) ("[T]he law's requirements turn on an offender's conviction alone—a fact that a convicted offender has already had a procedurally safeguarded opportunity to contest.").

275. *Id.*

simple historical fact of conviction. They demand constant, long-term attention on the part of registrants, in that the individual must periodically check in to verify information and provide current photos, and must immediately inform the government of any material changes in their status.²⁷⁶ The registries, in turn, consist of current and updated repositories of information about the status, residence, employment, and appearance of registered persons. This change in both the breadth and the character of the availability of the information constitute highly meaningful distinctions. Statutes that allow the broadcast of public court proceedings—but give victims and witnesses the opportunity to opt out—recognize as much.²⁷⁷ A public proceeding that requires finding a parking space, locating the right courtroom, and sitting through lunch breaks and irrelevant matters is simply not the same thing as a public proceeding that requires no more than flipping on the television and fast-forwarding to the relevant part. Thus, confronting the issue in *Smith*, the Court wrongly analogized an inquiry into a sex offender registry to “a visit to an official archive,”²⁷⁸ because the “official archive” would not be open twenty-four hours a day and have, as did the registry, a current photo of the individual along with current information about the person’s address, workplace, or other biographical characteristics.

In sum, the right story to tell about technological forms of surveillance and control is not one of streamlining or one-for-one substitution, but rather one of proliferation, expansion, and enhancement. Blinded by the economics of the physical world, courts overlook the far more productive economies of virtual control. And focused on the strictures that govern what appears to be a more restrictive physical alternative, courts neglect to ask whether the more restrictive option would apply or, even if it did, whether any distinct burdens of the technological restraint demand some special procedural due process.

276. See *supra* Part I.C.

277. See Audrey Maness, Comment, *Does the First Amendment’s “Right of Access” Require Court Proceedings to Be Televised? A Constitutional and Practical Discussion*, 34 PEPP. L. REV. 123, 147 & n.199 (2006) (“Many court rules also provide for exclusion of select testimony based upon objections from certain classes of persons: namely, victims, informants, undercover agents, relocated witnesses, or juveniles.”).

278. *Smith v. Doe*, 538 U.S. 84, 99 (2003).

B. Accumulation

The use of the physical world as the template for understanding the effects of noncorporeal restraints on liberty obscures more than just the net-widening effect of such restraints. It also can detract from full analysis of the degree to which such restraints can cumulate. Although each individual restraint may seem trivial in an isolated appraisal, a comprehensive review, focused on the regulated subject rather than a particular restraint, can reveal the true severity of such measures' potential reach. Discrete technological restraints on liberty can accumulate and fully fetter an individual while remaining largely disaggregated for purposes of assessing their effect.

That is, physical regulations of dangerous persons are easy to map: the body is free in society, the body is restrained in prison. Even when multiple legal forms of restraint operate—say, the same person is released in a criminal matter but detained in an immigration matter—the legal system can, and does, keep track of the actual physical self. For example, a court has to order corrections to make present the immigration-detained defendant to proceed in a criminal trial, even if the defendant is fictionally “free” in that criminal case. The institution of incarceration tracks the individual. The fiction of physical freedom even retains legal import: if the immigration interest dissipates, the physical self likewise will be freed.

But technological regulations operate virtually, fragmented from one another and difficult to view cumulatively. For example, imagine a hypothetical offender—say, a nineteen-year-old male convicted of having sex with his fifteen-year-old girlfriend. He finishes a jail term as well as a period of supervised release. Yet he remains governed by a web of technology-based surveillance requirements. Pursuant to a series of nondetention-based statutes, his criminal record will be placed online alongside his identifying information, home address, place of work, photograph, and the make and model of his car. Once every three months or so, he will have to spend the morning down at the local law enforcement office, verifying his information or providing an update. In between those visits, if he moves, or borrows a car, or cuts his hair, he will have to notify law enforcement.

At the same time, his DNA and fingerprints will be stored in a computer so that roughly one hundred thousand times a day, his biometric profile will be checked for comparison with a crime-scene

sample.²⁷⁹ His whole biological genome will sit in a police refrigerator, subject only to bare and vague restrictions on its misuse.²⁸⁰ Perhaps his facial features or license plate will be recorded electronically, so that whenever he boards a plane or drives by a playground he can be identified as a potential suspect. His every movement will be tracked electronically so that the government can know his location at all times. He may have to abide by zoning ordinances that prohibit him from living near a school or visiting a public park—or perhaps even any metropolitan area—and a GPS or biometric-based alert will sound or barriers will go up if he accidentally travels within the prohibited zones. In short, each time he enters the public sphere he will risk exposure—to a security guard with a biometric scanner, to a police officer who runs a crime scene cigarette butt through the database, or to a web-surfing vigilante neighbor who thinks that criminals like him should be chased out of town.

Despite all of these encumbrances, he will not only be considered fully free in the eyes of the law, but he will also hardly even be considered fettered. Had the state wished to incarcerate him criminally, he would have received full criminal process. Had the state sought civil incapacitation, say as a sexual offender or danger to the community, it would have likewise needed to meet some measure of heightened and individualized proof. But each of the regulations that constitute his virtual prison will have triggered barely any attention, and will almost certainly apply absent any individualized determinations or formal limitations on duration or scope. None will turn on any reference to, much less finding of, his likelihood of posing any danger to society.

Moreover, even if he wanted to contest these restraints, this fictional offender would have a hard time presenting to a court a coherent, cumulative picture of his oppression. Each instance of regulation—the online index, the DNA sample, the biometric image, or the GPS bracelet—constitutes its own independent intrusion. Considered separately, each may appear *de minimis*—no single

279. Nakashima, *supra* note 99 (“[A] request reaches an FBI server every second from somewhere in the United States or Canada, comparing a set of digital fingerprints against the FBI’s database of 55 million sets of electronic fingerprints. A possible match is made—or ruled out—as many as 100,000 times a day.”).

280. Antony Barnett, *Police DNA Database Is “Spiraling Out of Control,”* OBSERVER (London), July 16, 2006, at 4 (reporting scandals in England regarding a private company’s retention of genetic samples sent to a lab for outsourced testing, as well as reports that the Home Office gave permission for controversial genetic studies to be conducted on samples).

measure presents as particularly burdensome or unreasonable.²⁸¹ But neither does any basis exist for considering them together: there is simply no legal claim of “it is all too much,” or even “put all together, it is basically a form of jail.”

And even if the harm could be assessed cumulatively, there would remain a practical impediment to objecting to each aspect of its imposition. Technological restraints come to court cloaked in legal claims of various stripes, often dictated by the way in which the intrusion was imposed. First, each restraint may have a different source of legal authority. For instance, the legislature might impose DNA collection and electronic tracking requirements,²⁸² whereas the executive (say, the local police department) creates a biometric database or online index.²⁸³ Without a single comprehensive statute to challenge, or even necessarily a single source of legal authority to point to, it can be difficult to make the case for a broad form of relief. Second, these different sources of authority may express themselves through different officers of implementation even within a particular branch. The corrections office might take the DNA sample and affix the GPS bracelet, the police department might monitor the tracking data or run DNA database searches, and the parks or housing department might issue the exclusion orders and snap the biometric images.²⁸⁴

Moreover, across the states, the implementing authority can also vary such that a different constellation of agencies and offices regulate implementation of a particular program.²⁸⁵ For example, in a 2001 report on state sex offender registration acts that compiled an appendix tracking the relevant authority for each state, a broad catchall “other agency” category was necessary—second only to the “State Patrol” category—to capture the administrative complexity.²⁸⁶

281. One court noted that even within a single statutory regulation scheme, “looking at each provision in isolation tends to artificially dilute the overall impact of the ordinance.” *ACLU v. City of Albuquerque*, 137 P.3d 1215, 1225 (N.M. Ct. App. 2006).

282. *See supra* notes 30–34, 66–68 and accompanying text.

283. *See supra* notes 52–53, 101–114 and accompanying text. Increasingly, however, states have moved to enact legislation providing for GPS tracking of certain offenders. *See, e.g.*, N.J. STAT. ANN. § 30:4–123.92 (2007) (providing for “the continuous, satellite based monitoring of sex offenders in this State”).

284. *See* Katherine Beckett & Steve Herbert, *Dealing with Disorder: Social Control in the Post-Industrial City*, 12 THEORETICAL CRIMINOLOGY 5, 10–16 (2008) (describing a wide spectrum of official authorities capable of generating spatial exclusions).

285. *See* ADAMS, *supra* note 68, at 5.

286. *Id.*

A single individual, required to meet a panoply of requirements across several jurisdictions, would be incapable of presenting a unitary claim. The caption of the case and name of the defendant will likely differ for each technology and within each jurisdiction.

Third, the timing and nature of a legal challenge to one type of technological restraint might be dictated by concerns that do not apply equally to all other forms of restraint. For instance, if the government purchases software that transforms a database of already-obtained driver's license images into a biometric resource, then a regulated subject may be unaware of its use until a particular intrusion occurs. Accordingly, challenges to such a technology might occur piecemeal in criminal cases by individual defendants detained or arrested after being identified by a positive scan. On the other hand, if the government affirmatively seeks images from certain segments of the population, or if legislation is enacted requiring that certain classes of persons submit such images (as in the case of DNA or offender registries, for instance), then a civil class action might follow. In such a case, the practical ability to mount a comprehensive challenge, based on a range of applicable technological restraints, presents a formidable obstacle.

The litigation around these technologies reflects this complexity in the legal bases for their challenges. Claims related to DNA collection statutes, which have thus far primarily addressed DNA collected from convicted offenders, have tended to raise Fourth Amendment arguments in both criminal and civil cases, and *ex post facto* or double jeopardy claims of previously convicted persons.²⁸⁷ Litigation on sex offender registration acts, meanwhile, has tended to focus on equal protection or substantive or procedural due process claims,²⁸⁸ although *ex post facto* and double jeopardy claims have been raised as well.²⁸⁹

In no case, however, does it appear that an individual has challenged multiple restraints—for instance, a sex offender

287. See *supra* Part II.

288. See *Doe v. Phillips*, 194 S.W.3d 833, 842 (Mo. 2006) (en banc) (rejecting a host of state constitutional challenges to the state's registration act, including a substantive due process claim).

289. See *E.B. v. Verniero*, 119 F.3d 1077, 1111 (3d Cir. 1997); *ACLU v. City of Albuquerque*, 137 P.3d 1215, 1221 (N.M. Ct. App. 2006) (upholding city's sex offender registration act against *ex post facto*, double jeopardy, and cruel and unusual punishment attack, but striking certain provisions as violating federal constitutional substantive due process, equal protection, and the Fourth Amendment).

challenging registration, tracking, and DNA collection. There simply is no obvious single legal mechanism for claiming that the technological restraints, operating collectively, impose such a burden that some sort of check is required.²⁹⁰

C. *Unaccountability*

The harms wrought by technological restraints are difficult to visualize not only because they are often diffused into component fragments of regulation, but also because they may be imposed not by the state itself directly, but by a third party. Although physical punishment is the monopoly of the state,²⁹¹ virtual punishment may be meted out by the masses. If an individual cannot rent an apartment or find a job because of an online record, who is responsible? If a vigilante threatens to violently assault or even kill someone based on a registry, who is responsible? If an airline prevents an individual from boarding a flight because a commercial database contains inaccurate information, who is responsible? Likely, not the state.

The state action requirement for constitutional challenges permits the state to distance itself from the consequences of its use of technological restraints.²⁹² Whether it is a private employer denying a job, a landlord denying housing, a community member defacing property, or any of the myriad ways in which the regulated individual may face violence or discrimination, it need not be attributable to state action. Conversely, the state may collect information from third parties and then evade any obligation to verify or correct it if erroneous. For instance, because commercial databases are relied

290. Indeed, some courts expressly forbid a claim under one provision of the Constitution when the same claim better fits another part of the Constitution. *See, e.g.*, *Dubbs v. Head Start, Inc.*, 336 F.3d 1194, 1203 (10th Cir. 2003) (“[W]here a particular Amendment provides an explicit textual source of constitutional protection against a particular sort of government behavior, that Amendment, not the more generalized notion of substantive due process, must be the guide for analyzing these claims.” (quoting *County of Sacramento v. Lewis*, 523 U.S. 833, 842 (1998))).

291. *See, e.g.*, MAX WEBER, *POLITICS AS A VOCATION 2* (Fortress Press 1965) (1918) (defining a state as an entity which claims a monopoly on the legitimate use of physical force in a given territory); Donald Dripps, *The Exclusivity of the Criminal Law: Toward a “Regulatory Model” of, or “Pathological Perspective” on, the Civil-Criminal Distinction*, 7 J. CONTEMP. LEGAL ISSUES 199, 207 (1996) (“A monopoly on legitimate violence must be established in a government, and that government must commit itself to respecting the law in exercising its monopoly.”). *But see* Ric Simmons, *Private Criminal Justice*, 42 WAKE FOREST L. REV. 911, 911 (2007) (reporting the emergence of an “alternative private criminal justice system”).

292. Simmons, *supra* note 291, at 911 (describing the limited operation of the state action doctrine even with regard to private police).

upon to generate no-fly lists, the government can “circumvent the Privacy and Information Act” along with laws giving individuals the right to see and challenge such information.²⁹³ Indeed, states and localities have increasingly delegated a dimension of the police power to private entities, so that for instance a quasi-public housing development could use a registry to permanently bar individuals from its grounds—without employing any formal process—and then seek arrest in the case of subsequent trespass.²⁹⁴ The arrested individuals have no basis upon which to defend against the trespass, even if the barring notice were issued from their own homes and without notice or the opportunity to be heard.²⁹⁵

In contrast, even in this era of privatization, the authority to incarcerate the dangerous still rests solely with the state. Whatever its actual efficacy in political terms, this power renders the government democratically accountable for the harms it imposes on an individual. Such accountability has legal resonance as well. In depriving an individual of liberty the state in turn assumes a range of affirmative duties to provide for the health, sustenance, shelter, and general maintenance of its inmates,²⁹⁶ and the writ of habeas corpus provides an avenue of relief from wrongful incarceration. When individuals are sent to prison, it is unambiguous where they are, who sent them there, and who is responsible for their continued welfare.

293. Dummer, *supra* note 94, at 268 (explaining that such databases are privately maintained, and that no statutory regulation akin to the Fair Credit Reporting Act or other watchdog-type legislation exists to entitle individuals to access to or correction of wrong information); Linda L. Lane, *The Discoverability of Sensitive Security Information in Aviation Litigation*, 71 J. AIR L. & COM. 427, 427 (2006) (“A plaintiff’s inability to access Sensitive Security Information (‘SSI’) often defeats that plaintiff’s claim that he was harassed or denied boarding without cause.”).

294. Although this added layer of complexity is beyond the scope of this Article, an example of such action is evident in *Virginia v. Hicks*, 539 U.S. 113 (2003), in which the Supreme Court addressed a “trespass notice” issued by the Richmond Redevelopment and Housing Authority (RRHA), *id.* at 117. The RRHA, a “political subdivision of the Commonwealth of Virginia” that operates a low-income housing project in Richmond, purchased a previously public street from the city and then pursued trespass complaints against undesirable visitors to the development. *Id.* at 116–18. Addressing a First Amendment claim based on the “unfettered discretion” of the housing project’s manager to permanently ban visitors without any process or recourse, *id.* at 121, the Court held the policy sufficiently legitimate to overcome an overbreadth challenge, *id.* at 124.

295. *Id.*

296. *Estelle v. Gamble*, 429 U.S. 97, 103–04 (1976) (holding that the state owes a duty of care to those in its custody); *see also* *Youngberg v. Romeo*, 457 U.S. 307, 315 (1981) (noting in a due process claim by an institutionalized individual that “the State concedes that respondent has a right to adequate food, shelter, clothing, and medical care”).

But technology enables the state to delegate to the populace a share of its role in monitoring and controlling the dangerous. And even though monitoring technologies can approximate the harms imposed by incarceration in that they restrict the ability to work, associate, sleep, eat, and live as one chooses—generally speaking, imposing a “[l]oss of freedom of choice and privacy” similar to that occasioned by jail²⁹⁷—it will no longer technically be the government that metes out the punishment. Accordingly, any harms suffered as a result need not be its responsibility. The fictional offender described in Section B, who has trouble working or finding an apartment or even living without fear of random violence, will therefore lack something retained by those incarcerated: the right to hold the state accountable for affirmatively providing for his shelter, livelihood, health, and safety.

Indeed, the closest avenue for challenging government actions that adversely affect an individual as a result of the behavior of third parties is to cite the reputational harm a regulation imposes. Underlying the objection that a particular technique “stigmatizes” an individual is the notion that, even if the government is not itself oppressing or harming the person, it is approving or even inviting such harm by third parties. Yet the claim that a government action imposes “stigma” on an individual, or otherwise harms “reputation,” has repeatedly been rejected by the Court. In *Paul v. Davis*,²⁹⁸ which involved the distribution by police chiefs of a flyer displaying “active shoplifters,” the Supreme Court held that “defamation, standing alone,” does not deprive any protected liberty interest.²⁹⁹ In

297. *Bell v. Wolfish*, 441 U.S. 520, 537 (1979). See generally GRESHAM M. SYKES, *THE SOCIETY OF CAPTIVES: A STUDY OF A MAXIMUM SECURITY PRISON* 63–83 (Atheneum Printing 1970) (1956) (documenting and cataloging the effects of imprisonment as a deprivation of liberty, goods and services, sexual freedom, autonomy, and security).

298. *Paul v. Davis*, 424 U.S. 693 (1976).

299. *Id.* at 709. In fact, the Court in *Paul* used this basis to distinguish *Wisconsin v. Constantineau*, 400 U.S. 433 (1971), which found a liberty interest in the purchase of liquor that had been denied without due process when the chief of police posted a notice forbidding the sale of liquor to the defendant for one year, *id.* at 433. The opinion suggested that the problem was that the notice was “a stigma, an official branding of the person” in a “degrading” manner, without prior notice or opportunity to be heard. *Id.* at 437. The Court held, “Where a person’s good name, reputation, honor, or integrity is at stake because of what the government is doing to him, notice and an opportunity to be heard are essential.” *Id.* But the *Paul* Court reinterpreted the holding as not about stigma, finding that such an interpretation “could be taken to mean that if a government official defames a person, without more, the procedural requirements of the Due Process Clause . . . are brought into play.” *Paul*, 424 U.S. at 708. Instead, the linchpin was that the state action caused “a right or status previously recognized by

Connecticut Department of Public Safety, the Court declared that “mere injury to reputation, even if defamatory, does not constitute the deprivation of a liberty interest.”³⁰⁰ And in *Smith v. Doe*, the majority observed that any “attendant humiliation” or, for that matter, violence, that resulted from the online registry was therefore “but a collateral consequence” for which the state was not responsible.³⁰¹

By disavowing stigma as a legally cognizable harm, the state can brand the individual publicly while simultaneously disclaiming any responsibility for public reaction. But this lack of accountability enables serious incursions on liberty at a potentially high cost. As one scholar has commented in the context of shame punishments, such forms of delegation forge “an improper partnership between the state and the crowd.”³⁰² Delegation raises the specter of uncontrolled violence and arbitrary imposition of punishment³⁰³ in that the individual is in essence “compelled to dance with a madman,” and has “no way to predict or control the way in which the public will deal with him,” or any “rhyme or limit to the terms the public may impose.”³⁰⁴

And indeed, such violence and arbitrary discrimination has already occurred. Justice Souter, concurring in *Smith v. Doe*, observed that “there is significant evidence of onerous practical effects of being listed on a sex offender registry.”³⁰⁵ In support of this claim, he cited evidence of “numerous instances in which sex offenders have suffered harm in the aftermath of notification—ranging from public shunning, picketing, press vigils, ostracism, loss of employment, and eviction, to threats of violence, physical attacks, and arson,”³⁰⁶ along with instances of “private, unlawful violence and

state law [to be] distinctly altered or extinguished.” *Id.* at 711. Because “any harm or injury to that interest [in reputation] . . . does not result in a deprivation of any ‘liberty’ or ‘property’ recognized by state or federal law,” it needs no procedural safeguarding. *Id.* at 712.

300. *Conn. Dep’t of Pub. Safety v. Doe*, 538 U.S. 1, 6–7 (2003).

301. *Smith v. Doe*, 538 U.S. 84, 99 (2003).

302. James Q. Whitman, *What Is Wrong with Inflicting Shame Sanctions?*, 107 *YALE L.J.* 1055, 1059 (1998).

303. The debates surrounding the use of shaming penalties contain a parallel critique—specifically, that such penalties “involve a dangerous willingness, on the part of the government, to delegate part of its enforcement power to a fickle and uncontrolled general populace.” *Id.* at 1088.

304. *Id.* at 1090–91.

305. *Smith*, 538 U.S. at 109–10 n.* (Souter, J., concurring).

306. *Id.* (quoting *Doe v. Pataki*, 120 F.3d 1263, 1279 (2d Cir. 1997)).

threats” that “happen with sufficient frequency and publicity that registrants justifiably live in fear of them.”³⁰⁷ One couple in California sued the seller of a home they purchased, claiming he should have disclosed that he was a registered sex offender.³⁰⁸

Equally as troubling, the repercussions of these tools of surveillance are amplified in this age of information. Some general label of dangerousness may matter less when it is restricted by person-to-person contact—such as in a small town, where everyone knows the local felon who in turn either tolerates the ostracism or moves far enough away that a reputation is not likely to follow. But in a global society, such restraints can seriously inhibit freedom. More and more, individuals are constructed as compilations of abstract data in “digital dossiers.”³⁰⁹ Once labeled as a transgressor, it no longer is plausible to move towns or switch jobs to avoid permanent adverse consequences, much less stop driving or flying or going to the supermarket altogether. Regulatory provisions easily combine to force a life out of the public eye, which in these days may very well be impossible. Public isolation—whether due to the officers who always pick the same car to pull over on the highway or the employer who denies the only eligible job—can vastly impair the ability of an individual to live any kind of ordinary life.

D. Invisibility

Finally, technological restraints differ from their physical counterparts in that they acquire control over the regulated individual largely through the threat of sanction, rather than through the imposition of the sanction itself. Because they realize an abstracted form of disciplinary control, they are less visible and transparent.³¹⁰ Of course, some techniques exert manifest, evident power: a tracking

307. *Id.* (quoting *E.B. v. Verniero*, 119 F.3d 1077, 1102 (3d Cir. 1997)); see also Brief for Office of the Pub. Defender for the State of New Jersey et al. as Amici Curiae at 7–21, *Smith v. Doe*, 538 U.S. 84 (2003) (No. 01-729) (noting past instances of physical assault and harassment).

308. Eric Louie, *Seller's Sex-Offender Status Angers Alamo Home Buyers*, *CONTRA COSTA TIMES*, (Cal.) May 29, 2007, at A3.

309. Solove, *Digital Dossiers*, *supra* note 16, at 1084; see also MARK POSTER, *THE SECOND MEDIA AGE* 90 (1995) (“With databases, most often, the individual is constituted in absentia . . .”).

310. Many have written, perhaps most famously Michel Foucault, on the disciplinary power of panoptic institutions. MICHEL FOUCAULT, *DISCIPLINE & PUNISH: THE BIRTH OF THE PRISON* 215–16 (Alan Sheridan trans., 2d ed. 1995) (describing the formation of a “disciplinary society” characterized by “an indefinitely generalizable mechanism of ‘panopticism’” that evolves from formal institutions of power or control).

device or biometric tool might foreclose access (or at least alert others of unauthorized access) to certain places or activities. If the gate comes down on the wayward sex offender too close to a school or the barricade rises to cordon off the car with the errant license plate, then a physical exertion of control undoubtedly occurs.

But technologies of detection are also ones of noncorporeal restraint. GPS tracking or online indexing or biometric or DNA databasing need not *physically* curtail the individual's ability to move through society freely, because they achieve their deterrent and incapacitating effect through their capacity to sanction.³¹¹ They “control a specific population by confining them, not within geographical space, but through the dispersed trap of enhanced detection.”³¹² Like Jeremy Bentham's famous Panopticon,³¹³ technological restraints are both visible (in that the subjects know they *might* be watched) and unverifiable (in that they do not know *when* they are being watched). This virtual exercise of the state's power can in fact “render its actual exercise unnecessary.”³¹⁴

Consider DNA typing and databasing—likely the most detective, rather than preventive, technique of those discussed here. Arguably DNA databases can do no more than link offenders to completed crimes; they are not methods of physical incapacitation or of strict crime prevention. But in fact genetic databasing constitutes a powerful means of preventive restraint in the form of deterrence. It interposes the watchful eye of the state between the offender and the potential offense. As one scholar vividly describes, DNA databases represent “nothing short of a spectral intervention into criminal activity by forming the permanent shadow of an ever-present witness.”³¹⁵ This patrolled subject is self-circumscribing—“[h]e who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play

311. Indeed, in contrasting penal confinement with nonrestraining punishments, Professor Frank Zimring observed that “[t]he distinction between influence and control is somewhat moderated when temporal limits are imposed on incapacitation and when a quick response potential is built into monitoring systems.” FRANK ZIMRING, *INCAPACITATION* 157 (1995). After all, “well-designed monitoring systems that can respond rapidly to initial deviance may exercise more effective control over a population in the middle term than intermittent periods of secure confinement.” *Id.*

312. Williams & Johnson, *supra* note 17, at 11.

313. FOUCAULT, *supra* note 310, at 200.

314. *Id.* at 201.

315. Williams & Johnson, *supra* note 17, at 12.

spontaneously upon himself.”³¹⁶ Throwing away a soda can in a public trash bin becomes an assertion of territory, rather than a transient event.

In this respect, technological methods of regulating dangerous individuals exercise control not by cabining the capacity of the individual to self-actuate, but by narrowing the landscape in which one may do so without an actual or perceived risk of interference by others or the state.³¹⁷ That is why calls for a universal DNA database have been largely rejected,³¹⁸ and likely will always be—not because the vast majority of the population actually anticipates committing a crime in the future and hopes to avoid detection, but because even the most law-abiding of individuals can experience the threat of (even false) exposure as oppressive. It is that oppression—the omnipresent eye of the state—that embodies the harm done by technological restraints. A SCRAM-bracelet wearer’s inability to use perfume or mouthwash is not the gravitas of injury; it is the constant fear of detection, exposure, or capture.

Philosopher Isaiah Berlin expresses this idea in his definition of liberty as a dual concept: “positive freedom,” which “consists in being one’s own master,”³¹⁹ and “negative freedom,” or the freedom of “not being interfered with by others.”³²⁰ “Positive freedom” embodies the desire to “be somebody, not nobody; a doer—deciding, not being decided for, self-directed and not acted upon by external

316. FOUCAULT, *supra* note 310, at 202. Foucault noted that the patrolled subject “becomes the principle of his own subjection.” *Id.* at 203.

317. In this respect, it is the object of controlling information, rather than the means by which it is controlled, that matters. Professor Mark Poster observes that:

Properly understood the panopticon is not simply the guard in the tower but the entire discourse/practice that bears down on the prisoner, one that constitutes him or her as a criminal. The panopticon is the way the discourse/practice of the prison works to constitute the subject as a criminal and to normalize him or her to a process of transformation/rehabilitation. My argument is that, with the advent of computerized databases, a new discourse/practice operates in the social field, a super-panopticon if you will, which reconfigures the constitution of the subject.

POSTER, *supra* note 309, at 85.

318. See, e.g., Nigel Morris, *A ‘Chilling’ Proposal for a Universal DNA Database*, INDEPENDENT (London), Sept. 6, 2007, available at http://findarticles.com/p/articles/mi_qn4158/is_20070906/ai_n19519872; Weiss, *supra* note 35, at A1. But see D.H. Kaye & Michael E. Smith, *DNA Identification Databases: Legality, Legitimacy, and the Case for Population-Wide Coverage*, 2003 WIS. L. REV. 413, 415 (2003).

319. ISIAH BERLIN, *Two Concepts of Liberty*, in *FOUR ESSAYS ON LIBERTY* 118, 131 (1969).

320. *Id.* at 122–23.

nature”³²¹ It is the freedom of self-direction and self-realization. In contrast, “negative freedom” acknowledges that “a frontier must be drawn between the area of private life and that of public authority.”³²² It is this “minimum area of personal freedom” that is a necessary precondition to positive freedom, or to creating the conditions in which an individual can be “a being with a life of his own to live.”³²³ Professor Robert Post describes a similar interest in the maintenance of “the forms of respect deemed essential for social life.”³²⁴ He specifically distinguishes this critical sphere of autonomous will from abstract notions of intimacy or seclusion, and relates it wholly to the formation and preservation of the independent self.³²⁵

When the state imposes physical incarceration, it strips the individual of both types of freedom: the prisoner loses both the capacity for self-determination and the right to noninterference. But a state using technologies to regulate a dangerous person, in contrast, leaves the former interest largely untouched while greatly undermining the latter.³²⁶ An individual who must wear a GPS bracelet, supply updated biographical information to an online index, or submit to genetic or biometric surveillance is not, it is true, prevented by the state from self-direction. Indeed, courts repeatedly focus upon this positive freedom in justifying the technological intrusion, noting for instance in the sex offender registration statute cases that “[a]lthough registrants must inform the authorities after

321. *Id.* at 131.

322. *Id.* at 124 (noting this is so even if “[w]here it is to be drawn is a matter of argument”). Berlin also clarifies that this concept of self-actualization refers only to limitations placed by others; the inability to self-realize due to limitations of one’s own self, or of the physical world, does not count. *Id.* at 122.

323. *Id.* at 126–27.

324. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 971 (1989).

325. *Id.* (adding that the common law is “relatively indifferent to whether particular forms of respect should be denominated as ‘privacy’”). Professor Post writes, “An individual’s ability to press or to waive territorial claims, his ability to choose respect or intimacy, is deeply empowering for his sense of himself as an independent or autonomous person.” *Id.* at 973.

326. Professor Mark Poster, drawing upon Foucault’s analysis of the Panopticon as a discourse of disciplinary power, has observed that databases are “a new discourse/practice operat[ing] in the social field, a super-panopticon if you will, which reconfigures the constitution of the subject.” POSTER, *supra* note 309, at 85. Although Poster’s comments relate only to databases, and include all forms (not just public regulatory) of databases, his observations that “[c]omputerized databases are nothing but performative machines, engines for producing retrievable identities” ring particularly true in the context of preventive regulation of the dangerous. *Id.* at 89.

they change their facial features (such as growing a beard), borrow a car, or seek psychiatric treatment, they are *not required to seek permission to do so*.³²⁷

But though technological restraints may generally leave positive liberty relatively unimpaired, they wholly decimate the experience of “negative freedom.” It is this essential attribute of liberty that is roundly ignored by courts. For instance, the Seventh Circuit upheld an unlimited, lifetime ban of one particular convicted sex offender from all public parks in a city’s jurisdiction; the ban took a form no more elaborate than a letter issued on the basis of a request by a police chief to the park superintendent.³²⁸ Examining the “liberty interest” at stake, the court discarded any interest in “a generalized right to movement” or “to travel *through* parts of the City to engage in religious, political, commercial and social activities.”³²⁹ The banned individual claimed he wanted to enter the parks to “play softball, watch the Colt World Series, attend a company outing if one takes place at one of the City’s parks and take walks with friends,” an interest labeled by the court as the “right to enter the parks to loiter or for other innocent purposes.”³³⁰ The court upheld the banning letter,³³¹ finding such a right, although “not unimportant,” not “fundamental”³³² and observing that “[t]he historical and precedential support for a fundamental right to enter parks for enjoyment is, to put it mildly, oblique.”³³³

Of course, one easily imagines that this list was not exhaustive. Surely the asserted interest was not seriously measured best as a

327. *Smith v. Doe*, 538 U.S. 84, 101 (2003) (emphasis added); *see also Femedeer v. Haun*, 227 F.3d 1244, 1250 (10th Cir. 2000) (“[T]hey are nevertheless free to live where they choose, come and go as they please, and seek whatever employment they may desire.”).

328. *Doe v. City of Lafayette*, 377 F.3d 757, 760 (7th Cir. 2004) (en banc).

329. *Id.* at 769.

330. *Id.* at 769 & n.11.

331. *Id.* at 771. The court added that Doe “cites no case, state or federal, that has held that the right to enter the park to loiter or for other enjoyment purposes is ‘fundamental.’” *Id.* The court disputed that the plurality in *City of Chicago v. Morales*, 527 U.S. 41 (1999), intended “in this statement any type of fundamental rights analysis,” *City of Lafayette*, 377 F.3d at 772. The court then cited scholarly discussion of the dissenters in *Morales*, who accused the majority of claiming that “fundamental rights” liberty for substantive due process was distinguishable from “liberty interests” in procedural due process. *Id.* at 772 n.13 (citing 2 RONALD D. ROTUNDA & JOHN E. NOWAK, TREATISE ON CONSTITUTIONAL LAW: SUBSTANCE AND PROCEDURE § 15.5, at 52 (3d ed. Supp. 2004)).

332. *City of Lafayette*, 377 F.3d at 770.

333. *Id.* at 771.

desire to engage in a certain specified activity like watching a ball game. The true nature of the claim was the right to enter parks without having to justify or explain the decision to the government.³³⁴ In the words of Professor John Hart Ely, the right in question was one “to keep the government from disrupting our lives without at least moderately convincing justification.”³³⁵

Interestingly, in a decision concerning appellate review of federal sentencing, the Supreme Court lightly gestured in the direction of recognizing the nature of such an entitlement.³³⁶ In upholding a probationary sentence given in place of the Federal Sentencing Guidelines’ recommendation of a term of years, the Court found no abuse of discretion in part because a probationary sentence involves a “substantial restriction of freedom.”³³⁷ Observing that “custodial sentences are qualitatively more severe than probationary sentences of equivalent terms,” the Court nonetheless remarked that requirements to report regularly, seek permission to change addresses or jobs, and curtail certain undesirable associations in fact “substantially restrict [probationers’] liberty.”³³⁸ Although not framed in constitutional terms, the Court’s willingness to acknowledge a liberty interest framed in autonomy, rather than physical freedom, underscores Professor Ely’s intuition about such deprivations and

334. The district court even cited the fact that Doe had not entered a park for innocent purposes in ten years as support for its argument that the right was not fundamental. *Doe v. City of Lafayette*, 160 F. Supp. 2d 996, 1002 (N.D. Ind. 2001). Of course, such reasoning undermines the value of freedom from government interference by presenting liberty as a use-it-or-lose-it entitlement. Another case similarly reveals the cramped definition of liberty currently espoused by the courts. The Sixth Circuit addressed a public housing project’s practice of issuing “barring orders” that prohibit individuals from entering the property, even upon invitation of a guest. *See Thompson v. Ashe*, 250 F.3d 399, 403–04 (6th Cir. 2001). The “no-trespass” lists are formulated by the housing authority’s vice president, with “no formal set of written criteria to determine who should be placed on the list.” *Id.* at 403. There is no review of a decision to ban, and the banning notices “do not inform the individual of the reason for the ban, do not place a time limit on the ban, and do not advise the recipient how he or she may seek to be removed from the list.” *Id.* at 404. In fact, “[n]o established procedure exists to remove individuals from the no-trespass list.” *Id.* Violators are arrested and prosecuted for trespassing. *See id.* In rejecting the defendant’s procedural due process claim, the court noted that the policy affected no cognizable liberty interest. *Id.* at 407–08. After acknowledging the fundamental right to “carry on certain intimate or private relationships,” the court observed that there was no “constitutional protection to mere visitation with family members,” or general right to “freedom of movement.” *Id.* at 406–07.

335. JOHN HART ELY, *DEMOCRACY AND DISTRUST* 96 (1980).

336. *See Gall v. United States*, No. 06-7949, slip op. at 9–10 (U.S. Dec. 10, 2007).

337. *Id.* at 9.

338. *Id.*

stands in stark contrast to the Court's reasoning in cases such as those involving the sex offender registration statutes.³³⁹

Another instructive analogue might be found in the litigation and literature surrounding the recent proliferation of outpatient-civil commitment statutes.³⁴⁰ These statutes typically allow states to seek outpatient commitment, which may mean as little as requiring that an individual attend a monthly counseling session or as much as daily treatment and medication, as a prophylactic means of preventing decomposition.³⁴¹ Setting aside the wisdom of such laws, not even their staunchest advocates nor the courts that have addressed them deny that such regulations, however trivial an incursion into positive liberty, constitute a serious intrusion upon negative liberty.³⁴² Yet the inherent recognition of this intrusion relates more to ideals of autonomy and noninterference than to the simple fact that a person must physically appear at the hospital once a month or even ingest certain prescribed medications.

Likewise, the interest infringed by GPS monitoring is not the ability to decide to go into the bookstore or to drive a certain route home or to stay out until four in the morning; it is the capacity to make those choices without thinking "this will be noticed, and what will they think?"³⁴³ Online indexes or biometric collections likewise minimally affect positive liberty—requiring only that the offender check in once every three months or submit to a scan or swab—but they greatly impinge upon negative freedom by intruding upon the autonomous sphere in which the individual makes decisions about how to live, work, travel, eat, or wear one's hair.

To be clear, this impairment of negative liberty is not just suffered by the malfeasant, afraid of apprehension and surveillance. Rather, it inheres in the power of watching and is shared equally

339. See *Smith v. Doe*, 538 U.S. 84, 101 (2003); see also *id.* at 100–01 (emphasizing that registry regime does not curtail ability to engage in any activities, but merely requires regular reports about them).

340. John Monahan, *A Jurisprudence of Risk Assessment: Forecasting Harm Among Prisoners, Predators, and Patients*, 92 VA. L. REV. 391, 401–02 (2006).

341. *Id.* at 402 n.42.

342. See, e.g., *In re K.L.*, 806 N.E.2d 480, 486–87 (N.Y. 2004) (finding due process standard met by statutory scheme for outpatient commitment).

343. Cf. FOUCAULT, *supra* note 310, at 201 ("The crowd, a compact mass, a locus of multiple exchanges, individualities merging together, a collective effect, is abolished and replaced by a collection of separated individualities. From the point of view of the guardian, it is replaced by a multiplicity that can be numbered and supervised; from the point of view of the inmates, by a sequestered and observed solitude.").

among both “good” and “bad” subjects. It relates not to the fear of fair apprehension, but rather to the subjugation of the autonomous self and the fear of erroneous ascription or unexpected violence.³⁴⁴ Can even the most law-abiding individual freely decide to leave the house when aware that every movement will be recorded by GPS and compared against the day’s crime scenes,³⁴⁵ or that roughly one hundred thousand times a day a biometric profile will be checked against crime scene samples?³⁴⁶

Indeed, it is worth noting that as to the latter concern, such fears are well-founded. Online indexes also have an alarming tendency to contain outdated or inaccurate information.³⁴⁷ And the harms suffered by those required to register publicly as sex offenders have been well documented.³⁴⁸ Perhaps most dramatic and notorious is the murder of two sex offenders by a vigilante in Maine in 2006.³⁴⁹ The killer, who hailed from Canada, located and identified each offender according to an online profile that contained the offenders’ pictures, addresses, and other personal information. One of the victims was a young man

344. Cf. *Kehoe v. Fid. Fed. Bank & Trust*, 421 F.3d 1209, 1216 (11th Cir. 2005) (finding that the statute did not require proof of actual damages to privacy to recover liquidated damages); Alexandra Natapoff, *Snitching: The Institutional and Communal Consequences*, 73 U. CIN. L. REV. 645, 691 & n.205 (2004) (describing the widespread use of informants in low-income communities as engendering “a kind of personal and social ‘malaise, described by some as a form of schizophrenia, which developed in response to the permanent suspicion that one might be under surveillance’” (quoting BARBARA MILLER, *NARRATIVES OF GUILT AND COMPLIANCE IN UNIFIED GERMANY: STASI INFORMERS AND THEIR IMPACT ON SOCIETY* 133 (1999))); Post, *supra* note 324, at 960 (noting that court found the “gravamen of the plaintiff’s cause of action rested solely on the intrusive installation of the offensive device” by the landlord, rather than on the actual listening to conversations (citing *Hamberger v. Eastman*, 206 A.2d 239 (N.H. 1964))); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 487–88, 518 (2006) (describing cases that recognize a privacy interest founded in security of information).

345. California apparently has a collaborative program between sheriff’s departments and the Department of Corrections that compares tracking and crime scene data for certain parolees. Janicki, *supra* note 47, at 295–96.

346. Nakashima, *supra* note 99.

347. Adam Liptak, *Expunged Criminal Records Live to Tell Tales*, N.Y. TIMES, Oct. 17, 2006, at A1 (reporting that “real expungement is becoming significantly harder to accomplish in the electronic age,” because large commercial databases contain so many improperly retained records).

348. See *supra* Part III.C.

349. John R. Ellement & Suzanne Smalley, *Sex Crime Disclosure Questioned*, BOSTON GLOBE, Apr. 18, 2006, at A1; see also Gregory D. Kesich, *Killings Rekindle Vigilante Debate; Critics Say that Federally Mandated Sex Offender Registries Waste Resources and Invite Harassment*, PORTLAND PRESS HERALD, Apr. 19, 2006, at A1 (listing other instances of vigilantism).

whose only conviction was for having consensual sex with his girlfriend when she was fifteen.³⁵⁰

Moreover, consider the range of scandals concerning mishandling and malfeasance in DNA typing that has resulted in wrongful arrests and incarceration. In Houston, a DNA analyst falsely implicated teenager Josiah Sutton in a murder; he served four and a half years in prison until another test exonerated him.³⁵¹ At a Las Vegas lab, a technician mislabeled the samples, resulting in a wrongful accusation of double rape.³⁵² A Virginia laboratory botched two DNA tests for Earl Washington, Jr., allowing him to linger on death row until a 2004 test exculpated him.³⁵³ In Michigan, the blood of a then four-year-old who lived one hundred miles from the crime scene showed up in the forensic testing of a twenty-year-old murder case.³⁵⁴ And in Illinois, a woman charged with a crime on the basis of DNA evidence was exonerated after she supplied the perfect alibi: she was in jail in Nevada at the time.³⁵⁵

Yet in assessing the risks posed by public dissemination of current biographical data of sex offenders, the courts label negative effects as mere “conjecture.”³⁵⁶ Similarly, courts have dismissed the potential for misuse in the collection and retention of genetic samples as merely speculative, and have admonished litigants to make arguments based “not on dramatic Hollywood fantasies but on concretely particularized facts.”³⁵⁷ In short, courts roundly dismiss any

350. Kesich, *supra* note 349, at A1; *see also* Judy Harrison, *Deaths of Gunman, Sex Offenders Probed*, BANGOR DAILY NEWS, Apr. 19, 2006, at A1.

351. *See* Murphy, *supra* note 27, at 767 & n.202.

352. *Id.* at 755 n.154 (citing Glenn Puit, *Police Forensics: DNA Mix-Up Prompts Audit at Lab*, LAS VEGAS REV.-J., Apr. 19, 2002, at B1).

353. *Id.* at 756 n.155.

354. *Id.* at 755 n.151.

355. Scandals have likewise raged outside of the United States. In Australia, forensic testing in a child murder case turned up a clear suspect profile, which matched an unquestionably uninvolved rape victim whose DNA had been tested in connection with her own assault. *Id.* at 755 n.153. In the United Kingdom, it emerged that the Forensic Science Service authorized twenty research studies on DNA samples it had collected and that a private company, which was contracted to process DNA, had retained samples and demographic data. Barnett, *supra* note 280.

356. *Smith v. Doe*, 538 U.S. 84, 100 (2003).

357. *United States v. Kincade*, 379 F.3d 813, 837–38 (9th Cir. 2004) (en banc). In *Johnson v. Quander*, 440 F.3d 489 (D.C. Cir 2006), the court held that “[n]othing in the record suggests such future testing is imminent, nor can we analyze its invasiveness until it appears,” *id.* at 500. One state court curtly concluded that the “assertion that the state might misuse the information

risk of injury as hypothetical and noncognizable, even in the face of evidence of actual injuries, and therefore disregard any associated effect on liberty.

E. Summary

In sum, the use of physical incapacitation as the comparative standard for assessing the impact of noncorporeal restraints on liberty not only fails to capture, but also actively obscures, profound concerns raised by the use of new technological means of control. That is certainly not to suggest that technological restraints are inherently more troubling than physical ones; it is just to say that they should be treated neither as equivalents nor as somehow inherently less onerous. Rather, regulatory incapacitation raises specific concerns of proliferation, accumulation, unaccountability, and invisibility that ought to consciously animate inquiries into the legitimacy of such restraints.

IV. “DIFFERENT CONSTITUTIONAL PRINCIPLES”:
NEW PARADIGMS OF LIBERTY AND RESTRAINT

*Respondent . . . expresses the generalized view that . . . ‘twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision.’ But . . . if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.*³⁵⁸

Having outlined the distinct perils of proliferation, accumulation, unaccountability, and invisibility that technological restraints on liberty pose, it remains to ask how recognition of those concerns might change the kinds of questions asked by courts in reviewing the use of such restraints. Implicit in this task, however, is the assumption that courts should undertake such questioning. Some scholars question whether the judicial branch is an appropriate or effective check on executive and legislative punitiveness or zeal, and still others argue that courts are particularly ill suited to review the use of new technologies. This Part first makes the case that courts can and

derived from his DNA samples, when he makes no allegations of any specific misuse, fails to state a justiciable controversy.” *Boling v. Romer*, 101 F.3d 1336, 1341 (10th Cir. 1996).

358. *United States v. Knotts*, 460 U.S. 276, 283–84 (1983) (citations omitted) (emphasis added) (addressing the placement of an electronic device to surreptitiously track movement).

should engage in constitutional scrutiny of targeted technological restraints on liberty. Although it is beyond the scope of this Article to engage fully in this debate, this Part nonetheless endeavors to respond to some of the chief arguments against such intervention. This Part then considers how such review ought to proceed.

A. *The Case for Constitutional Regulation*

Most observers of the criminal justice system agree that legislatures, and to some extent executive branch officials, have become too punitive towards criminals and too complacent in regulating invasive policing.³⁵⁹ But a significant body of work—mainly concerning the proper scope of the Fourth Amendment—disputes whether the current state of criminal justice can be blamed on, or cured by, close judicial oversight.³⁶⁰ Professor William Stuntz has argued that the close constitutional supervision of criminal procedure initiated in the era of the Warren Court actually corrupted the system by compromising the incentives of the other branches.³⁶¹ Other scholars have responded that the current state of the criminal justice system, although undoubtedly messy, would likely have only been messier absent important and worthwhile judicial intervention.³⁶²

359. See, e.g., William J. Stuntz, *The Political Constitution of Criminal Justice*, 119 HARV. L. REV. 780, 781–82 (2006) (“[o]vercriminalization, excessive punishment, racially skewed drug enforcement, overfunding of prisons and underfunding of everything else” are “familiar political problems” on the criminal justice landscape).

360. See generally Henry J. Friendly, *The Bill of Rights As a Code of Criminal Procedure*, 53 CAL. L. REV. 929, 930 (1965) (arguing as early as 1965 that “the Court . . . ought to realize there is danger in moving too far too fast; and that the statesmanship it has generally exhibited calls for a pause until the legislative process has had a fair chance to react to its great initiatives”).

361. See Stuntz, *supra* note 359, at 785 (“Current constitutional law makes the politics of criminal justice worse: more punitive, more racist, and less protective of individual liberty.”). See generally William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505 (2001) (detailing ways in which procedural entitlements perversely affect executive and legislative decision making). Stuntz instead advocates less procedural regulation by courts and greater substantive scrutiny of legislative measures. *Id.*

362. See, e.g., Robert Weisberg, *First Causes and the Dynamics of Criminal Justice*, 119 HARV. L. REV. F. 131, 139 (2006) (observing that hoping the legislature would step in to regulate more positively in the absence of judicial regulation “requires many leaps of faith about what the public will allow judges to do and what legislators will be willing to do”); David Alan Sklansky, *Killer Seatbelts and Criminal Procedure*, 119 HARV. L. REV. F. 56, 61 (2006) (arguing that “the ways in which Americans (and their elected representatives) ‘value both privacy and process more than they once did’—have more than a little to do with the parallel changes in constitutional law, and the causation likely runs in both directions” and pointing out that when the Court “has left the political branches with a blank slate regarding the regulation of law enforcement, the slate has tended to remain blank”); see also 1 WAYNE R. LAFAVE, JEROLD H.

Professor Donald Dripps has suggested that legislative apathy—or even antipathy—toward criminal defendants is not a consequence of interbranch dynamics but rather simply a product of ordinary public choice failures in that *a priori*, most constituencies identify as law abiding not lawbreaking.³⁶³

This controversy has played out even more robustly in the specific context of judicial supervision of new technologies. Typically, the conversation centers on how broadly the Fourth Amendment should regulate claims related to investigative policing. Some scholars urge increased judicial oversight in light of the aggressive assault on privacy that such technologies represent.³⁶⁴ Others suggest that new technologies constitute particularly poor candidates for such review both as a descriptive and normative matter because courts are poorly positioned to assess emerging issues and lack the flexibility to adapt readily to unanticipated situations.³⁶⁵

Rather than rehash the well-trodden paths carved out by these debates, this Section aims to anticipate and counter the primary arguments that might particularly arise in the context of judicial regulation of targeted technological restraints. Specifically, critics might contend that the determination to impose civil regulatory restraints, and the scope of their application, should be left to the legislative branches, which are better situated in terms of accountability, flexibility, and competence. After all, technology has

ISRAEL & NANCY J. KING, *CRIMINAL PROCEDURE* § 2.8(c) (2d ed. 1999) (reviewing various theories explaining the Supreme Court’s protection of constitutional rights and noting that the notion that the Court is “protecting minorities” has “substantial force”).

363. Donald A. Dripps, *Criminal Procedure, Footnote Four, and the Theory of Public Choice; Or, Why Don’t Legislatures Give a Damn About the Rights of the Accused?*, 44 SYRACUSE L. REV. 1079, 1093 (1993) (“[T]he class of persons at risk from false positives is relatively small and restricted to a diffuse and politically disinterested segment of society. The class of people at risk from false negatives is very large, and quite sensibly frightened about crime. Their interests are supported by a professional class with a very intense interest in the outcome of legislative decisions regarding criminal justice.”).

364. See, e.g., Solove, *Digital Dossiers*, *supra* note 16, at 1126–27 (defending the warrant requirement and the role of Fourth Amendment enforcement as a “neutral and external oversight of the executive branch’s power”); see also Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 803 n.7 (2004) (collecting citations).

365. See, e.g., Kerr, *supra* note 364, at 857–82 (arguing that Fourth Amendment law fails to effectively regulate intrusive technologies and also that, from an institutional competence perspective, “[c]ourts tend to be poorly suited to generate effective rules regulating criminal investigations involving new technologies”); Stuntz, *supra* note 209, at 1265 (suggesting that the enactment of statutes designed to fill gaps left by the courts in regulating privacy demonstrates that, if left unregulated by courts, legislatures will step in and provide the necessary safeguards).

upended conventional notions of liberty and privacy for every member of society, not just those labeled “dangerous.” In a world filled with Google searches and street cameras, as well as publicly available mortgage and professional disciplinary information, the presumptive cloak of anonymity has been lifted from daily life. The four fears enumerated in Part III attend the use of red light–running cameras or E-ZPass chips—or any other generally applicable technology—just as much as they do restraints targeted at particular classes of persons.

But regardless of whether wisdom counsels special attention to the use of invasive technology against the general population, technological regulations that are targeted in nature constitute distinctly strong candidates for judicial attention. General society, however beset by technological intrusions, retains some democratic power to reclaim a measure of its liberty—whether through the wallet or the ballot box. By contrast, targeted technologies specifically isolate particular subgroups, thereby diminishing the probability of effective democratic safeguards.

At the same time, the regulatory zeal of the state reaches its zenith with regard to the exercise of its police power. Indeed, “[p]ublic hatred of crime and criminals invites the use of extreme forms of governmental power to suppress and punish criminals.”³⁶⁶ Targeted technological restraints mimic, even if they do not replicate, the violence inherent in the relationship between the state and the physically incarcerated individual.³⁶⁷ The same arguments that favor the exercise of judicial control over the penal apparatus of the state equally favor judicial oversight with regard to efforts to marshal technological restraints for the same end.³⁶⁸ Indeed, if anything, close

366. Frank Zimring & Gordon Hawkins, *Democracy and the Limits of Punishment: A Preface to Prisoners' Rights*, in *THE FUTURE OF IMPRISONMENT* 157, 157 (Michael Tonry ed., 2004); see also Dripps, *supra* note 291, at 210 (observing that the government “can circumvent the procedural safeguards of the criminal process” by “resort[ing] to a civil sanction for conduct that is widely despised in the community”).

367. Cf. Dripps, *supra* note 291, at 216 (“[I]f the government resorts to institutions that both restrain and blame, it is appropriate to subject these nominally different institutions to the criminal procedure safeguards, for those safeguards respond to the very political risks posed by the institutional innovation.”); Schulhofer, *supra* note 3, at 84 (“A much more robust limitation on ‘civil’ deprivations of liberty can be suggested. That limitation is, I argue, implicit in the foundational principles that frame the relation between government and the individual.”).

368. Significantly, this position is consistent with the argument that constitutional criminal procedure should “reorient” itself from an unhealthy and ritualistic preoccupation with privacy to instead focus on the real locus of concern: coercive and abusive government power. William

regulation of criminal restraints urges closer scrutiny over regulatory ones, since “as the criminal sanction becomes hedged with safeguards against abuse, a malign government may attempt to circumvent those safeguards by resorting to purportedly civil processes.”³⁶⁹

Some scholars have commented that the capacity of technologies to concentrate their impact constitutes an improvement over the bluntness of the police power when wielded in its physical forms. This line of argument claims that technology allows intrusive policing to focus acutely on suspicious areas or individuals, which in turn decreases the amount or degree of intrusion that the general populace must endure.³⁷⁰ A checkpoint in the park aimed at identifying sex offenders is inconvenient and unnerving, but most park visitors will not even notice that the park ranger has installed a camera that links to a database of known sex offenders and will sound an alert when one walks into the park. The same can be said for no-fly lists or DNA collection or GPS devices. After all, if technology can identify those persons in the security queue that have suspicious histories or backgrounds, then the rest of the passengers can get through the airport with far fewer insults to their dignity or time-management needs.

But because targeted restraints, by their nature, affect only a discrete and insular minority—typically, convicted or accused criminal offenders, and those unfortunate enough to share those offenders’ names or facial structures—they leave the majority of the body politic undisturbed. Thus, even if, as some argue, a collection of “potential criminal suspects” or “potential government targets” might be able to generate some measure of political clout,³⁷¹ no equally

J. Stuntz, *Privacy’s Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1069, 1076–78 (1995) [hereinafter Stuntz, *Privacy’s Problem*] (reviewing contradictory doctrines). It is also consistent with the argument that the heavy lifting for constitutional criminal procedure might better be done by the Equal Protection and Due Process Clauses, rather than by the Fourth Amendment or Bill of Rights generally. Stuntz, *supra* note 359, at 821.

369. Dripps, *supra* note 291, at 208.

370. See Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 570 (2005) (noting that computer searches may become less invasive as technology allows officials to pinpoint exactly the kinds of files they need); Paul Rosenzweig, *Civil Liberty and the Response to Terrorism*, 42 DUQ. L. REV. 663, 682 (2004) (noting that invasions of electronic privacy may reduce the need for invasions of physical privacy, for instance in the context of data mining for no-fly lists).

371. Stuntz, *supra* note 359, at 795 (arguing that in fact “criminal suspects are a powerful interest group” and attributing legislative failures to protect the rights of criminal defendants to aggressive judicial constitutional intervention). *But see* Weisberg, *supra* note 362, at 134 (“[T]here is an important, if nuanced, difference between that portion of the populus that gets

powerful constituency protects the isolated subgroup. The harm and inconvenience of the technology will truly be visited only upon those few (innocent or guilty) who find themselves repeatedly picked out of the crowd by law enforcement on the basis of a selectively applied technique. That number, inevitably, will be far smaller than the larger political constituency likely necessary to rally against such invasive uses. And the remainder of the population, even if they can imagine falling under government suspicion,³⁷² may find the very targeted nature of such methods to be proof of their general efficacy and enjoy the benefit that freedom from generally applicable measures provides.

In addition, to the extent that the targeted groups are largely comprised of once convicted criminal offenders, they likely reflect the least politically powerful group in every imaginable respect.³⁷³ Many previously convicted persons have been extirpated quite literally from the body politic through mandatory disenfranchisement statutes.³⁷⁴ The vast majority were poor when they entered the criminal justice system and are unlikely to have gained financial stature upon exiting.³⁷⁵ Even the very fact that these technologies can zero in on particular groups may increase the societal stigma they suffer, further diminishing their political salience. It is hard to imagine a constituency eager to coalesce under the banner of the Registered Sex Offenders Political Action Committee. And even if one did, it is harder still to imagine such a group carrying much political sway.

Moreover, even if targeted groups were able to surmount the handicap of their countermajoritarian posture, the unaccountability and invisibility that characterize technological restraints make the

intrusively stopped by police and the much broader, more powerful class of people whose fear of privacy invasions is related not to criminal justice but to intrusive government more generally.”).

372. Dripps, *supra* note 363, at 1088–89 (offering explanation of public choice failures in criminal justice context).

373. Weisberg, *supra* note 362, at 135–36 (observing that even white collar suspects and defendants have minimal political clout); *see also* JONATHAN SIMON, GOVERNING THROUGH CRIME: HOW THE WAR ON CRIME TRANSFORMED AMERICAN DEMOCRACY AND CREATED A CULTURE OF FEAR 70–78, 109–10 (2007) (describing the emergence of crime control as a salient topic for attaining political power due to the general lack of opposition).

374. George P. Fletcher, *Disenfranchisement As Punishment: Reflections on the Racial Uses of Infamia*, 46 UCLA L. REV. 1895, 1897–98 (1999).

375. CAROLINE WOLF HARLOW, U.S. DEP’T OF JUSTICE, DEFENSE COUNSEL IN CRIMINAL CASES 1 (2000), available at <http://www.ojp.usdoj.gov/bjs/pub/pdf/dccc.pdf> (finding that roughly 82 percent of state defendants and 66 percent of federal felony defendants are indigent).

exercise of democratic power an all the more unlikely means of cabining their use. Ordinary policing already contains a fair amount of “low visibility discretion”³⁷⁶ that is difficult to regulate—an officer patrolling the highway chooses which of many speeding cars to stop, or which of many offenders to arrest and charge.

Technological restraints pose even greater obstacles. A person detained is indisputably material; the state’s action is difficult to hide or obscure. But individuals under surveillance may not even know that their liberty has been compromised. No alert sounds when a name is entered into a computer-records search, database, or online index. The 70,000 fans at the so-called Tampa snooperbowl³⁷⁷ undoubtedly rooted for their teams without feeling any sense of personal intrusion. Even the nineteen innocent fans questioned might not have known why they were singled out, or had much by way of recourse for their troubles. Bluntly stated, it is a lot easier for the government to obscure the existence—much less the contents—of a government database than it is a physical prison. And because technological restraints emanate from so many different sources of state authority, even a vigilant individual may not know where, or how broadly, to look. If the population at large is simply unaware of a measure, it is less capable of organizing politically to regulate it.

It might be argued that this lack of awareness reflects the negligibility of the harm. Yet just because you did not know that your zipper is down does not mean that your privacy was not compromised when everyone saw your underpants. More importantly, although the throngs of fans at the ball game may not feel any ill effects, the nineteen individuals stopped on that occasion³⁷⁸—and perhaps stopped every time they attend the game or board a plane or drive on a highway—unquestionably suffer a harm. Yet the ability of technology to isolate them from the masses, and singularly visit the harm on that minority, renders them politically less powerful.

Furthermore, the concern is not just that technological control can be easily exercised surreptitiously, but also that it need not even be wielded exclusively by the state. The unaccountability of

376. ELY, *supra* note 335, at 97.

377. The term was apparently coined by Republican House Majority Leader Dick Armey in reference to the face-recognition technology used at the Super Bowl. Rachel Konrad, *Airport Security Technology Under Scrutiny*, CNET NEWS.COM, Sept. 12, 2001, <http://www.news.com/2100-1001-272938.html>.

378. *See supra* note 100.

technological restraints, which can be delegated to third parties, renders them impervious to political control. When the state incarcerates an individual, it assumes clear responsibility for the welfare of that person. Failures in health care, safety, and general well-being, however common, fall within in the state's domain. But the government, though causally connected to the misappropriation or misuse of forms of technological restraint, may nonetheless not be directly accountable for it. In other words, even assuming that the Sex Offender Political Action Committee succeeded in curtailing the scope of sex registry requirements, it would have no one to lobby to address the problem of private expressions of violence, bias, or discrimination.

Lastly, it is worth noting that to the extent that new technologies may be difficult to grasp due to their technical nature or fast-changing quality, those concerns are outweighed by the particular expertise of courts in dealing with questions of state power and due process. Although courts may not be the optimal branch for understanding the nuances of a technology's operation, they remain the preferred locus for checking governmental, particularly majority-driven, overreaching and abuse. Whereas deference to legislative and executive judgments on the use and deployment of new technologies might be warranted when such measures apply indiscriminately across the population, such deference is inappropriate when the state acts against the targeted few in the name of the safety of the many.

In sum, the very qualities that differentiate technological restraints from their physical counterparts—their capacity to proliferate, accumulate, be delegated, and impose contingent harms—counsel in favor of greater, not lesser, intervention by the judicial branch. Moreover, the targeted nature of these restraints further reinforces the need for a constitutional check on legislative or executive excess.

B. The Shape of Constitutional Regulation

Having accepted the novel challenges presented by technologies of restraint and the need for courts to exercise some oversight authority in their implementation, it remains to ask what form such supervision might take. It is not enough to categorically preclude their use on the theory that the risks outweigh the benefits. In many cases, the use of a technological restraint offers an attractive alternative (for both the state and the individual) to some more

severe regulatory regime. Conversely, however, this Article has endeavored to show that neither can it suffice to proceed on the current path, which largely treats these new technologies as simply less intrusive alternatives to physical restraint and wholly defers to legislative and executive judgments about the kind of process, if any, that should circumscribe their use.

To the extent that jails were once treated as a physical space accessible only after the government surmounted high hurdles of criminal process, the Court's rulings on regulatory incapacitation have devitalized that ideal. But that is no reason to assume that the landscape of regulatory restraints should automatically be considered free terrain. The diversity of available restraints suggests that, rather than the current dichotomous regime that focuses exclusively on the distinction between civil and criminal (or regulatory and punitive) measures, a more nuanced approach might be warranted. Different restraints effectuate different deprivations of liberty, and the continuum along which those deprivations spread in turn informs the determination of the appropriate degree of regulation.

The questions asked and answers given by application of the *Mendoza-Martinez* test prove too blunt an instrument for the subtleties of technological regulation. Requiring full criminal process for measures labeled "punitive" exacts a steep cost for what may be fairly nonrestrictive impositions. The "reasonable expectation of privacy" test can similarly be too zero-sum: either an action requires a warrant and probable cause or nothing at all.³⁷⁹ Setting such high stakes only incentivizes courts to ignore the real liberty concerns raised by technological restraints. As a result, many of these intrusive measures go effectively unregulated.

Rather than force a choice between providing full criminal process or else invalidating a sex registry requirement or DNA collection program, the law should carve some space for a more finely granulated assessment of a particular restraint's validity. Such an inquiry would ask questions aimed at ensuring the procedural

379. The Supreme Court has increasingly exhibited resistance to this dichotomous formulation, and has slowly created a variation on the kind of nuanced inquiry advanced here. Although the Court remains reluctant to eschew its "reasonable expectation of privacy" test, it has carved out a sliding scale of procedural safeguards, measured in terms of "reasonableness" for a variety of special circumstances. Silas J. Wasserstrom, *The Court's Turn Toward a General Reasonableness Interpretation of the Fourth Amendment*, 27 AM. CRIM. L. REV. 119, 129 (1989) (observing trend); see also Stuntz, *Privacy's Problem*, *supra* note 368, at 1018–19 (reviewing contradictory doctrines).

safeguards necessary to superintend its use rather than simply to classify it into a prefabricated and Manichean typology for an idea of restraint that belongs to a different time. Measures merit particularly close scrutiny when they: (a) target a particular class, (b) on the basis of the asserted dangerous character of individuals in that class, (c) in the name of the safety of the general public.³⁸⁰

This formulation intends to isolate measures least amenable to democratic accountability. By looking to provisions applicable only to particular subgroups—based on character or status rather than behavior or activity—this initial inquiry zeroes in on those measures most likely to raise legitimate constitutional concerns rather than merely reflect differing policy preferences. It also offsets the concerns raised by the unaccountability and invisibility of restraint mechanisms; if the government is to label certain persons as dangerous to the public at large or subject them to particular burdens of surveillance, then heightened scrutiny is essential to ensure that such labeling and its concomitant exposure is warranted.

Under conventional analysis, due process and equal protection are the two doctrines most readily adapted to the task of constitutionally regulating targeted technological restraints.³⁸¹ Equal protection analysis ensures that the boundaries delimiting those targeted by such restraints are narrowly and justifiably drawn; due process guarantees that those within those boundaries do in fact legitimately belong there. In addition, rather than wholesale forbid or approve the use of technological restraints, both analyses could provide a constitutional review that encourages the government to exercise its power narrowly and judiciously rather than broadly and haphazardly.

Reconceiving the nature of targeted technologies aids in understanding how such scrutiny might first be triggered. With respect to the Equal Protection Clause, numerous theories support

380. Such a purpose might be ascertained from the context surrounding the measure's implementation, from express statements by the enacting officials, or even inferred from the nature of the measure itself.

381. Although it may at first glance seem odd to discuss both doctrines almost interchangeably, the reality of their relative applications reveal that they are in fact closely related. As Professor Laurence Tribe wrote with reference to the substantive aspect of the due process clause, "due process and equal protection, far from having separate missions and entailing different inquiries, are profoundly interlocked in a legal double helix." Laurence H. Tribe, *Lawrence v. Texas: The "Fundamental Right" That Dare Not Speak Its Name*, 117 HARV. L. REV. 1893, 1898 (2004).

heightened scrutiny of such restraints. As argued in this Article, technological restraints target and affect precisely the kind of “discrete and insular minorit[y]” that lack political protection³⁸² and burden a host of fundamental rights. But even absent express appeal to the doctrine of strict scrutiny, a meaningful application of a lesser standard of review might go far to uncover irrationalities in the “physics” of such restraints as described in Part III. Recall that Justice Souter, writing separately in *Connecticut Department of Public Safety v. Doe* and joined by Justice Ginsburg, raised the possibility that the broad lines drawn by the sex offender registration statute potentially raised equal protection problems.³⁸³ And the Court has held that “mere negative attitudes, or fear, unsubstantiated by factors which are properly cognizable . . . are not permissible bases” for distinguishing one subpopulation from another.³⁸⁴

With respect to due process, dissipating the cloud of the physical paradigm reveals a range of important liberty interests that arguably even draw support from unexpected corners. For instance, the Supreme Court’s decision in *City of Chicago v. Morales*³⁸⁵ can be read as essentially acknowledging an interest in negative liberty for isolated subgroups in that the Court invalidated on vagueness grounds an ordinance that vested law enforcement with targeted authority to disperse gatherings that included alleged gang members.³⁸⁶ Recognizing what the plurality termed the “attribute of personal liberty” known as the “right to remove from one place to another according to inclination,” the Court found that the ordinance granted too much discretion to law enforcement to intrude upon the lawful activity of citizens.³⁸⁷ This liberty interest—which the dissenters derisively called a “Fundamental Freedom to Loiter”³⁸⁸—was in part described as relevant to the right to be in a chosen place; yet it more fundamentally protected a notion of freedom that is not so much

382. *United States v. Carolene Prods. Co.*, 304 U.S. 144, 153 n.4 (1938); *see also* Ben Geiger, Comment, *The Case for Treating Ex-Offenders As a Suspect Class*, 94 CAL. L. REV. 1191, 1216–30 (2006) (arguing that ex-offenders constitute a “suspect class” for Equal Protection purposes and refuting arguments against such treatment on grounds of either moral blameworthiness or constitutional approbation of disenfranchisement of ex-offenders).

383. *Conn. Dep’t. of Pub. Safety v. Doe*, 538 U.S. 1, 9 (2003) (Souter, J., concurring).

384. *City of Cleburne v. Cleburne Living Ctr., Inc.*, 473 U.S. 432, 448 (1985).

385. *City of Chicago v. Morales*, 527 U.S. 41 (1999).

386. *Id.* at 64.

387. *Id.* at 53 (quoting *Williams v. Fears*, 179 U.S. 270, 274 (1900)).

388. *Id.* at 84 (Scalia, J., dissenting).

about physical restraint, but rather about the freedom to make those choices without (unjustified) interference from the state.³⁸⁹

Support for a cognizable liberty interest might also be drawn from cases recognizing the propriety of due process review of outpatient commitment statutes. Although typically framed as a fundamental right to refuse medical care,³⁹⁰ the adequacy of the process accorded by such statutes presumably does not turn upon whether the prescribed treatment was a physical invasion of the body via psychotropic medicine or a non-physical invasion of liberty in the form of mandatory attendance at weekly groups. Indeed, in *Youngberg v. Romeo*,³⁹¹ the Supreme Court acknowledged that even involuntarily committed persons retain liberty interests in “freedom of movement” and “freedom from bodily restraint” beyond the initial commitment decision to include the manner in which they are restrained within that commitment.³⁹² In *Youngberg*, the Court determined that the unreasonable imposition of physical restraints violated the Due Process Clause.³⁹³

Once triggered, both doctrines ask questions of the kind most familiar to courts, and with which courts have great familiarity. An equal protection inquiry considers whether an action is “narrowly tailored to a compelling government interest,”³⁹⁴ or alternatively, “bears a rational relation to some legitimate end.”³⁹⁵ A due process claim can sweep quite broadly,³⁹⁶ but a procedural due process claim typically inquires into:

389. *Cf.* *Lawrence v. Texas*, 539 U.S. 558, 562 (2003) (“Liberty protects the person from unwarranted government intrusions into a dwelling or other private places. . . . Liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct.”).

390. *See In re K.L.*, 806 N.E.2d 480, 482–83 (N.Y. 2004) (framing the issue seemingly, but ambiguously, as such under state constitution). The Supreme Court, for its part, has recognized a liberty interest in “avoiding the forced administration of antipsychotic drugs.” *Sell v. United States*, 539 U.S. 166, 178 (2003).

391. *Youngberg v. Romeo*, 457 U.S. 307 (1982).

392. *Id.* at 319.

393. *Id.* at 310, 322.

394. Geiger, *supra* note 382, at 1206 & nn.89–92 (citing cases).

395. *Romer v. Evans*, 517 U.S. 620, 631 (1996).

396. *See Lassiter v. Dep’t of Soc. Servs.*, 452 U.S. 18, 24–25 (1981) (“[D]ue process is not a technical conception with a fixed content,” and thus “[a]pplying the Due Process Clause is . . . an uncertain enterprise which must discover what ‘fundamental fairness’ consists of in a particular situation by first considering any relevant precedents and then by assessing the several interests that are at stake.” (citations omitted)).

[f]irst, the private interest that will be affected by the official action; second, the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards; and finally, the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail.³⁹⁷

How then, might review of technological restraints proceed, mindful of their particular qualities? Eradication of a physical paradigm to invoke the relevant review is only half the battle; an adequate execution of that review also requires dislodging the conventions of the physical paradigm.

Importantly, both equal protection and due process involve inquiries into the tailoring—either to a class or to an individual—of a provision as measured against the government's interests. This is the essential question to ask of a technological restraint, and also the one least articulated in prevailing forms of review.³⁹⁸ Although physical incapacitation is necessarily bimodal, technological restraints can operate in finer degrees that must be measured in terms of their efficacy and intrusiveness. Thus, they warrant greater sensitivity to the manner of their application. Specifically, courts should examine the nexus between the purpose and the population restrained; the duration, repetition, or longevity of the restraint's application; the demonstrated efficacy of the particular restraint; the existence of less intrusive alternatives; and the degree to which the technique is amenable to external constraints impeding its abuse. Each individual factor can first be judged along a spectrum and then considered in constellation to determine the measure's constitutionality.

Thus, for instance, a measure that has a loose nexus between its purpose and population, operates indefinitely and repetitively, has not been proven efficacious, compounds other forms of restraint, could be achieved through less restrictive means, and is difficult to check or safeguard against abuse would be presumptively

397. *Mathews v. Eldridge*, 424 U.S. 319, 335 (1976).

398. *But cf. Kansas v. Hendricks*, 521 U.S. 346, 388 (1997) (Breyer, J., dissenting) (observing that the state's "failure to consider, or to use, 'alternative and less harsh methods' to achieve a nonpunitive objective can help show that the legislature's 'purpose . . . was to punish'"). Professor Christopher Slobogin has proposed a series of principles to govern preventive incapacitation determinations, derived from a variety of cases espousing similar values. Christopher Slobogin, *A Jurisprudence of Dangerousness*, 98 NW. U. L. REV. 1, 48–58 (2003).

impermissible. To the contrary, a measure applied to a narrow and select population, that operates for a short period of time and on an infrequent basis, is proven highly effective, is the only means of achieving its goal, and is readily amenable to public scrutiny or check would be presumptively acceptable. Many measures will fall somewhere in between, but this inquiry proffers a set of optimal values that such techniques ought to aspire to embody, and which are designed to counter the concerns outlined in Part III.

First, assessing the nexus between a restraint's purpose and its targeted population helps counter both the proliferation and accumulation tendencies of technological restraints and also minimizes the risks of unaccountability and invisibility. For instance, consider GPS tracking requirements. If the purpose of such requirements is to protect the public from reoffending sex offenders, then they should be tailored to those offenders for whom real-time location information operates as an effective form of apprehension or deterrence. A regulation drawn so generally that it sweeps in a sex offender whose behavior demonstrates a propensity toward molesting family members or engaging in consensual but underage sexual activity therefore is overly broad: it includes individuals for whom location information serves no useful purpose.

This defect would not render it immediately unconstitutional: if such tracking was imposed for only a short period, was demonstrably effective, and constituted the only means of achieving the safety goal, for instance, it might nonetheless withstand challenge. But otherwise, invalidating such a provision would ensure that the ease of imposing such requirements do not cause them to proliferate, especially in light of real concerns about third-party violence or impediments to personal liberty. Poorly drawn requirements also suggest that goals other than those proffered by the government are animating the determination to impose the restraint.³⁹⁹ For instance, a sex offender registry that provides general information about the location or appearance of a particular offender is more readily defensible than one that gives unnecessarily specific details likely to serve no purpose other than to arouse private violence.

399. *Cf. Romer*, 517 U.S. at 632 (observing that statutes that impose “a broad and undifferentiated disability on a single named group” are unconstitutional, in part because the “sheer breadth is so discontinuous with the reasons offered for it that . . . [it] seems inexplicable by anything but animus toward the class it affects”).

Second, restraints that operate for long periods of time or impose repetitive burdens or encumbrances on the regulated population deserve greater scrutiny than those imposed on a onetime basis or for shorter periods of time. Consider, for example, a sex offender registration requirement. A requirement that an individual register once should be treated differently than a requirement to update registration on a quarterly basis. And a requirement that individuals register for five years deserves different analysis than one that they register for life. Similarly, a DNA sample kept in a national database during a window of time in which an individual is most likely to reoffend deserves different consideration than one that remains after a long period of time has passed or even the person's death. Such review helps counter the accumulation concern because techniques that operate in a shorter window are less likely to bump up against other methods of control. Shorter operational periods and fewer repetitive intrusions likewise diminish the proliferation and unaccountability concerns. Because only those applications that score high on the other factors will survive scrutiny, the state will have an incentive to be particular about whom it subjects to the longest and most invasive forms of surveillance.

Third, review should look for evidence that a regulatory restraint actually achieves its stated purpose. Technological restraints impinge important interests in the name (usually) of public safety. Accordingly, a highly efficacious measure might garner strong support for its continued application, perhaps even if applied against a large subpopulation for an extended period of time. Conversely, an inefficacious or error-prone measure should raise a red flag even if targeted fairly narrowly. In simple terms, courts should ask how effectively the restraint as imposed is at accomplishing what it is purports to accomplish. Acknowledging the harms wrought by technological restraints necessarily carries with it the responsibility to concentrate the visitation of that harm only where needed. Whereas a largely inefficacious restraint might nonetheless be justified as briefly imposed on a very narrow class of persons, the same restraint should not be permitted to apply more broadly.

Moreover, rather than rely upon speculative assessments that a particular technology achieves a particular goal, courts should demand evidence of its capacity to achieve its stated purpose. Thus far, courts have proven far too reluctant to question the effectiveness of a technological restraint. In assessing the benefit to "public safety" advanced by sex offender registries, for instance, the Supreme Court

observed no more than that there existed a “high rate of recidivism among convicted sex offenders.”⁴⁰⁰ The Court then concluded that requiring sex offenders to register was therefore “reasonable.”⁴⁰¹ There was no discussion, much less evidence, about whether registration in any way reduced recidivism or worked to prevent future victimization. The Court did not examine key aspects of the registry—in terms of its reporting requirements and notification provisions—to determine whether they each supported that ultimate purpose. Such an inquiry would likely have proved fruitful: many registries are in fact drawn in such broad terms and contain such large quantities of poorly distinguished data that they are virtually useless to the general population.⁴⁰² If a concerned individual runs a search of offenders in the neighborhood that turns up fifty people in a five-mile radius, entirely unsorted by whether they actually pose any danger, then the provision simply fails to safeguard the public adequately while imposing a serious restriction on liberty.

Likewise, courts across the board have deemed collection and retention of DNA samples as serving “society’s enormous interest in reducing recidivism”⁴⁰³ or “solving crimes.”⁴⁰⁴ Yet courts fail to substantiate either of those claimed interests with actual data demonstrating the efficacy of widespread DNA collection, either in terms of cases closed, convictions secured, or crimes deterred.⁴⁰⁵ Even if a court were to accept that DNA typing has proven effective at linking convicted offenders to old, current, or future cases, then that conclusion still only supports the continued collection of genetic profiles from the convicted offender population. No evidence

400. *Smith v. Doe*, 538 U.S. 84, 103 (2003).

401. *See id.*

402. For instance, a search of the California sex offender registry for a two-mile radius around the University of California at Berkeley School of Law turned up over 30 offenders. *See* Office of the Attorney Gen., California Megan’s Law, <http://www.meganslaw.ca.gov/> (last visited Apr. 6, 2008). Clicking the “address” box and then entering the search terms “2240 Piedmont Ave.” in Berkeley, CA 94720 returns a map with dots indicating registered offenders. Clicking for individual information gives a photograph, name, address, and other identifying information—but gives only the code provision of conviction (making it difficult to determine the factual underpinnings of the offense) and no sense of how long ago the conviction occurred.

403. *United States v. Kincade*, 379 F.3d 813, 838 (9th Cir. 2004) (en banc).

404. *Nicholas v. Goord*, 430 F.3d 652, 668 (2d Cir. 2005).

405. In fact, most data on the efficacy of DNA testing appears to demonstrate its ability to exculpate offenders in specific cases. *See* Frederick R. Bieber, *Turning Base Hits into Earned Runs: Improving the Effectiveness of Forensic DNA Data Bank Programs*, 34 J.L. MED. & ETHICS 222, 222 (2006) (noting that statistics on DNA’s effectiveness are urgently needed).

supports the need for the continued retention of genetic *samples* by the government or for broader collection provisions.⁴⁰⁶ Indeed, when a hit occurs in a database and the individual is apprehended, a new set of DNA samples is typically taken for confirmatory purposes.⁴⁰⁷ Given the infringement on liberty—both in the positive and negative senses—represented by the government storage of an individual’s entire genetic code, and the lack of a justification for keeping it, that requirement of the restraint should be parsed out from the general regime and invalidated as suspect.

Factoring in evidence of efficacy helps counter the proliferation, invisibility, unaccountability, and accumulation tendencies of restraint technologies. Without any measure of efficacy and absent a constituency capable of holding legislatures accountable, such restraints can easily propagate unchecked. The invisibility of the harms—in that they are visited only upon the population that must endure the burdens of the restraint—makes ordinary accountability difficult.

Fourth, as a corollary of the requirement that courts factor the efficacy of restraint techniques into an assessment of their constitutionality, courts should also ask whether the restraint in question is the least restrictive means of achieving a stated goal. Such an inquiry directly checks the proliferation and accumulation tendencies of new technological restraints: the government can only justify a broadly applicable set of restraints applied cumulatively upon the same individual if it can show that all are essential components of its overarching goal. Thus, if applying the restraint to a smaller set of individuals, or for a lesser amount of time or in a different manner than that contemplated would achieve the same ends, that lesser restriction should govern. Similarly, a court might determine that a measure that does not provide procedures for review or lifting of the restraint is more restrictive than necessary.

The last factor inquires into the capacity of particular individuals to challenge a requirement that they submit *ab initio* to a particular

406. Rather, speculation regarding the success of collection and retention apparently sufficed. Of course, this is even so as documented evidence of malfeasance and misuse of DNA samples is dismissed as “conjecture.” *Nicholas*, 430 F.3d at 669.

407. See, e.g., Am. Prosecutors Research Inst., DNA Evidence Policy Considerations for the Prosecutor, http://www.dna.gov/audiences/officers_court/policy_prosecutor/ (last visited Apr. 6, 2008) (advising prosecutors in a cold-hit case to “review[] the viability of the case before law enforcement obtains a confirmation DNA sample from the subject”).

restraint—including whether there exists any opportunity to remove oneself from the class. As noted, technological restraints typically elude the economics of the physical world and often operate largely invisibly. They likewise are delegable and prone to proliferation and accumulation. To the extent that external forces can cabin their potential abuse, the courts need not act as vigorously in supervising their deployment. The degree to which a technological restraint contains either endogenous or exogenous constraints on its use should sensibly influence a court's receptiveness to its terms. Regulations that include individualized process, or even the opportunity to opt out of a generally drawn class through a particular showing, should be far more likely to withstand challenge than one that draws broad categorical lines based solely upon status.⁴⁰⁸

For instance, if the government compiles a database—whether of DNA, names for a no-fly list, or biometric images of “suspicious” persons—and then permits parties to access or challenge that database for errors or oversights, then its use in a closed system of regulatory restraint may be justified as appropriately safeguarded. But the same database, if impermeable to challenge or inspection in any reasonable way, should cause a court pause. Similarly, a sex offender registry that requires mandatory lifetime listing—with no provisions to demonstrate either that an individual is incapable of causing the harm contemplated (for instance, a comatose individual) or unlikely to cause such harm (for instance, has not offended for many years)—should be greeted with suspicion. Broadly drawn, indefinite regulatory restraints are the equivalent of technological “life sentences,” and like their physical counterparts, they should be reserved only for cases of utmost and demonstrable need.

CONCLUSION

In 1987, only six Supreme Court Justices could agree that the Constitution countenanced the preventive jailing of persons charged by probable cause with a narrow category of dangerous crimes and found by a judge after an adversarial hearing to pose a clear and convincing danger to the community.⁴⁰⁹ Twenty years later, eight

408. This is also consistent with the historically disfavored category of status offenses. *See* *Robinson v. California*, 370 U.S. 660, 666–67 (1962) (finding it a violation of due process and cruel and unusual punishment to punish an individual for being addicted to narcotics).

409. *United States v. Salerno*, 481 U.S. 739, 754–55 (1987) (noting flight risk also justifies detention).

Justices agreed that a statute that requires people to report for the rest of their lives each time that they change hair color does not even invoke any constitutional scrutiny.⁴¹⁰ Courts around the country demonstrate the same indifference toward requirements that individuals give biological samples for government retention or attach lifetime tracking devices to human beings.

Justice Brandeis presciently urged long ago that the Constitution retain the “capacity of adaptation to a changing world.”⁴¹¹ Just as new communication technologies prompted Fourth Amendment doctrine to shift its focus to “people, not places,”⁴¹² so too do new incapacitation technologies require renewed reckoning with societal understandings of what it means to deprive liberty. There may one day come a time when incapacitation no longer requires physical restraint: instead of using bricks and mortar to keep the dangerous in check, the government may rely upon microchips and face scans, the Internet and DNA. If that day comes to pass, then it will be up to every individual to ensure that American ideals of liberty have kept pace with technological innovations and to relinquish at last the image of the jail as the paradigmatic form of restraint.

410. See *Conn. Dep’t of Pub. Safety v. Doe*, 538 U.S. 1, 1 (2003).

411. *Olmstead v. United States*, 277 U.S. 438, 472 (1928) (Brandeis, J., dissenting).

412. *Katz v. United States*, 389 U.S. 347, 351 (1967).