

PARADIGMS OF RESTRAINT

Erin Murphy
Assistant Professor of Law
University of California, Berkeley
Boalt Hall

Friday Faculty Colloquium
Friday, October 27, 2006
12:15 PM – 1:30 PM
Law Building, Room 2448

For UCLA School of Law workshop. Please do not cite or quote without permission.

Paradigms of Restraint

Erin Murphy¹

Twenty years ago, the Supreme Court decided *United States v. Salerno*² and upheld the federal Bail Reform Act along with the pretrial detention of a seventy-four year old gangster jailed on charges stemming from his tenure at the head of the Genovese Family.³ The *Salerno* decision marked a watershed moment in criminal justice.⁴ If pre-trial detention constituted “punishment,” then the Bail Reform Act was unconstitutional because it applied without the elaborate processes and high burden of proof of a criminal trial. Finding such detention “regulatory, not penal” in character, however, enabled the Court to endorse the defendant’s physical incapacitation in advance of trial.⁵

Although the Court described its holding in *Salerno* as the “carefully limited exception”⁶ to the norm of liberty, its endorsement of “regulatory” pre-trial incapacitation set the stage for prophylactic incapacitation in other contexts.⁷ In the years since the decision, pretrial detention of defendants has become quite common.⁸ Civil commitment of the mentally ill was already in good legal standing at the time of *Salerno*,⁹ and the Court’s reasoning has since justified the detention of violent sexual predators,¹⁰ certain illegal immigrants,¹¹ and most recently, terrorist suspects.¹² In the words of Carol Steiker, *Salerno* has helped to create a “preventive state” -- one that “incarcerate[s] all of those whom we know (or think we know) to pose a danger of serious harm to others.”¹³

¹ Assistant Professor, University of California, Berkeley (Boalt Hall). I owe a debt of gratitude to Carol Steiker, who invited me to participate in the *Criminal Procedure Stories* conference at Harvard at which a preliminary version of this work was given, and to Dan Richman, whose excellent piece on *Salerno* that inspired me to think about these issues. Thanks are also due to the junior faculty working group at Berkeley, and to my wonderful colleagues David Sklansky and Jonathan Simon. The participants in the junior criminal professor workshop hosted by GWU Law School also provided extremely helpful comments. Finally, Boalt students Ben Wolff, Debbie Won, and Steven Sassaman provided invaluable research assistance.

² 481 U.S. 739 (1987).

³ Daniel Richman, *United States v. Salerno: The Constitutionality of Regulatory Detention*, in *CRIMINAL PROCEDURE STORIES* 420 (ed. Carol Steiker, 2005).

⁴ Apart for its implications for regulatory detention, *Salerno* has resonated generally in constitutional law for another principle, namely the proper scope of facial versus as applied challenges outside of the First Amendment. *See, e.g., United States v. Booker*, 543 U.S. 220, 275 n.1 (2005) (Stevens, J., dissenting in part) (citing *Salerno* and *Chicago v. Morales*, 527 U.S. 41, 54-55 n.22 as examples of the debate).

⁵ *Salerno*, 481 U.S. at 746.

⁶ *Id.* at 755.

⁷ *See id.* at 747.

⁸ Richman, *supra* note XX, at 439-40 & nn. 122-124.

⁹ *Addington v. Texas*, 441 U.S. 418, 428 (1979) (upholding civil commitment statute but noting that reasonable doubt standard not constitutionally required).

¹⁰ *See, e.g., Kansas v. Hendricks*, 521 U.S. 346 (1997).

¹¹ The Court initially rejected the constitutionality of detaining all deportable aliens in *Zadvydas v. Davis*, 533 U.S. 678 (2001), but then upheld detention of a limited class of aliens, without requiring individualized determinations of dangerousness, in *Demore v. Kim*, 538 U.S. 510 (2003).

¹² *See, e.g., Hamdi v. Rumsfeld*, 542 U.S. 507 (2004) (allowing detention of citizen captured on foreign soil based on less than *Salerno* would require).

¹³ Carol Steiker, *Punishment and Procedure: Punishment Theory and the Criminal-Civil Procedural Divide*, 85 *Geo. L.J.* 775, 819 (1997).

Salerno's legacy with regard to the preventive *incarceration* of the allegedly dangerous is well-established.¹⁴ But the regulatory/punitive distinction applied in *Salerno* also cleared the way for an array of non-detention based forms of regulation. As Justice Marshall in his dissent in *Salerno* observed, the majority's reasoning justified a broad range of restrictive measures imposed in the name of safety or prevention.¹⁵ He laid out a doomsday scenario in which a statute imposed a "dawn-to-dusk curfew on anyone who is unemployed," and noted that the Court's logic permitted such an ordinance as "preventing danger to the community . . . a legitimate regulatory goal."¹⁶

These projections proved prophetic. Only a few years later, one California court cited *Salerno* as support for affirming the constitutionality of a community-wide emergency curfew.¹⁷ And today, the regulatory/punitive rubric has applied to a range of measures intended "regulate" the dangerous, ranging from forfeiture statutes¹⁸ to restrictions on where an individual can live or work,¹⁹ and even whether they can see their children.²⁰

Regardless of the wisdom of such enactments, however, there is one general area in which the wide latitude accorded to preventive measures should raise cause for concern. In the twenty years since the *Salerno* decision, society has undergone a critical shift. Specifically, the preventive state has now become a technological one. Physical incapacitation is no longer the only means of closely and intensively monitoring large numbers of individuals. In the modern world, regulation of the dangerous has become as much about keeping a person out of a place as it used to be about locking him up in one.

When *Salerno* set forth its framework approving the use of prophylactic, "regulatory" measures, this technological brave new world was still the stuff of science fiction fantasies. But the advent of new forms of surveillance has dramatically augmented the ability of the state to "regulate" the individual. Without relying upon jail cells: law enforcement can today still be all seeing, all knowing, and all controlling. In a relatively short span of time, the Panopticon imagined by Jeremy Bentham has become a virtual reality. Technology now allows us to track real-time movement of large numbers of individuals;²¹ to prove conclusively exactly which person wore a hat or took a sip from a discarded soda can;²² to find with the click of a mouse a neighbor's personal and intimate details; and, soon enough, to pick one face out of a 10,000

¹⁴ Richman, *supra* note XX, at 437-449. Some have argued directly that perhaps "individual prevention should become the predominant goal of the criminal justice system." Christopher Slobogin, *The Civilization of the Criminal Law*, 58 VAND. L. REV. 121 (2005).

¹⁵ *United States v. Salerno*, 481 U.S. 739, 760 (Marshall, J., dissenting).

¹⁶ *Id.*

¹⁷ See, e.g., *In re Juan C.*, 28 Cal. App. 4th 1093, 1101 (Cal. Ct. App. 1994) (*quoting Salerno*, 481 U.S. at 748).

¹⁸ *US v. Peter Monsanto* ("it would be odd to conclude that the Government may not restrain property ... based on a finding of probable cause, when we have held that ... the Government may restrain *persons* where there is a finding of probable cause....")

¹⁹ See, e.g., *Doe v. Miller*, 405 F.3d 700 (8th Cir. 2005) (upholding residency restriction); *Doe v. City of Lafayette*, 377 F.3d 757 (7th Cir. 2004) (en banc) (upholding a lifetime ban from all city parks imposed, via a letter from the City Superintendent of Parks, against an individual with a history of arrest and conviction for sex-related offenses); Richard R. Whidden, Jr. & Tiffany A. Richards, *Local Government Regulation of Sex Offenders: Addressing a Threat*, MUNICIPAL LAWYER Mar./April 2006 n.xxix (listing statutes restricting sex offenders);

²⁰ See, e.g., *Doe v. Donahue*, 829 N.E.2d 99 (Ind. 2005) (upholding prison regulation that prohibited male and female sex offenders from visiting with minor children, including their own).

²¹ See, e.g., *United States v. Moran*, 349 F.Supp.2d 425 (N.D.N.Y. 2005) (upholding warrantless use of GPS tracking device).

²² See, e.g., *State v. Piro*, 112 P.3d 831 (Id. App. 2005) (upholding of testing of water bottle retained by officers for DNA testing after defendant offered drink while in custody).

person crowd.²³ A person can be electronically zoned into or out of a particular physical space, excluded from a particular line of employment or entertainment, or globally shamed and stigmatized.

In short, new technologies ensure that the effective execution and enforcement of regulatory controls over “dangerous” persons need no longer focus exclusively upon physical incarceration. In such a world, what special concerns attend the use of such restraints? How should we appraise the harms caused by such regulations? This Article begins by sketching four new kinds of technological means for regulating the “dangerous,” and outlines the general contours of each category. The second Part explores the legal landscape against which these technologies operate, and explains that each applies not just outside of conventional criminal process, but also outside of constitutional or procedural constraints of any kind. The third Part endeavors to explain the failure of courts to recognize that technological regulations significantly affect liberty interests, and then identifies the ways in which such regulations do undermine core constitutional values. Finally, the last Part underscores the degree to which the contemporary conception of physical incapacitation as the “paradigm of restraint” threatens to overlook the emerging new paradigms of restraint, which take technological forms. Accordingly, this Article closes by urging a richer understanding of interests that technological regulations place in jeopardy and the development of new legal constructs to regulate their use.

I. TECHNOLOGY AND THE NEW REGULATION OF THE DANGEROUS.

*Any sufficiently advanced technology
is indistinguishable from magic.*²⁴

Control of dangerous persons is a preoccupying interest of contemporary American society. Scholars have written extensively about the ongoing rise in incarceration rates and the expansion of substantive criminal law.²⁵ As a generic fear of crime has come to dominate the social consciousness, a targeted interest in controlling criminals has grown.²⁶ At the same time, a range of technologies have emerged that enable the state to undertake new forms of surveillance and control. Many of these technologies initially aim to supplement or enhance traditional forms of control,²⁷ but then quickly expand to innovative uses outside of conventional criminal process.

History shows that the use of technology as a regulatory measure rarely stops where it starts. Increasingly, these new forms of restraint are used outside of and distinct from the criminal justice system, as a means of preventing or controlling those alleged to be dangerous. This shift from enforcement uses of technology to prevention uses of technology comports

²³ See, e.g., *People v. Johnson*, 139 Cal. App.4th 1135 (Ct. App. Ca. 2006) (discussing future possible uses of facial recognition software); *Eyeticet Corp. v. Unisys Corp.*, 155 F.Supp.2d 527 (E.D. Va. 2001) (describing iris scanning technology); David Lamb, *One Last City Is Scanning for Faces in the Crowd*, L.A. Times (Sept. 29, 2003) (reporting that Virginia Beach continues to use facial-recognition systems to scan for terrorists, felons with outstanding warrants, and missing children).

²⁴ ARTHUR C. CLARK, *PROFILES OF THE FUTURE: AN INQUIRY INTO THE LIMITS OF THE POSSIBLE* (1972).

²⁵ See, e.g., William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505, 512-19 (2001) (giving examples of breadth of criminal law); MICHAEL JACOBSON, *DOWNIZING PRISONS: HOW TO REDUCE CRIME AND END MASS INCARCERATION* (New York University Press 2005).

²⁶ See generally Jonathan Simon, Carol Steiker, et al.

²⁷ Thus, for instance, DNA typing might be used in a criminal case to conclusively link a suspect to an offense; or GPS monitoring might be imposed upon a parolee or a probationer.

generally with 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.”²⁸

The use of new technology to regulate wholesale those alleged to be dangerous, outside of the realm of conventional criminal process, is this Article’s central concern.

A. DNA databasing.

All fifty states, as well as the federal government, require certain categories of convicted offenders to submit DNA samples.²⁹ The DNA is tested and typed, and then uploaded to state and national databases.³⁰ The databases retain the typed genetic information indefinitely and without regard to any period of incarceration or supervision; currently no state provides for deletion of an otherwise lawfully retained sample.³¹ Almost all states also provide for indefinite retention of the physical genetic sample, which of course contains the individual’s entire genetic code.

Initially, most of these mandatory collection statutes applied to those convicted of sexual offenses or violent felonies. Then they began to expand to include all those convicted of felonies. Next came statutes that required collection of DNA from all convicted persons, whether felons or misdemeanants. Presently, most states require all felons to contribute DNA samples, and some include even misdemeanor offenders. Then states moved to require samples from those merely arrested for a crime. Presently, the federal government and seven states -- California, Kansas, Louisiana, Minnesota, New Mexico, Texas, Virginia-- include arrestees,³² and other states have considered following suit.³³ At the same time, calls for a universal DNA database have sounded.³⁴ Each of these mandatory collection statutes and regulations applies categorically and indefinitely. None requires any findings of particularized need for collection. Moreover, most impose no limit on the retention of either the sample or profile.

In addition, less formal methods of obtaining DNA have also proliferated. Police officers in numerous jurisdictions have relied upon DNA dragnets -- demands from tens to thousands of “suspect” individuals for “voluntary” samples -- as an investigative tool.³⁵ Officers knock on

²⁸ Malcolm M. Feeley & Jonathan Simon, *The New Penology: Notes on the Emerging Strategy of Corrections and Its Implications*, *Criminology* Vol. 30, No. 4 (1992) at 452.

²⁹ See Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, *CAL. L. REV.* (forthcoming).

³⁰ *Id.*

³¹ Some states require deletion of a sample and/or profile if a conviction is expunged or overturned.

³² See 42 U.S.C. § 14132; Cal. Penal Code § 296 et seq.; Kan. Stat. Ann. Sup. § 21-2551(e); La. Rev. Stat. Ann. § 15:609(A)(1); Minn. Stat. Ann. §299C.105; N.M. Stat. § 29-3-10(A); Tex. Gov’t Code Ann. § 411.1471; Va. Code Ann. § 19.2-310.2:1.

³³ See, e.g., Illinois (HB 4607 & 779); Michigan (SB 575); North Carolina (SB 746, SB 2015); New Jersey (HB 4708; SB 378); New York (HB 9169); Penn (HB 2765); Tenn 2649.

³⁴ See D.H. Kaye & Michael E. Smith, *DNA Identification Databases: Legality, Legitimacy, and the Case for Population Wide Coverage*, 2003 *WISC. L. REV.* 413, 415.

³⁵ See paper on file with author. See also 60 Minutes, *DNA Dragnets* (CBS television broadcast Sept. 12, 2004), transcript available at <http://www.cbsnews.com/stories/2004/09/10/60minutes/main642684.shtml>; Pam Belluck, *To Try to Net Killer, Police Ask A Small Town's Men for DNA*, *N.Y. Times*, Jan. 10, 2005, at 1 (describing police efforts to catch a killer by requesting and testing the DNA of all male residents of Touro, MA, who numbered approximately 790).

doors, flash a badge, and ask for a cheek swab; often, the message is that to refuse is to become the primary suspect in the case.³⁶ Litigation regarding the scope of permissible use of such contributions has tended to find that voluntary relinquishment grants law enforcement broad and indefinite control over the biological information.³⁷

As collection standards have broadened, the database inclusion requirements have responded in kind. At present, the federal database contains the genetic profiles of 3.3 million convicted offenders, and it is reportedly growing by roughly 80,000 individuals per month.³⁸ The federal government recently enacted legislation to authorize inclusion in the national database of any sample collected according to state law, replacing the previous statutory limit that restricted the database to convicted offenders.³⁹ These growing databases are in turn a powerful investigative tool, allowing officers to make associations between individuals and evidence in cases with no known suspects. As a result, courts have had to confront cases in which a DNA match constituted the only evidence; thus far, most courts have upheld those convictions as constitutional.⁴⁰ Most recently, DNA database searches have been used as tools for finding suspects via the profiles of relatives contained in the database.⁴¹

As a legal matter, most courts have thus far endorsed a wide range of practices and uses of DNA evidence. Nearly every state court has endorsed DNA collection from convicted offenders.⁴² 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,⁴³ every federal court to consider the issue has upheld contribution requirements.

Because the arrestee statutes are of recent vintage, courts have yet to fully air these challenges. But by many accounts, the reasoning used to uphold convicted felon statutes applies equally to arrestees. In the words of Judge Kozinski, dissenting in the Ninth Circuit case upholding the federal collection statute,

if we accept the legal presumption -- not questioned here by anyone -- that once [the defendant] leaves supervised release he will be just like everyone else, authorizing the extraction of his DNA now to help solve crimes later is a huge end run around the Fourth Amendment. Or, to state it in the reverse, if the reason for taking [the defendant's] DNA while he's on supervised release is that it will help solve crimes

³⁶ See, e.g., Glynn Wilson, *In Louisiana, debate over a DNA dragnet*, CHRISTIAN SCIENCE MONITOR, Feb. 21, 2003, available at <http://www.csmonitor.com/2003/0221/p03s01-usju.html> (noting that “those who hesitate” to provide a voluntary DNA sample in a dragnet “draw swift notice,” according to the police chief deputy, who reported that he would then seek an order to have them swabbed); see also *Kohler v. Englade* (5th Circuit) (raising complaint that refusal to submit sample caused individual to be publicly labeled a suspect in serial rapes).

³⁷ Pam Belluck, *To Try to Net a Killer, Police Ask Small Town Men for DNA*, N.Y. TIMES, Jan. 10, 2005 (reporting on several dragnets across country, and legal claims to have collected DNA purged from records and repositories).

³⁸ Rick Weiss, *Vast DNA Bank Pits Policing v. Privacy*, WASH. POST (June 3, 2006).

³⁹ DNA Fingerprint Act of 2005, P.L. 109-162 /VAWA

⁴⁰ See, e.g., *Roberson v. Texas*, 16 S.W.3d 156 (Ct. App. Tx. 2000) (upholding conviction based on DNA evidence alone); *People v. Rush*, 242 A.D.2d 108 (App. Div. N.Y. 2000).

⁴¹ Henry T. Greely, Daniel P. Riordan, Nanibaa' A. Garrison, Joanna L. Mountain, Symposium, *Family Ties: The Use of DNA Offender Databases to Catch Offender's Kin*, 34 J. L. Med. & Ethics 248 (Summer 2006). Bieber's paper in Science. See also case in England cited in your other paper.

⁴² See Ron Sherer, *Should DNA be Collected From All Criminals?*, CHRISTIAN SCIENCE MONITOR, May 19, 2006, 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, 3044-06-04, 0574-02-04 et al., (Vt. Dist. Ct. Apr. 24, 2006) (holding that state statute that allows DNA collection from nonviolent convicted felons violates state constitution).

⁴³ See *Nicholas v. Goord*, 430 F.3d 652, 658-59 (2d Cir. 2005) (summarizing cases).

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.⁴⁴

Although practices surrounding DNA dragnets, familial searching, and other creative uses of DNA evidence have yet to undergo serious legal scrutiny, it seems very possible that courts will endorse such applications.

B. Online indexing.

Another increasingly popular tool used to monitor the "dangerous" is the online publication of criminal histories. The most common and popular type of online index are sex offender registries, which swept the nation in the wake of federal legislation that reduced grant funding to states without mandatory registration statutes.⁴⁵ Now, every state has such an act. Although the statutes vary in specific terms, all require online publication of certain sex offenders' biographical information and charge of conviction. Most statutes post publicly at least a name, offense of conviction, and current photograph. Others include a home and work address, date of birth, physical characteristics, or other identifying information. Just recently, in July of 2006, Congress passed and President Bush signed into law a bill authorizing the creation of a national federal database of convicted sex offenders.⁴⁶ There are also websites that allow a person to put in their address and call up a map of nearby listed offenders.⁴⁷

Like DNA collection statutes, these statutes tend to be triggered by broad categorical classifications based on prior conviction. Most statutes impose on the offender the obligation to submit regular updates -- typically every 90 days -- to the government, and to actively notify the registry if the offender relocates, uses an automobile not registered to him, or changes his appearance in any way. Like DNA statutes, the data collection and dissemination provisions apply without regard to any term of supervision or formal entanglement with criminal process, and some operate for the entire lifetime of the individual.

Over time, these statutes have largely withstood legal challenges of various kinds in state and federal courts. In 2003, the Supreme Court examined both the onerous Alaska Sex Offender Registration Act⁴⁸ and the Connecticut registration act⁴⁹ 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.

Momentum has already gathered to expand the use of online registration beyond this initial scope. An Ohio legislative panel recently moved to enact a law that requires registration

⁴⁴ *United States v. Kincade*, 379 F.3d 813 (9th Cir. 2004) (en banc) (Kozinski, J., dissenting).

⁴⁵ Crimes Against Children and Sexually Violent Offender Registration Act, 42 U.S.C. § 14071 (2000) (reducing federal grants to states that fail to enact registration statutes).

⁴⁶ Adam Walsh Child Protection & Safety Act of 2006, H.R. 4472, 109th Cong. (2d Sess. 2006) (creating national database and also granting money for GPS tracking programs).

⁴⁷ <http://www.mapsexoffenders.com/index.asp> (last visited Sept. 27, 2006). After putting in one's own address, small flags designate the location of nearby offenders. Clicking on the flags pulls up a photo, name, and address, as well as a hyperlink to the sex offender registry site for the state.

⁴⁸ *Smith v. Doe*, 538 U.S. 84 (2003).

⁴⁹ *Connecticut Dep't of Safety v. Doe*, 538 U.S. 1 (2003).

of alleged sex offenders, even if the individual has never been convicted of an offense.⁵⁰ There is also increased interest in creating registries of those convicted of making or selling methamphetamine,⁵¹ or those convicted of operating illegal drug laboratories.⁵²

Lastly, some jurisdictions -- no doubt in response to the proliferation of online private companies that offer online instant background checks for an affordable price⁵³ -- have begun placing all criminal records online. Postings include not just judgments of conviction, but also arrest records and dates of court proceedings.⁵⁴ 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."⁵⁵ 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 still flickers with a "techno-cops" link that allows users to search by name for outstanding arrest warrants and has a "crime of the week" feature that displays full arrest information and mugshots upon selection of an offense from a drop-down menu.⁵⁶

C. *Electronic monitoring.*

The third trend in the use of technology to regulate the dangerous is electronic tracking and monitoring. A variety of such technologies currently exist, falling into two general categories: electronic location monitors and remote alcohol monitors. Currently, the most common use of these technologies is within the criminal justice system, as a form of enhanced surveillance during probation or parole. But attention has increasingly been drawn to using these technologies outside of criminal process.

Of the two, location monitors are by far the most popular. Again, programs vary in the details, including how the system operates, what class of individuals it covers, and how long the monitoring is in place. Some devices rely upon transmitters that only relate whether the individual is within range of a pre-established point. Active GPS systems relate more 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.⁵⁷

⁵⁰ See *Plan Gains to Publicly Identify Accused*, Toledo Blade, Aug. 29, 2006, .

⁵¹ See, e.g., Methamphetamine Manufacturer Registry Act, 730 Ill. Comp. Stat. 180/1-99 (2006).

⁵² Donna Leinwand, States list meth offenders on Web, USA Today, 8/23/06.

⁵³ For example, <https://www.backgroundchecks.com> (last visited Sept. 23, 2006) offers a series of background check packages, ranging from \$19.95 for either a nationwide search of sex offender registries or a single state search criminal history search to \$44.95 for the "U.S. 360° Report," which includes a national search for the addresses, neighbors, family members, single-state criminal history and real property of any person of interest.

⁵⁴ For example, one may visit the website of Washington Access to Criminal History (W.A.T.C.H.) and, upon paying ten dollars, may 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. See <https://watch.wsp.wa.gov/> (last visited Sept. 22, 2006). Florida and Indiana are among other states with such systems.

⁵⁵ *Demery v. Arpaio*, 378 F.3d 1020, 1025 (9th Cir. 2004). For a critical discussion of the implications of jail cameras, see Mona Lynch, *Punishing images*, Punishment & Society Vol. 6(3), 255-70.

⁵⁶ <http://www.mcso.org/submenu.asp?file=MugIndex> (last visited Sept., 2006)

⁵⁷ See, e.g., *Chism v. State*, 824 N.E.2d 334, 335-36 (Ind. 2005).

Presently, at least seventeen states currently have statutes in place that authorize some form of electronic location tracking for sexual offenders on supervised release.⁵⁸ Other states are exploring both legislative enactments or executive orders to implement such programs.⁵⁹ Many programs contain limits that restrict their application to specific classes of offenders, commonly violent sexual predators or those convicted of sex offenses against children.

However, in keeping with the inherent contagiousness of new technologies, location tracking has already spread beyond the regulation of just those sexual offenders on formal release. The current trend is to require lifetime monitoring of certain offenders, either through independent statutory mandate or as conditions of specially concocted mandatory lifetime supervision terms.⁶⁰ Such statutes are drawn on broad categorical grounds, and provide for no individualized determination of dangerousness or likely recidivism.

Further expansions in the categories of persons subjected to GPS monitoring, beyond just convicted sex offenders, are also currently evident. One jurisdiction is contemplating a bill to require tracking and registration of persons never convicted, but instead declared a sex offender according to the lesser evidentiary and proof standards of the civil system.⁶¹ San Bernardino County has initiated a pilot project using GPS tracking to monitor alleged gang members on supervised release.⁶² Surely the use of such devices after formal supervision is a plausible next step, as is extension to other troublesome 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 (or SCRAM), which have also increasingly caught the attention of law enforcement agents. SCRAMs are eight inch devices that attach to the ankle, and tests alcohol concentration levels hourly throughout the day.⁶³ The device then date and time stamps the data and stores it for transmission -- typically to a probation officer -- via the home phone of the individual.⁶⁴ Jurisdictions have adopted the devices as ways of monitoring offenders on release, especially those who have incurred multiple driving under the influence convictions.⁶⁵ According to company materials, SCRAM programs are in place in "35 states and more than 600+ courts and

⁵⁸ These states include Alabama, Arizona, Arkansas, Colorado, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Michigan, Missouri, Oklahoma, South Carolina, Virginia, Washington, and Wisconsin.

⁵⁹ For instance, California, Idaho, Minnesota, Montana, and North Dakota all apparently engage in some forms 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.

⁶⁰ See, e.g., Ga. Code Ann. § 42-1-14; Mich. Comp. Laws § 791.285; Mo. Rev. Stat. § 217.735. California has a ballot initiative for November 2006, Proposition 83, that would enact a lifetime GPS tracking requirement for certain categories of convicted offenders.

⁶¹ See also *Plan gains to publicly identify accused: Ohio panel backs registry proposal*, Toledo Blade, Aug. 29, 2006.

⁶² California 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*, Press Release (Mar. 15, 2006).

⁶³ See <http://www.alcoholmonitoring.com/products/bracelet.html> (last visited Oct. 10, 2006).

⁶⁴ According to one report, the device -- which measures alcohol in perspiration -- is so sensitive that offenders are instructed not to wear cologne, use mouthwash, or any other products containing alcohol. *Keeping Watch: New Device Helping Court Monitor Those on Probation*, The Times Reporter (Dover-New Philadelphia, Ohio), Sept. 6, 2005.

⁶⁵ See, e.g., Tony Bizjak, *Bracelet Monitors Human Drunkenness*, Sacramento Bee, Sept. 23, 2006 (reporting use of device and California Assembly bill that urges county to consider using bracelets); *N.C. Courts test alcohol-detecting bracelet*, Winston-Salem Journal, July 22, 2005.

agencies, conducting more than 27.6 million alcohol tests each year.”⁶⁶ Again, although this technology is presently used for offenders within formal criminal process, it is easy to imagine that -- like the bills requiring lifetime tracking of sex offenders -- similar lifetime monitoring requirements might be imposed upon habitual alcoholics or other such persons.

Unlike DNA collection and online registration acts, challenges to electronic monitoring devices by those outside of the formal criminal system have yet to be fully litigated. However, the courts’ treatment of sexual predator commitment statutes,⁶⁷ coupled with the treatment of sexual offender registration acts,⁶⁸ gives some indication that such programs may very well withstand any constitutional challenge.

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. Various pilot programs have been instituted throughout the country, although most have met with only limited success. Perhaps most famous use of facial recognition technology occurred in 2001, when law enforcement scanned the faces of 70,000 people attending the Superbowl in Tampa, yielding nineteen “hits” to faces of known terrorists, none of which panned out.⁶⁹

Current uses of these technologies are piecemeal. Several airports, including Boston, Tampa, and Virginia Beach, have attempted to implement facial scanning programs at security checkpoints, although again each program met with only limited success.⁷⁰ States have sought to introduced facial recognition software at state motor vehicle offices, to combat identity theft and the fraudulent acquisition of state identification cards.⁷¹ One Florida county has even gone so far as to install 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.⁷² Another pilot program attempted to scan crowds in a downtown district to find felons and runaways, but with no success.⁷³

Iris scanning initiatives have also gained recent ground. According to one report, a county in North Carolina recently initiated a database that stores the biometric images of the iris scans of sex offenders.⁷⁴ Deputies will then be assigned hand-held PDA devices that allow them to scan irises on sight, and connect remotely to the database. Federal customs officials are moving toward iris scanning and digital fingerprinting to document those who enter the country,

⁶⁶ <http://www.alcoholmonitoring.com/about/index.html>

⁶⁷ *Kansas v. Hendricks etc. Kansas v. Crane* (finding constitutional requirement of some inability to control behavior before civil commitment of sexual predator).

⁶⁸ *Smith & Doe*.

⁶⁹ See Barnaby J. Feder, *Technology Strains to Find Menace in Crowd*, N.Y. Times, May 31, 2004, at C1.

⁷⁰ See Lamb, *supra* note XX (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).

⁷¹ See, e.g., Mark Brunswick, *State seeks to get in the face of ID theft*, Star Tribune (Minneapolis, MN), Jan. 6, 2006, at 1B..

⁷² *Facial ID Technology Makes Gains in Florida*, ORGANIZED CRIME DIGEST, May 4, 2005 (reporting that use of technology has led to 45 arrests since implementation nine months earlier).

⁷³ See also *Chambers v. Commonwealth*, No. 2005-CA-000815-MR, 2006 WL 1451566 (Ky. Ct. App. May 26, 2006) (unpublished opinion) (noting that the defendant, who gave a false name on arrest, was identified through an iris scan at the jail).

⁷⁴ *Iris Scans: Keeping an Eye on Sex Offenders*, Newsweek, July 24, 2006.

and now encode biometric information in United States' passports in an effort to integrate scanning systems.⁷⁵ Finally, research is currently underway to develop devices capable of long-range iris scans, which are perceived to have a higher accuracy rate than traditional facial recognition programs.

Because these biometric technologies are still in development, few legal challenges appear to have been yet brought. And, of course, these technologies will be the least dependent on formal criminal process to isolate eligible "dangerous persons" or to exercise oversight in their use. Currently, nothing prohibits law enforcement from snapping a photograph of an individual while in public (or, as the technology develops, a long-range iris scan) and placing it into a database of "suspicious individuals" for later comparison.⁷⁶ The government has, in effect, already established a more rudimentary form of such surveillance in the form of "no fly lists" compiled without any meaningful procedural protections.⁷⁷

II. SURVEYING THE LEGAL LANDSCAPE.

*The dossiers on all citizens mount in number and increase in size.
Now they are being put on computers so that by pressing one button
all the miserable, the sick, the suspect, the unpopular, the offbeat
people of the Nation can be instantly identified.*⁷⁸

As the horizon fills with new technological methods to control and regulate dangerous persons, questions arise about the role that the Constitution and the courts should play in supervising their implementation. Viewed superficially, each of these technologies appears distinct and unrelated. Certainly they do not all operate in the same manner or against the same class of persons. Even with reference to a particular technology, different terms might apply to different categories of offenders. Generally, the appropriate scope of application may turn upon what population is affected -- for instance, the implementation of GPS tracking, DNA typing, biometric scanning, and online indexing to monitor a convicted offender may trigger different concerns than the same devices used to monitor an individual merely suspected of criminal activity.

Notwithstanding these differences, each technology shares two traits in common: each endeavors to control or prevent harm by targeting those "dangerous" to the community for special attention, and each achieves this goal by curtailing in some degree the liberty and privacy of the "dangerous" person. In light of this shared purpose, it is perhaps unsurprising that courts have tended to analyze these technologies as favorable alternatives to physical incarceration, which likewise curtails individual liberty for the purpose of controlling or preventing harm.

But one highly significant factor distinguishes measures of physical incapacitation from the type of technology-based monitoring techniques outlined above: when utilized outside of formal criminal process, physical incapacitation always triggers some measure of procedural and

⁷⁵ http://travel.state.gov/passport/eppt/eppt_2498.html

⁷⁶ See, e.g., *United States v. Dionisio*, 410 U.S. 19, 26 (1973) (facial scars, birthmarks, and other facial features have been said to be 'in plain view' and not protected); *United States v. Karo*, 468 U.S. 705, 711-12 (2005) (finding no expectation in privacy in what is exposed to public).

⁷⁷ See Laura K. Donahue, *Anglo-American Privacy and Surveillance*, 96 J. Crim. L. & Criminology 1059, 1136-37 (2006) (discussing creation of lists forbidding or limiting airline travel by certain individuals but without any procedural safeguards on creation or accuracy of lists).

⁷⁸ *Osborn v. United States*, 385 U.S. 323, 343 (1966) (Douglas, J., dissenting).

constitutional scrutiny that circumscribes the permissible scope of detention.⁷⁹ Recall where this Article began, with *Salerno*. Even though the Court in *Salerno* deemed preventive detention “regulatory” in character, and therefore authorized incarceration of individuals in the absence of full criminal process, the Court specifically cited the procedural protections provided by the Bail Reform Act as support for finding such detentions constitutional. In many respects, the statute provided streamlined criminal process: the prosecutor carried the burden, and had to prove the need for detention by that clear and convincing evidence in an individually-tailored adversarial hearing where the defendant is represented by counsel.⁸⁰ 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, pre-trial period.⁸¹ The Court in *Salerno* specifically relied on these categorical and procedural limitations as evidence that the statute was lawfully tailored, rather than simply a “scattershot attempt[s] to incapacitate those who are merely suspected of crime.”⁸²

In contrast, each of the four techniques outlined in this Article ventures just such a “scattershot attempt.” Not one of the techniques -- DNA typing, online indexing, electronic tracking, or biometric technologies -- requires adversarial process or an individualized determination before use or imposition. Each can apply retroactively, or duplicatively of one another or other forms of restraint. Few impose temporal limitations on its period of use. Rather, technological methods of incapacitation are typically approved without any oversight or scrutiny at all, and with little effort to analyze, much less differentiate, their appropriate scope of application.

Technological restraints pose conceptual challenges to courts, which have grown accustomed to viewing restrictions on liberty through the lens of physical incapacitation as the archetypal paradigm of restraint. But the concerns raised by technological regulations are rarely best encapsulated with reference to their physical dimension. Wearing an electronic bracelet, giving a DNA sample, submitting to facial scanning, or complying with indexing requirements subjects the individual to little to no restrictions on physical liberty, yet each nevertheless causes a real and meaningful deprivation or harm. This Part explores the three primary legal doctrines that serve as gateways to adjudication of procedural and constitutional questions on the legitimate scope of these technologies, and explains how reliance upon the physical paradigm obscures the harm caused by technological regulations and leaves the question of their proper application dangerously unaddressed.

A. *The Dominance of the Physical Paradigm*

1. “Regulatory” v. “Punitive”

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, tailored 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.” A punishment cannot be

⁷⁹ Even the government’s recent attempts to push the limit of this principle met with some resistance. See, e.g., *Hamdan v. Rumsfeld*, 126 S. Ct. 2749 (2006).

⁸⁰ *Salerno*, 481 U.S. at 750.

⁸¹ *Salerno*, 481 U.S. at 750.

⁸² *Salerno*, 481 U.S. at 750.

retroactive,⁸³ cannot be imposed in duplicate,⁸⁴ and certain categories and kinds of punishments such as those that are cruel and unusual are forbidden altogether.⁸⁵

The important determination as to whether a particular restraint constitutes “punishment” is made with reference to a multi-factor test first outlined in *Kennedy v. Mendoza-Martinez*.⁸⁶ In *Mendoza-Martinez*, the Court found that a statute that automatically revoked the citizenship of those who left the country to evade military service was “punitive” in nature and thus violated the Fifth and Sixth Amendments.⁸⁷ Defining the distinction, the Court explained that it first considers whether Congress intends a statutory regulation to be “civil” and regulatory. Typically, this determination reaches no farther than to ask what the legislature intended; ironically, the Court has viewed the failure to include procedural safeguards associated with criminal procedure as an indication that a particular measure is in fact civil and regulatory.⁸⁸

If a statute is intended to be civil, then only the “clearest proof” that the effects of the regulation are punitive “will suffice to override legislative intent.”⁸⁹ 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 assigned....⁹⁰

In the years since its articulation, this seven-factor test has emerged as the standard “in various constitutional contexts,”⁹¹ including in assessing rights related to substantive due process,⁹² procedural due process,⁹³ self-incrimination,⁹⁴ ex post facto,⁹⁵ double jeopardy,⁹⁶ and cruel and unusual punishment⁹⁷ -- are judged.⁹⁸

⁸³ *Kansas v. Hendricks*, 521 U.S. 346 (1996);

⁸⁴ See, e.g. *United States v. Ursery*, 518 U.S. 267 (1996).

⁸⁵ See *Bell v. Wolfish*, 441 U.S. 520, 535 & n.16 (1970). The Cruel and Unusual Punishments Clause applies, as its title suggests, only to punishments. *Id.* at n.16 (noting that the Eighth Amendment applies only after punishment is imposed, and thus concerns about the incarceration conditions of pre-trial detainees are properly addressed as due process matters that ask whether the conditions have matured into “punishments” under a *Mendoza-Martinez* test).

⁸⁶ 372 U.S. 144 (1963).

⁸⁷ *Id.* at 165-66.

⁸⁸ *Smith*. But the inclusion of such safeguards does not necessarily render it punitive, *Allen v. Illinois*.

⁸⁹ *Smith v. Doe*, 538 U.S. 84, 92 (2003).

⁹⁰ *Id.* at 168-69 (footnotes omitted).

⁹¹ *Smith v. Doe*, 538 U.S. at 97.

⁹² *Salerno*, 481 U.S. 746-47 (finding that pre-trial detention is “regulatory” and not “punitive,” and therefore does not violate substantive due process); *Bell v. Wolfish*, 441 U.S. 520, 534 (1979) (rejecting prison conditions case raised by pre-trial inmates on substantive due process grounds because alleged discomfort was not punishment, and did not otherwise “rise to the level of [a] fundamental liberty interests”).

⁹³ *Mendoza-Martinez*, 372 U.S. 144 (1963) (holding that Due Process prohibited imposition of “punishment” of deprivation of nationality in the absence of full criminal process).

⁹⁴ *Allen v. Illinois*, 487 U.S. 364 (1986) (finding that state Sexually Dangerous Persons Act requirement that defendant answer questions about his acts did not violate Fifth Amendment self-incrimination clause, because proceeding was civil not criminal in nature); *United States v. Ward*, 448 U.S. 2424 (1980).

⁹⁵ *Kansas v. Hendricks*, 521 U.S. 346 (1996);

⁹⁶ *Hendricks*, 521 U.S. 346; *United States v. One Assortment of 89 Firearms*, 465 U.S. 354 (1984).

Whereas “punitive” restraints merit intense scrutiny and cannot be imposed without surmounting high procedural hurdles, “regulatory” restraints may operate almost entirely unfettered. A “civil” or “regulatory” restriction can apply retroactively and can duplicate other measures (including punitive ones). Regulatory measures trigger procedural scrutiny only if they implicate a “liberty interest” founded in state law or the Constitution,⁹⁹ and even then the process required before their imposition is likely to fall far short of the full panoply of entitlements given to a criminal defendant. Finally, only substantive due process -- a very hard standard to meet -- can categorically prohibit a regulatory measure of a particular kind.¹⁰⁰

As applied to regulations of individuals using new technologies, it is always the case that the intent of the statute is to protect public safety, and thus the legal status of the measure typically turns entirely on the analysis of the *Mendoza-Martinez* factors. Yet courts examining technological measures under *Mendoza-Martinez* repeatedly analyze the nature of a regulation at issue with reference to physical incarceration or physical intrusion, rather than consider other less corporeal harms. Given that the harm imposed by new technologies can rarely find accurate expression in physical form, the result is that such techniques inevitably are viewed as regulatory, rather than punitive, and thus deserving of no constitutional attention.

For instance, in *Smith v. Doe*,¹⁰¹ 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, which is the paradigmatic affirmative disability or restraint.”¹⁰² Noting that “minor and indirect” restraints are “unlikely to be punitive,” the Court even dismissed even the physical restrictions clearly imposed by the registration statute, such as the “requirement of periodic updates”¹⁰³ 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.”¹⁰⁴ Reliance upon the paradigm of incarceration was likewise used by the D.C. Circuit in *Johnson v. Quander*,¹⁰⁵ in which the court upheld the retroactive application of the DNA collection statute against an Ex Post Facto claim, noting that the “DNA Act ‘imposes no physical restraint, and so does not resemble the punishment of imprisonment.’”¹⁰⁶

Other *Mendoza-Martinez* factors are also applied with narrow reference to the physical world, while simultaneously dismissing its virtual counterpart. In *Smith v. Doe*, the lower court concluded that an online index was “of fairly recent origin” and thus could not qualify as “punishment” given the “history and traditions” of punishment.¹⁰⁷ On appeal to the Supreme

⁹⁷ See *Bell*, 441 U.S. 537 n.16 (noting that Cruel and Unusual Punishments clause protects only those individuals subjected to “punishment”).

⁹⁸ This approach has also been used for to determine cases under the Bill of Attainder Clause, see, e.g., *De Veau v. Braistead*, 363 U.S. 144, 160 (1960).

⁹⁹ See *infra* Part II.B.

¹⁰⁰ See *Bell v. Wolfish*, 441 U.S. 520, 535 & n.16 (1970) (noting concerns about the incarceration conditions of pre-trial detainees are properly addressed as due process matters).

¹⁰¹ *Smith v. Doe*, 538 U.S. 84 (2003).

¹⁰² *Id.* at 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”).

¹⁰³ 538 U.S. at 100.

¹⁰⁴ *Id.* at 101.

¹⁰⁵ *Johnson v. Quander*, 440 F.3d 489 (D.C. Cir. 2006).

¹⁰⁶ *Id.* at 502 (quoting *Smith*)

¹⁰⁷ *Smith v. Doe*, 538 U.S. at 97.

Court, however, the litigants had anticipated this line of reasoning and therefore likened the registry to the shaming and banishments punishments of old. Dismissing the analogy, the Court observed that these historical punishments “staged a direct confrontation between the offender and the public” and “either held the person up before his fellow citizens for face-to-face shaming or expelled him from the community.”¹⁰⁸ The registries, to the contrary, merely “disseminated information,” and its purpose was to “inform the public for its own safety, not to humiliate the offender.” Thus, because the confrontation takes place in virtual rather than physical space, and its purpose informational rather than experiential, it could not be punitive.

In sum, in making the first order determination of whether a measure is regulatory or punitive, and thus whether a host of constitutional protections should govern its application, courts tend to ask whether the restraint on its face resembles physical imprisonment. If the answer is no, which in the case of technological regulations it almost always will be, then the restraint escapes any scrutiny or safeguards.¹⁰⁹

2. “Liberty” and Procedural Due Process

Claims that challenge the application of new technologies on procedural due process grounds likewise rely upon an assessment of the nature of the technological regulation. Similar to the substance of the inquiry in the “regulatory/punitive” analysis, which looks to the effect and context of the restriction, the trigger for procedural due process is whether a cognizable “liberty interest” has been infringed. Such “liberty interests” must materialize either in positive state law or from the fundamental rights enshrined in the Constitution¹¹⁰

Yet, just as above, current doctrine privileges physical deprivations of liberty over other forms of restraint. Common consensus holds that the government most unquestionably infringes liberty when it physically incarcerates individuals. In fact, freedom from “physical detention by one’s own government” has been described as “the most elemental of liberty interests.”¹¹¹ By contrast, the nature of the liberty interest compromised by deprivations of privacy¹¹² or impediments to work,¹¹³ housing,¹¹⁴ or movement are less well-established. As a result,

¹⁰⁸ *Id.* at 98.

¹⁰⁹ There is one factor in the *Mendoza-Martinez* test -- whether the restraint is “excessive” in relation to its purpose - that can transform it from a regulatory to a punitive measure. But because it is so zero sum, it is rarely invoked. (dissenters in *Smith* used).

¹¹⁰ See *Kentucky v. Thompson*, 490 U.S. 454, 460 (1989); see generally Jane Rutherford, *The Myth of Due Process*, 72 B.U. L. Rev. 1, 44-45 & nn. 241-45 (describing the Court’s approach to liberty and summarizing popular critiques).

¹¹¹ *Hamdi v. United States*, 542 U.S. 507, (2004) (citing *Foucha v. Louisiana*, 504 U.S. 71, 80 (1992) (“Freedom from bodily restraint has always been at the core of the liberty protected by the Due Process Clause from arbitrary governmental action”)).

¹¹² In *Paul v. Davis*, 424 U.S. 693, 713 (1976), the Court observed that “[w]hile there is no ‘right to privacy’ found in any specific guarantee in 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.” However, it also noted that “right to privacy cases, while defying categorical description, deal generally with substantive aspects of the Fourteenth Amendment.” *Id.* The Court rejected the defendant’s claim, which was based on the sheriff’s public posting of his 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.” *Id.*

¹¹³ For instance, the Court has held that a state may clearly enact a general scheme of legislation that inhibits an individual’s economic liberty by foreclosing their ability to pursue a lawful occupation. Rejecting the notion that a search of an attorney’s office infringed upon his right to freely exercise his profession, the Court stated that while

technological regulations, which rarely impinge physical freedom in any meaningful way, receive no constitutional attention at all.

For instance, in *DPS v. Doe*, decided in 2003, the Supreme Court addressed a procedural due process challenge to the Connecticut law creating a state sex offender registry.¹¹⁵ The law required every eligible offender to provide the state with personal information including a name, current address of residence, photograph, and DNA sample. 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. The act applied without any individual determination of dangerousness, and its scope included nonviolent offenders. 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.

Eight of nine justices, in addressing a procedural due process claim, agreed that these reporting requirements likely invoked no liberty interest. Arguably, this statute contained an express, recurring deprivation of the defendant's physical liberty: the defendant had to check in at a government office every ninety days for the rest of his life. Yet because the reporting obligation was framed in informational terms, it did not even register with the Court as an infringement deserving of any scrutiny or procedural oversight.¹¹⁶ The closest the *DPS v. Doe* Court could come to recognizing an interest implicated by the mandatory registration and dissemination regime was the nod to a foggy, trivial interest in "reputation" that was deemed non-cognizable.¹¹⁷

Similarly, challenges to DNA collection statutes on procedural due process grounds have likewise been rejected on the grounds that the interest intruded upon does not rise to a constitutionally cognizable level. As the Ninth Circuit 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."¹¹⁸

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." See *New Motor Veh. Bd. V. Orrin W. Fox Co.*, 439 U.S. 96, 106-07 (1978) (upholding California statute regulating grant of franchises in auto industry); see also *id.* at 108 (citing comparable cases).

¹¹⁴ Courts have rejected a constitutional right to housing in a variety of contexts. See, e.g., *Lindsey v. Normet*, 405 U.S. 56 (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 are 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 v. City of Oak Grove*, 374 F.3d 685 (8th Cir. 2004) (finding no property interest in having unlimited access to a public building).

¹¹⁵ 538 U.S. at 1.

¹¹⁶ 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 (1976).

¹¹⁷ Regardless, the Court held, to the extent that a cognizable interest existed, that the offenders' request for individualized determinations of dangerousness were not warranted because the statutory regime drew no distinctions nor worked any deprivations on that basis. 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. 538 U.S. at 9.

¹¹⁸ *Rise v. Oregon*, 59 F.3d 1556, 1562-63 (9th Cir. 1995); see also *Johnson v. Quander*, 370 F.Supp.2d 79 (D.D.C. 2005); *Doe v. Moore*, 410 F.3d 1337 (11th Cir. 2005) (rejecting procedural due process challenge to DNA collection statute due to lack of cognizable liberty interest). A Kansas district court reached the same conclusion, adding that "even if [the] challenge is 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. Bd. of Parole.*, 259 F.Supp.2d 1166, 1169-70 (D. Kan. 2003).

3. Expectations of Privacy and the Fourth Amendment

Finally, Fourth Amendment doctrine requires that courts assess the nature and degree of the interest affected by a technology-based intrusion on the individual. In order to trigger any constitutional scrutiny, a police practice must constitute an intrusion on a “legitimate expectation of privacy” that society is “prepared to recognize as reasonable.” Yet the courts tend to define such expectations with reference to the physical world. Thus, the home remains a citadel¹¹⁹ while the entire genetic make-up of a person is free game so long as it is derived from a discarded Coke can.¹²⁰

Each of the above technologies raises potential Fourth Amendment claims, although not every technology has actually raised them. From cases concerning DNA typing, one of the most developed of the technologies, can be gleaned some sense of the manner in which courts have assessed the nature of the interest at stake.

For example, in *United States v. Kincade*,¹²¹ the Ninth Circuit reviewed the compulsory DNA testing requirement for certain federal offenders. Applying a totality of the circumstances balancing test, the court began by assessing the burden the statute placed on the offenders. The primary approach looked to the *physical* intrusion that a blood test imposes, and concluded that the intrusion was minimal. Of course, the court easily concluded that blood tests are now “routine,” and certainly far less intrusive than the body cavity searches and other physical indignities to which federal offenders are routinely subjected.¹²² Concerns of a less corporeal variety, such as those regarding privacy and misuse of information, were readily disregarded: since the expressed profile included only “a record of the defendant’s identity,”¹²³ retention of both the information and, more problematically, the entire biological sample, was deemed inconsequential.¹²⁴

The Second Circuit’s analysis of the impact of the New York DNA database law was similarly dismissive of noncorporeal interests.¹²⁵ The inquiry began with the physical intrusion, which the court easily immediately discarded as *de minimis*.¹²⁶ To its credit, the court then did expressly admit a second, “potentially far greater intrusion than the initial extraction of DNA,”¹²⁷ 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,”¹²⁸ ignoring that the statutes also sanctioned government retention of the entire DNA sample for no apparent purpose. The closest the court came to acknowledging any less corporeal concerns like the

¹¹⁹ *Kyllo v. United States*, 533 U.S. 27 (2001).

¹²⁰ See generally *Kyllo v. United States*, 533 U.S. 27 (2001). In a high profile Durham, NC murder case, the prosecution presented evidence of the defendant’s DNA on a diet coke can found at the crime scene. See John Springer, *Witness Juggling Puts Trial on Hold*, CourtTVNews, July 30, 2003, available at http://www.courtTV.com/trials/novelist/073003_ctv.html.

¹²¹ 379 F.3d 813 (9th Cir. 2004) (en banc).

¹²² *Id.* at 836-37.

¹²³ *Id.* at 837.

¹²⁴ *Id.* at 837-38.

¹²⁵ *Nicholas v. Goord*, 430 F.3d 652 (2d Cir. 2005).

¹²⁶ *Id.* at 669.

¹²⁷ *Id.* at 670.

¹²⁸ *Id.*

significance of police possession of an individual's entire genomic code,¹²⁹ was to observe that evidence of abuse of samples was "not present here"¹³⁰ and that a range of statutes prohibited the intentional disclosure or misuse of "DNA records"¹³¹ (although notably, not *samples*).

Although challenges to tracking devices placed on humans have yet to fully be aired, there are some indications of how the court has viewed tracking generally. In *Karo*, the Supreme Court found that the Fourth Amendment was not implicated by the use of electronic tracking devices to ascertain publicly available knowledge, like the movement of a vehicle on a public street.¹³² By analogy, it would be easy to argue that the physical intrusion of a monitoring bracelet -- or perhaps even the painless implantation of a chip the size of a grain of rice -- was more like a routine blood test than an intrusive surgery. Any information about movement in public, then, would infringe no cognizable interest.

B. *The Inaptness of the Physical Paradigm.*

Across doctrinal contexts, then, the measurement of the interest implicated by a technological restraint carries great significance. It determines both whether a particular practice is permissible at all, and if so, what standards govern its application. Yet as the preceding section illustrates, courts invariably tend to assess technological regulations by comparing them to the "paradigmatic" or "elemental" interest of physical deprivation of liberty.

Of course, the mere fact that courts compare the harms wrought by new technologies against the standard of the harm of physical incapacitation need not, in itself, raise alarm. Indeed, this failure to privilege interests not founded in physical integrity may be as much a matter of strategy as it is of inattentiveness. Designating a particular measure "punitive," or finding that it intrudes cognizably upon an interest in liberty or an expectation of privacy, as observed above, carries with it a throng of obligations and entitlements. Thus the choice to find a measure "regulatory" is in essence a choice to allow it to operate free of the rubric of the criminal process, which forbids multiple and retroactive punishment, and imposes the highest evidentiary and procedural standards in law. Given that even the most onerous technological restrictions generally do not, in fact, mirror the burden of incarceration, it is perhaps then understandable that courts prove so parsimonious in recognizing measures other than incarceration as necessarily requiring such stringent restrictions on their use.

Yet the problem is that designating a measure "regulatory," or finding that it impinges no cognizable liberty interest or expectation of privacy, is that it grants the measure free reign to operate in a procedural and practical vacuum. But just because the harm wrought by monitoring technologies does not fully replicate the harm of physical incapacitation does not mean that such technologies cause no harm at all. In this sense, the comparison to physical restrictions is inconclusive and inapt.

If the question is simply, "given the choice between intensive technological surveillance and full-fledged incarceration, which infringes liberty more?" then of course few would contest

¹²⁹ N.Y. Exec. Law § 9995-c(5). Of course, 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.

¹³⁰ *Id.* at 671.

¹³¹ *Id.* at 670 (emphasis added) (citing N.Y. Exec. Law § 995-d(1) et seq.).

¹³² *United States v. Karo*, 468 U.S. 705, 711-12 (2005)

that surveillance represents the less intrusive alternative. But that question presupposes that the conditions of application are identical: that, for instance, there is equivalence in the terms of regulation and the determination of who needs regulating. Rephrase the question as a choice between one day of incarceration and a lifetime of intensive technological surveillance, or between incarceration imposed only if the state can meet high procedural hurdles requiring proof of dangerousness versus surveillance imposed without any individualized findings at all, and the answers as to which is worse become more complicated. Indeed, it is not for nothing that some defendants actually prefer incarceration to government supervision,¹³³ or that individuals tend to harbor dread at the thought of engaging with bureaucracies.

Yet 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, in fact, the technology was imposed with specificity or procedural protection remotely approximating that which would have been required for such a physical deprivation.

For example, in *In re the commitment of William P. Browning*,¹³⁴ a Texas Court of Appeals addressed that state's sexual predator commitment act, which allowed for "outpatient" commitment and electronic surveillance. 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*.¹³⁵ Observing that "the intrusion is far less restrictive than if he were confined in a secure facility," the Court upheld the requirements as "nonpunitive," without considering whether the limitations and processes were identical.¹³⁶

Lower courts addressing sex offender registries have likewise contrasted online indexing requirements to incarceration, citing the comparison between online indexing and the "paradigm" of incarceration as grounds for finding registration regulatory rather than punitive. In *E.B. v. Verniero*,¹³⁷ the Third Circuit upheld a sex offender registry, noting that dangerous sex offenders can be detained both pretrial and post-sentence through civil commitment procedures. In contrast, the court commented, "[a]ll Megan's Law mandates is registration and notification.... Certainly, in terms of the impact on the everyday lives of registrants, the burden of this aspect of Megan's Law pales by comparison to the civil commitment of sex offenders."¹³⁸ An Ohio court followed similar reasoning, concluding that: "[t]he impact on the lives of the appellants pales by comparison to the commitment of sex offenders,"¹³⁹ and thus "however onerous the requirement

¹³³ See, e.g., *State v. Cooley*, 587 N.W.2d 752 (Iowa 1998) (reporting that defendant did not desire the "problems and harassment" accompanying any form of probation and therefore "would rather serve his whatever time he gets rather than being put on probation for this"); cf. Lawrence Van Gelder, *Arts, Briefly*, N.Y. Times, April 27, 2006, at E2 (After having been arrested for drunk driving in Hawaii, Michelle Rodriguez, formerly of the television program "Lost," recently faced the choice of going to jail for five days or paying a \$500 fine and spending 240 hours performing community service. Saying, "I kind of have to get back to my life," she chose jail.)

¹³⁴ 113 S.W.3d 851 (Tx. App. 2003).

¹³⁵ 521 U.S. 346 (1997).

¹³⁶ *In re the Commitment of William P. Browning*, 113 S.W.3d at 859. Interestingly, the committed individual also raised a vagueness challenge to the GPS monitoring requirement, because it failed to specify the purpose of such monitoring. In his words, the "requirement implies that [Browning] will be prohibited from going certain places or being in certain areas; however, the prohibited places or areas are not specified, leaving [Browning] uncertain as to what conduct is expected of him." The court rejected the challenge. *Id.* at 864.

¹³⁷ 119 F.3d 1077 (3d Cir. 1997). This was the original "Megan's Law," named after a child who was brutally raped and murdered by a convicted sex offender.

¹³⁸ *Id.* at 1105.

¹³⁹ Other lower courts have taken the hint as well; as one court of appeals explained in examining whether a sex offender statute was permissible, the scheme "imposes no physical restraint." *In re W.M.*, 851 A.2d 431, 444 (D.C. 2004). Typical is the argument of another court, which justified its decision to uphold a state statute by observing

of registration, verification, and notification, the appellants may not be deprived of their liberty under [the statute's] dictates."¹⁴⁰

Yet neither court acknowledged that, although the burden to a sex offender of civil commitment is certainly higher than that of registration, the process surrounding the determination for civil commitment greatly exceeds that surrounding registration in magnitudes of degree. Civil commitment requires some individualized process. In contrast, the registration statutes applied generally and categorically, without exception. Moreover, whereas civil commitment occasions periodic review for continued necessity, the registration statutes carry only abstract and artificial temporal limits -- typically either ten years or life, which have no basis in any empirical information or individualized findings regarding recidivism. Even the Supreme Court in *Smith v. Doe*, specifically rejecting the need for individualized assessment in the case of regulatory registration statutes, differentiated such schemes from confinement schemes on the grounds that the "magnitude of the restraint made individual assessment appropriate." The former "[a]ct, by contrast, imposes the more minor condition of registration."¹⁴¹

The Supreme Court claimed that, to the extent process was necessary, it had already been provided, because the Act only applied to those previously convicted of an offense.¹⁴² Yet registries (or DNA collection or GPS tracking statutes) are more than simply representations of the factual findings of guilt made in a criminal case: they are ongoing, updated resources for current information about an individual. Registries supply up-to-date biographical information about the status, residence and appearance of convicted persons, GPS tracking devices supply real-time information about location, and DNA can supply whatever the science of the day allows it to -- ranging from whether an individual is the biological descendant of the defendant to what health problems run in the family.

The fact-finding in a criminal trial bears no rational relationship to the determination that a particular individual, or even class of individuals, ought to owe the government access to such information -- not beyond the period of time in which the individual is under sentence or supervision. The Supreme Court acts disingenuously in *DPS v. Doe* when it suggests that online registries do nothing more than reflect the fact of conviction, and thus the process of conviction need be all the process required. In fact, the registries contain much more, and the Act demands much more, than that one simple fact of conviction.

None of the technologies described above applies with anything even approximating the particularized and individualized scrutiny that attends physical incapacitation. GPS tracking applies as much to the geriatric offender confined to his bed as it does to the strange pedophile who trolls public parks. Registries require information from the college student who had sex with his under-aged girlfriend, not just the habitual rapist. DNA samples are collected and stored from both the serial killer and the one-time insider trader. Biometric images can arguably be captured and stored without any express legal authority at all.

that, "however onerous the requirement of registration, verification, and notification, the appellants may not be deprived of their liberty under [the statute's] dictates." Other courts have drawn the same analogy, *see State v. Druktenis*, 86 P.3d 1050 (N.M. Ct. App. 2004); *Doe v. Sex Offender Registry Board*, 697 N.E.2d 512 (Mass. 1998); *Commonwealth v. Williams*, 832 A.2d 962 (Pa. 2003).

¹⁴⁰ *NM v. Druktenis*, 135 N.M. 223 (Ct App NM 2004); *Doe v. Sex Offender Registry Board*, 428 Mass. 90 (Mas SJC 1998); *Penn v. Williams*, 574 Pa. 487 (SCT PA 2002).

¹⁴¹ *Smith*, 538 U.S. at 104.

¹⁴² *DPS v. Doe*, 538 U.S. at 7 ("[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.").

At the same time, each of these technologies can and do cause meaningful harms, and pose significant threats to liberty, worth contemplating. In fact, monitoring technologies can approximate, even if they do not wholly replicate, the harms imposed by incarceration by restricting the ability to work, associate, sleep, eat, and live as one chooses -- generally speaking, the same “[l]oss of freedom of choice and privacy” occasioned by jail.¹⁴³ But because such harms do not graft directly onto the harms of physical incapacitation, however, they tend to be wholly overlooked.

III. A NEW TECHNOLOGICAL PARADIGM.

*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.*¹⁴⁴

Given that incarceration provides an ineffective point of reference from which to comprehend the harms wrought by technological regulations of liberty, it remains to ask how might such harms in turn be ascertained or assessed. In order to begin a conversation about what level of procedural scrutiny should attend the use of such regulations, it is first necessary to identify characteristics that distinguish the nature of technological regulations from their more corporeal counterparts.

This section explores three ways in which monitoring technologies encroach upon serious liberty interests given their distinctive manner of operation. The first section argues the manner in which these technologies operate -- in the virtual rather than physical world -- can make the harms they do impose less visible. The next section highlights that the kinds of harms that new technologies impose are of the type and kind that courts have typically struggled to evaluate. The final section underscores that the comparison to physical forms of restraints obscures differences in the economies of scale in the virtual world make the breadth of impact of new technologies less immediately apparent.

A. *The visibility of the harm.*

1. Fragmentation and cumulation.

Physical regulations of dangerous persons are easy to map: the body is free in society, the body is restrained in prison. Even where multiple legal forms of restraint operate -- say, the same person is released in a criminal matter but detained in an immigration matter -- the courts can, and do, keep track of the body. The court has to order up the defendant from the jail to proceed in the criminal trial, even if the defendant is fictionally “free” in the case at hand. The institution of incarceration must keep track of the individual. Conversely, the fiction of physical freedom retains legal import: if the immigration interest dissipates, the physical self is freed.

But technological regulations operate virtually, fragmented from one another and difficult to see cumulatively. Each harm may seem trivial in its isolated appraisal, but severe when

¹⁴³ *Bell v. Wolfish*, 441 U.S. at 537.

¹⁴⁴ *Osborn*, 385 U.S. at 343 (Douglas, J., dissenting).

viewed collectively. In this respect, it is possible to fetter an individual with an entire battery of distinct technological restraints on liberty, without ever having to account for the cumulative effect.

Imagine a fictional offender, perhaps a nineteen year old convicted of having sex with his teen-age girlfriend. He is released from all forms of state supervision but governed nonetheless by a web of technology-based surveillance requirements, all of which apply without regard to whether he poses any actual threat to society. Pursuant to a series of non-detention based statutes, his criminal record, stripped of all context, will be placed online alongside his identifying information, home address, place of work, identifying information, and the make and model of his car. He will be required to take the morning off from work once every three months, so that he can provide an update to law enforcement. In between, if he moves, or borrows a car, or cuts his hair, he will have to notify law enforcement. His DNA is stored in a computer so that every time a crime scene sample is processed in the nation, his DNA profile can be compared. His actual biological genome sits in a police refrigerator, subject only to bare and vague restrictions on its misuse.¹⁴⁵

His face or license plate will be scanned electronically, so that whenever he boards a plane or attends a game, 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 residential zoning laws that prohibit him from living near a school or visiting a public park, thereby isolating him geographically; perhaps a GPS or biometric-based alert will sound if he accidentally travels within the prohibited zones. In short, he will risk exposure each time he enters the public sphere—from a security guard with a biometric scanner, from a police officer who runs a crime scene cigarette butt through the database, or from a vigilante neighbor who thinks that guys like him should be chased out of town.

Despite all of these encumbrances, he will not only be considered free in the eyes of society and the law, he will hardly even be considered fettered. Had the state wished to incarcerate him, he would have received full criminal process. But each regulation in his virtual prison will have triggered barely any attention, and will likely apply absent any individualized determination or formal limitation on use. Moreover, even if he tried, our 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, which considered on its own may appear *de minimis*. There is simply no legal claim of “it is all too much,” or even “if you put it all together, it is almost as if I were in jail.” Viewed independent of one another, no isolated form of regulation presents as particularly burdensome or unreasonable.

Even if the harm could be assessed cumulatively, there would remain a practical impediment to objecting to its forms of imposition. Technological regulations come to court cloaked in legal claims of various stripes, often dictated by the way in which the intrusion was imposed. DNA collection and sex offender registration requirements are typically the product of legislation action, whereas biometric scanning and electronic tracking frequently stem from

¹⁴⁵ *Police DNA Database is ‘Spiraling Out of Control*, THE OBSERVER (U.K.) July 16, 2006 (reporting scandals in England regarding private company’s retention of genetic samples sent to lab for outsourced testing, as well as reports that the Home Office gave permission for controversial genetic studies to be conducted on samples).

executive action.¹⁴⁶ It might be the probation officer that enforces registration and electronic tracking requirements, whereas the police departments collect the DNA samples and the corrections officer captures the biometric image. Thus, the caption of the challenge might be different, according to the technology. Moreover, some technologies -- like biometric scanning -- are more likely to be challenged piecemeal by individual defendants detained or arrested after a positive scan, whereas others such as GPS tracking are more readily imagined as class actions against the regulating body.

Similarly, the legal basis for lawsuits challenging these technologies varies across techniques. Claims related to DNA collection statutes, which have thus far primarily addressed DNA collected from convicted offenders, have tended to raise Fourth Amendment arguments that they constitute warrantless, suspicionless searches,¹⁴⁷ and Ex Post Facto or Double Jeopardy claims of previously convicted persons.¹⁴⁸ Litigation on sex offender registration acts, meanwhile, has tended to focus on Equal protection or Substantive or Procedural Due Process claims, although Ex Post Facto and Double Jeopardy claims have been raised as well.¹⁴⁹ It is easy to imagine that biometric technologies will be raised piecemeal in the Fourth Amendment litigation of individual defendants stopped or searched on the basis of electronic recognition, while GPS tracking statutes will be more likely to be attacked on due process or equal protection grounds as statutes impose monitoring requirements on individuals. There simply is no obvious legal mechanism for claiming that the technological restraints, operating collectively, impose such a burden that some measure of process, or limitation on the applicable duration or scope of implementation, is required.¹⁵⁰

2. Stigma and the delegation of harm.

The harms wrought by new technologies are not just difficult to visualize because they are often diffused into component fragments of regulation, but also because they are often imposed not by the state itself directly, but by a third party. Technology in essence permits the government to delegate to the populace at large the responsibility and authority to regulate targeted individuals.

Consider that, 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 means that government is democratically accountable for the harms it imposes on an individual. This accountability has legal resonance, as well. The writ of habeas corpus provides an avenue of relief from wrongful incarceration, and 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

¹⁴⁶ Increasingly, however, states have moved to enact legislation providing for GPS tracking of certain offenders. *See, e.g.*, N.J.S.A. 30:4-123:83 (providing for two year pilot program for “continuous, satellite based monitoring of not more than 250 subjects”); *infra*.

¹⁴⁷ *See infra*.

¹⁴⁸ *See infra*.

¹⁴⁹ *See, e.g.*, E.B. v. Verniero, 119 F.3d 1077, 1101-02 (1997).

¹⁵⁰ 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.”).

maintenance of its inmates. When a man is sent to prison, it is unambiguous where he is, who sent him there, and who is responsible for his continued welfare.

But while physical punishment is the monopoly of the state;¹⁵¹ virtual punishment may be meted out by the masses. If a regulated individual cannot rent an apartment or find a job because of an online record, who is responsible? If a vigilante determines to violently assault or even kill someone based on the database, who is responsible? If an individual is arrested on the basis of a “familial search” of a DNA database in which his relative’s DNA was entered, who is responsible? Likely, not the state. Technology enables the state to delegate to the populace some of its role in monitoring and controlling the dangerous. Any harms suffered as a result, therefore, need not be its responsibility.

That is, current legal doctrine permits the state to distance itself from such consequences. That is, 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*, which involved the distribution by police chiefs of a flyer displaying “active shoplifters,” the Supreme Court held that “defamation of an individual, standing alone” does not deprive any protected liberty interest.¹⁵² In *DPS v. Doe*, noting that “mere injury to reputation, even if defamatory, does not constitute the deprivation of a liberty interest.”¹⁵³ 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.¹⁵⁴ The hand of the government in inflicting the restraint vanishes, and only the public and the offender remain.

Disavowing stigma as a cognizable injury in essence authorizes the state to serve as an intermediary between the individual and the public, while simultaneously disclaiming any responsibility in that role. If the individual cannot work, or find housing, or get employment, or otherwise faces violence or discrimination, it need not be traceable back to state action.

B. The nature of the harm.

¹⁵¹ See MAX WEBER, *POLITICS AS A VOCATION* (1918) (defining a state as an entity which claims a monopoly on the legitimate use of physical force in a given territory).

¹⁵² *Paul v. Davis*, 424 U.S. 693, 708 (1976). 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. 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; the Court stated that “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.* at 437. 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 709. Instead, the linchpin was that the state action caused “a right or status previously recognized by state law” to be “distinctly altered or extinguished.” *Id.* at 712. Because “any harm or injury to the [interest in reputation] . . . does not result in a deprivation of any “liberty” or “property” recognized by state or federal law,” it need no procedural safeguarding. *Id.* at 712.

¹⁵³ *DPS v. Doe*, 538 U.S. at 6-7.

¹⁵⁴ *Smith v. Doe*. at 99.

In addition to the problems that new technologies pose in terms of their diffusion and delegation of harm, the particular kind of harm wrought by these techniques also tend to be more difficult to value. Current doctrine privileges harms of the corporeal kind: most deprivations of physical liberty trigger some measure of scrutiny or review. Accordingly, courts tend to evaluate new technologies with reference to their physicality, asking questions such as: How painful is the blood sampling? How cumbersome is the GPS bracelet? Do you even notice when your face is scanned?

But as even the Supreme Court has acknowledged, “liberty” protects more than just physical freedom: “[a]lthough the Court has not assumed to define “liberty” . . . with any great precision, that term is not confined to mere freedom from bodily restraint.”¹⁵⁵ Nevertheless, to the extent that some non-corporeal interest in liberty is acknowledged, it tends to be devalued or dismissed as non-cognizable an interest in “reputation” or “stigma.” Even Justice Stevens, the only justice to recognize a liberty interest in the sex offender registration cases, had trouble quantifying it. In his dissent in *Smith v. Doe*,¹⁵⁶ which also constituted his concurrence in *DPS v. Doe*,¹⁵⁷ the best he could muster was to state that “these statutes unquestionably affect a constitutionally protected interest in liberty.”¹⁵⁸ New technologies implicate core concerns of liberty and privacy; they are just of a variety that courts have been reluctant to recognize.

Corporeal harms are privileged because they are objectively identifiable and presently realized; the loss of liberty suffered by an incarcerated person is incontestable and real. The harm of technological surveillance, in contrast, is founded less upon the actual intrusion or injury visited on the regulated subject, than upon the uncertainty that exposure to such harms creates. Indeed, technology can injure even without notifying the injured party. A DNA sample may be extensively and impermissibly researched, cloned, or tested, and yet the subject need never be told. No alert sounds when a name is run through a computer records search, database, or online index. The 70,000 fans at the Tampa so-called “Snooperbowl” undoubtedly rooted for their teams without feeling any sense of personal intrusion, and one may go for an evening walk unaware that a camera records every step.

Yet lack of notice as to the precise instance of intrusion or injury does not eliminate the existence of cognizable injury altogether. That is because the harm to liberty caused by technological surveillance is not just the harm of the actual intrusion, but also the harm caused by the risk of intrusion. In his taxonomy of privacy, Daniel Solove identifies “architectural problems” that result from invasions of privacy, which “involve less the overt insult or reputational harm to a person and more the creation of the risk that a person might be harmed in the future.”¹⁵⁹ This risk take two shapes: first, as an “enhancement of the risk that a harm will

¹⁵⁵ *Bolling v. Sharpe*, 347 U.S. 497, 499 (1954). Indeed, the Court has held that 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.” *Conn v. Gabbert*, 526 U.S. 286, 291 (1999) (quoting *Bd. of Regents v. Roth*, quoting *Meyer v. Nebraska*, 262 U.S. 390, 349 (1923)).

¹⁵⁶ 538 U.S. at 84 (Stevens, J., dissenting).

¹⁵⁷ Justice Stevens observed that, under the Alaska statute, registrants had “one working day” to provide updated information upon moving, and that they could not “shave their beards, color their hair, change their employer, or borrow a car without reporting those events to authorities.” *Id.* at 113.

¹⁵⁸ *Id.*

¹⁵⁹ Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 487-88 (2006).

occur” and second, as an “upset” in “the balance of social or institutional power in undesirable ways” that leads to a “chilling effect.”¹⁶⁰

Technological regulations evade necessary scrutiny because their greatest impact is in the form of these contingent risks. Yet the mere contingency of the realized harm does not render the technology harmless.¹⁶¹

1. Risk of misuse, error, or misappropriation.

The first kind of architectural interest labels exposure to harm as itself a form of harm. Conventionally, mere risk of injury has been considered “speculative” and non-cognizable by courts. Courts have dismissed the risks posed by public dissemination of current biographical data of sex offenders as mere “conjecture.”¹⁶² The potential for misuse in the collection and retention of genetic samples has likewise been discarded as merely speculative, and litigants chastised for arguments based “not on dramatic Hollywood fantasies ... but on concretely particularized facts....”¹⁶³ But this approach overlooks what conventional privacy doctrine has increasingly recognized, that the harm is the insecurity,¹⁶⁴ or the speculation or risk of abuse, not just the actual abuse itself.

Ironically, courts have proven more forgiving with regard to analysis of the benefit or advantage of a technology. In assessing the benefit to “public safety” advanced by sex offender registries, for instance, the Court observed that there existed a “high rate of recidivism among convicted sex offenders.”¹⁶⁵ The Court then concluded that the requiring sex offenders to register was therefore “reasonable.”¹⁶⁶ Yet there was no discussion, much less evidence, about whether registration in any way reduced recidivism or worked to prevent future crime.

Indeed, given the broad and inclusive scope of the statute at issue, which applied broadly and included even offenders who could prove that they posed “no threat of recidivism,”¹⁶⁷ the notion that registration in fact prevents recidivism seems itself, at best, conjecture and speculation. Likewise, courts across the board have deemed collection and retention of DNA samples as serving “society’s enormous interest in reducing recidivism,”¹⁶⁸ or “solving

¹⁶⁰ *Id.* at 489.

¹⁶¹ See also 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))).

¹⁶² See, e.g. *Smith*, 538 U.S. at 100.

¹⁶³ *Id.* at 837-38. In *Johnson v. Quander*, the Court held that “[n]othing in the record suggests such future testing is imminent, nor can we analyze its invasiveness until it appears,” 440 F.3d at 500. One state court frankly concluded that the “assertion that the state might misuse the information 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. 1997).

¹⁶⁴ See, e.g., *Kehoe v. Fidelity Bank Trust*, 421 F.3d 1209 (11th Cir. 2005) (finding that statute did not require proof of actual damages to privacy in order to recover liquidated damages); Post, at 960 (citing *Hamberger v. Eastman*, noting that court found “gravaman of the plaintiff’s cause of action rested solely on installation of intrusive device” by landlord, rather than on actual listening to conversations); Solove, *supra* note X, at 518 (describing cases that recognize privacy interest founded in security of information).

¹⁶⁵ *Smith*, 538 U.S. at 103.

¹⁶⁶ *Id.*

¹⁶⁷ *Smith*, dissent, at 193.

¹⁶⁸ *Kincade*, 379 F.3d at 838.

crimes.”¹⁶⁹ Yet courts fail to substantiate either of those claimed interests with actual data demonstrating the actual efficacy of indiscriminate DNA collection -- much less *sample retention* -- on deterring or solving crime.¹⁷⁰ Instead, speculation regarding the success of collection and retention apparently sufficed.

In contrast, strong evidence demonstrates that technological restraints do in fact expose the individual to meaningful harms. Thus, even if speculative in an individual case, such harms are not wholly imaginary. For example, the adverse consequences suffered by those required to register publicly as sex offenders have been well documented. Perhaps most dramatic and notorious is the killing of two sex offenders by a vigilante in Maine in 2006.¹⁷¹ The killer, who hailed from Canada, located and identified each offender according to an online profile that contained the offenders’ pictures, address, and other personal information was posted. One of the victims was a young man whose only conviction was for having consensual sex with his girlfriend when she was fifteen.¹⁷²

More mundane incidents of violence and discrimination have been well-documented across the country. In the words of Justice Souter, concurring in *Smith v. Doe*:

It is true that the Act imposes no formal proscription against any particular employment, but there is significant evidence of onerous practical effects of being listed on a sex offender registry. *See, e.g., Doe v. Pataki*, 120 F.3d 1263, 1279 (C.A.2 1997) (noting “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”); *E.B. v. Verniero*, 119 F.3d 1077, 1102 (C.A.3 1997) (“The record documents that registrants and their families have experienced profound humiliation and isolation as a result of the reaction of those notified. Employment and employment opportunities have been jeopardized or lost. Housing and housing opportunities have suffered a similar fate. Family and other personal relationships have been destroyed or severely strained. Retribution has been visited by private, unlawful violence and threats and, while such incidents of ‘vigilante justice’ are not common, they happen with sufficient frequency and publicity that registrants justifiably live in fear of them”); Brief for Office of the Public Defender for the State of New Jersey et al. as *Amici Curiae* 7-21 (describing specific incidents).¹⁷³

Moreover, online indexes have an alarming tendency to be wrong, and contain outdated or inaccurate information.¹⁷⁴

¹⁶⁹ *Goord*, 430 F.3d 630.

¹⁷⁰ In fact, most data on the efficacy of DNA testing appears to demonstrate its ability to exculpate offenders in specific cases.

¹⁷¹ John R. Ellement & Suzanne Smalley, *Sex Crime Disclosure Questioned: Maine Killings Refuel Debate Over Registries*, BOSTON GLOBE, Apr. 18, 2006; *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 (Maine) April 19, 2006 (listing other instance of vigilantism).

¹⁷² *Id.*; *see also* Judy Harrison, *Deaths of gunman,; Sex Offenders Probed*, BANGOR DAILY NEWS (Maine), Apr. 19, 2006.

¹⁷³ *Smith*, 538 U.S. at 109 n.* (Souter, J., concurring).

¹⁷⁴ *See, e.g.*

http://www.nytimes.com/2006/10/17/us/17expunge.html?_r=1&hp&ex=1161144000&en=b41c734d19a150a1&ei=5094&partner=homepage&oref=slogin

Or consider the range of scandals concerning mishandling and malfeasance in DNA typing, which have resulted in wrongful arrests and incarceration. In Houston, a DNA analyst falsely implicated Josiah Sutton in a murder; he served four and a half years in prison until another test exonerated him.¹⁷⁵ At a Las Vegas lab, a laboratory technician mislabeled the samples, resulting in a wrongful accusation of double rape. The Virginia laboratory botched two DNA tests for Earl Washington, Jr., allowing him to linger on death row until a 2004 tests exculpated him. 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. 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.

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 assault. 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.¹⁷⁶ Each of these instances reveals the extent to which exposing genetic information -- whether a simple profile or a sample containing one's entire genetic code -- compromises one's ability to maintain anonymity and privacy.

2. Autonomy and self-realization.

Beyond mere fear of misuse, however, lies a distinct interest founded at the border between privacy and liberty. This interest captures the need for a sphere of autonomous space necessary to constitute a personal self. It is linked to the familiar trope of Jeremy Bentham's Panopticon, which conceives of surveillance as a means of control and power.¹⁷⁷ Robert Post describes this interest as distinct from abstract notions of intimacy or seclusion, but rather about the maintenance of "the forms of respect deemed essential for social life, ... relatively indifferent to whether particular forms of respect should be denominated as "privacy.""¹⁷⁸

The Supreme Court's decision in *City of Chicago v. Morales*, can be read as essentially acknowledging this interest, by invalidating on vagueness grounds an ordinance that vested law enforcement with authority to disperse congregations that included alleged gang members. Recognizing what the plurality termed the "attribute of personal liberty" known as the "right to remove from one place to another according to inclination,"¹⁷⁹ the Court found that the ordinance

¹⁷⁵ See Murphy, *supra* note X.

¹⁷⁶ Antony Barnett, *Police Database 'is spiraling out of control': Secret emails show private firms store genetic data from innocent victims*, The Observer (London) (July 16, 2006).

¹⁷⁷ In this respect, it is the object of controlling information, rather than the means by which it is controlled, that matters. 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." Mark Poster, *Databases as Discourse, or Electronic Interpellations*, in *THE SECOND MEDIA AGE*, at 85.

¹⁷⁸ Robert Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 971 (1989). "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.

¹⁷⁹ *Chicago v. Morales*, 527 U.S. 41 (1999).

granted too much discretion with law enforcement to intrude upon the lawful activity of citizens. This liberty interest -- which the dissenters derisively called a “Fundamental Freedom to Loiter”¹⁸⁰ -- in essence protects some notion of freedom that is not so much about physical restraint, but rather about autonomy and self-direction without (unjustified) interference from the state.¹⁸¹

This notion of freedom from interference accords with Isaiah Berlin’s expression of two concepts of liberty: “positive freedom,” which “consists in being one’s own master,”¹⁸² and “negative freedom,” or the freedom of “not being interfered with by others.”¹⁸³ “Positive freedom” captures the desire to “be somebody, not nobody; a doer -- deciding, not being decided for, self-directed and not acted upon by external nature....”¹⁸⁴ It is the freedom of self-direction and self-realization. In contrast, “negative freedom” acknowledges that “a frontier must be drawn between the areas of private life and that of public authority,” even if “[w]here it is to be drawn is a matter of argument.”¹⁸⁵ It is this “minimum area of personal freedom” which is a necessary pre-condition to positive freedom, or to creating the conditions in which an individual can be “a being with a life of his own to live.”¹⁸⁶ Solove’s architectural interests captures this same desire to preserve a field of negative liberty by noting that incursions into that interest can have a “chilling effect,” causing the individual to withdraw from society.¹⁸⁷

A state imposing physical incarceration strips the individual of both types of freedom: the prisoner loses both the capacity for self-determination and the right to non-interference. A state regulating a dangerous person using the technologies above, in contrast, can leave the former interest largely untouched while greatly undermining the latter interest.¹⁸⁸ 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 prevented by the state from self-realization. Indeed, courts repeatedly focus upon this freedom in justifying the technological intrusion, noting that none of these technologies prohibit the individual from choosing freely where to go

¹⁸⁰ *Id.* at 84 (Scalia, J., dissenting).

¹⁸¹ *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.”). Robert Post’s account of the normative underpinnings of the intrusion tort describes how “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.” Robert Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 973 (1989).

¹⁸² *Id.* at 131.

¹⁸³ ISAIAH BERLIN, *FOUR ESSAYS*, at 122-23.

¹⁸⁴ *Id.* at 131.

¹⁸⁵ *Id.* at 124. Note that he clarifies that only about limitations placed by others; the inability to self-realize due to limitations of one’s own self, or of the physical world, don’t count. *Id.* at 122.

¹⁸⁶ BERLIN, *supra* note at 126-67. Note that Berlin critiques Mill’s account of negative liberty, on the grounds that 1) Mill equates all coercion as bad, even though some might be good; 2) Mill assumes that self-realization cannot occur without freedom from interference, yet history (in totalitarian states) suggests otherwise. But just points out that can argue about size of space.

¹⁸⁷ Solove, *supra* note X, at 489.

¹⁸⁸ 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 superpanopticon if you will, which reconfigures the constitution of the subject.” Mark Poster at 277. Although Poster’s comments relate only to databases, and include all forms (not just public regulatory) of databasing, his observations that “[c]omputerized databases are nothing but performative machines, engines for producing retrievable identities” rings particularly true in the context of preventive regulation of the dangerous. At 280.

or what hairstyle to wear or what job to take.¹⁸⁹ In the straightforward estimation of the Supreme Court reviewing a sex offender registration statute: “Although registrants 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*.”¹⁹⁰

Rather, 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 he may do so without an actual or perceived risk of interference by others or the state. In this respect, the comparison to physical incarceration becomes even less instructive as a means for understanding the harm wrought by a technological regulation. Of course a SCRAM bracelet wearer’s inability to perfume or use mouthwash causes less of an interference than full-fledged incarceration; but that is not to say it causes no interference at all. And the interference, moreover, is different in kind than that of an incarcerated person: it is about the capacity to construct an identity free of state control, an attribute of free persons that does not inhere to inmates. The deprivation is not simply the ability to communicate with one others, but rather the symbolic and actual capacity to realize personal identity and relationships unhindered by government controls.

Yet, this more subtle notion of non-interference receives no recognition from the courts, and is difficult to articulate with precision. For instance, the Seventh Circuit recently upheld an unlimited, likely lifetime ban of one particular convicted sex offender from all public parks in a city’s jurisdiction that was issued on the basis of a request by a police chief to the park superintendent.¹⁹¹ Undertaking an examination of the “liberty interest” at stake, the court discarded the notion that the interest was “a generalized right to movement” or “to travel through parts of the City to engage in religious, political, commercial, or social activities.”¹⁹² Doe 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,”¹⁹³ an interest labeled by the Court as the “right to enter to parks to loiter or for other innocent purposes.” The court found such a right “while not unimportant,” not “fundamental,”¹⁹⁴ observed that “[t]he historical and precedential support for fundamental right to enter parks for enjoyment is, to put it mildly, oblique,” and upheld the letter indeterminately banning the individual from all parks.¹⁹⁵

Of course, one easily imagines that Doe’s list was not exhaustive. That is because the asserted interest is not literally a desire grounded in engaging in certain specified activities; the true nature of the claim is the right to enter parks without having to explain or justify your decision to be there to the government.¹⁹⁶ Similarly, the interest infringed by GPS monitoring in

¹⁸⁹ See, e.g., *Femedeer v. Huan*, 227 F.3d 1244 (10th Cir. 2000).

¹⁹⁰ *Smith*, 538 U.S. at 102.

¹⁹¹ *Doe v. City of Lafayette*, 377 F.3d 757, 760 (7th Cir. 2004).

¹⁹² *Id.* at 769.

¹⁹³ *Id.* at 769 n.11.

¹⁹⁴ *Id.* at 770.

¹⁹⁵ *Id.* at 771. The court added that Doe “cites no case, state or federal, that has held that he right to enter a park to loiter or for other enjoyment purposes is fundamental.” *Id.* As for the *Morales* case, the court simply contested the plurality intended “in this statement any fundamental rights analysis.” *Id.* 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.*n.13 (citing Rotunda & Nowak).

¹⁹⁶ In fact, the Court even used as an argument that the right was not fundamental the fact that Doe had not entered a park in four years. Of course, such reasons precisely undermines the notion of freedom from government

not the ability to decide to go into the bookstore, or to drive a certain route home, or stay out until four in the morning; it is the capacity to make those choices without thinking “what will the government think of this?” Online indexes likewise minimally infringe positive liberty -- requiring only that the offender “check in” once every three months -- but they greatly intrude upon negative freedom by threatening the autonomous sphere in which the individual makes decisions about how to live, work, travel, or wear one’s hair.¹⁹⁷

These technologies, which allow the government to isolate or identify a suspicious individuals from among the anonymous masses, in some respects pose the greatest threat to this notion of liberty. An offender may know he wears a GPS bracelet or that his biometric image or DNA profile is held in a database, but he does not know when someone is watching his particular movements or running a particular search. As Daniel Solove observes, “there can be an even greater chilling effect when people are generally aware of the possibility of surveillance, but are never sure if they are being watched at any particular moment.”¹⁹⁸ Thus, while such techniques do not prohibit an individual from going to the football game or boarding the airplane or driving through the city, they raise the very real specter that doing so will expose the individual to government inquiry or control.

In a sense, a closer analogue might be found in the recent proliferation of outpatient civil commitment statutes.¹⁹⁹ 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.²⁰⁰ 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 physical freedom, constitute a serious intrusion upon individual liberty.²⁰¹ Surely our understanding about the infringement entailed relates more to ideals of autonomy and non-interference than to the simple fact that a person must show up at the hospital once a month.

In short, technological regulations raise impinge not so much on the ability to self-determine as upon the capacity to do so outside of the watchful eye of the government. Of course, the government can and does intrude upon individual autonomy in a range of ways in a civilized society, and the permissible scope of that interference is a constant source of

interference by presenting liberty as a use-it-or-lose-it entitlement. Another case similarly reveals the cramped vision 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. *Thompson v. Ashe*, 250 F.3d 399 (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.” 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 individual how he or she may seek to be removed from the list.” *Id.* at 404. In fact, “no established procedure exists to remove individuals from the no-trespass list.” *Id.* Violators are arrested and prosecuted for trespassing. 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 407.

¹⁹⁷ *Smith*, 538 U.S. at 7.

¹⁹⁸ Solove, *supra* note X, at 495.

¹⁹⁹ John Monahan, *A Jurisprudence of Risk Assessment: Forecasting Harm Among Prisoners, Predators, and Patients*, 92 Va. L. Rev. 391, 401-02 (2006).

²⁰⁰ *Id.* at 402 n.42.

²⁰¹ *See, e.g., In the Matter of K.L.*, 806 N.E.2d 480 (2004).

disagreement. The trouble is that the nature of the harm to liberty wrought by technological regulations has not managed to trigger enough interest to even enter the debate.

C. Net widening.

Lastly, the scope and application of technological restraints tends to evade notice in part because their implementation is typically contemplated with reference to the economies of the physical world, rather than to its digital or virtual analogue. That is, the typical assessment of technological advances is that they simply render the ordinary mechanics of criminal process more accurate, less intrusive, and more efficient. In this view, GPS tracking simply enables a one-for-one swap; rather than lock up the offender, we can place him on tracking, which even he would probably prefer to jail. Instead of questioning every fan at the ballpark, we can sit silently on the sidelines with our iris scanner in hand or our DNA swab ready. Rather than go downtown to look up the criminal record of my new neighbor, I can just run a web search online.

As the majority in *Smith v. Doe* contended, in responding to the complaint that sex offenders suffered adverse consequences from public posting of their criminal histories, “[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.”²⁰² Dismissing the notion that any special significance should be accorded to the fact that online publication made intimate information available world-wide, the Court reasoned that “the process is more analogous to a visit to an official archive of criminal records than it is to a scheme forcing an offender to appear in public with some visible badge of past criminality.”²⁰³ Rather than view internet publication as significantly enlarging the population of persons with access to the information, the Court asserted that it simply “makes the document search more efficient, cost effective, and convenient.”²⁰⁴

But technologies do not simply provide more efficient means to the same end. In fact, technology has the capacity to alter, not just mechanize, our actions. This phenomena of “net widening” is well-documented.²⁰⁵ Its principles are intuitive: think about the local red light-runner camera installed at the corner intersection. This technology enables law enforcement, for minimal expense,²⁰⁶ to photograph every car that passes through a red light and then instantly mail a ticket to the owner of the offending car. Obviously, it is not the case here that technology has no effect on the rate of apprehension; before the camera, myriad constraints prevented officers from achieving perfect enforcement of the traffic code. Instead, technology allows the

²⁰² *Smith*, 538 U.S. at 100.

²⁰³ *Id.* at 99.

²⁰⁴ *Id.* Interestingly, the 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 (Maine), April 30, 2006 (describing how killer compiled a list before leaving his home in Nova Scotia).

²⁰⁵ Even more pertinently, 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. STANLEY COHEN, *VISIONS OF SOCIAL CONTROL* 43 (1985). 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.

²⁰⁶ See, e.g., Howard County, Maryland Police Department, Red Light Camera Program, available at http://www.co.ho.md.us/Police/pd_redlight.htm (last visited October 2, 2006) (reporting 70% reduction in red light violations at monitored locations, and claiming cost savings over old three hour enforcement method, which cost roughly “\$360.00 for personnel alone”).

net to widen—now instead of catching five red-light runners a day, the camera can catch fifty. To say that an individual receiving a camera-issued ticket is in no different position than a person would be had the police happened to be watching that intersection, then, is to miss the point. In fact, the implementation of the technology radically alters the position of the driver, who goes from one set of odds of apprehension to another magnitudes higher.

Thus, the right story to tell about the development of technological forms of surveillance and control is not one of streamlining or one-for-one substitution, but proliferation, expansion, and enhancement. GPS is not used to release more offenders from the greater intrusion of incarceration, but is instead used to regulate some individuals that would have instead remained fully free. The ballpark passengers would not have each been interrogated; they would have been left undisturbed unless they aroused some suspicion. The neighbor never would have gotten around to going downtown to check the records in the first place. The trade-off is rarely jail-for-life versus GPS-for-life, or records-checked-downtown versus records-checked-online; it is free versus fettered, anonymous versus exposed. As the Court in another context has acknowledged, a significant change occurs when “scattered ... bits of information” are collected into a “compilation of otherwise hard-to-obtain information.”²⁰⁷

Moreover, technology transforms passive information into actively available data. Whereas biographical information, including names, fingerprints, and so on -- might have technically been indefinitely stored in the past, the confines of the physical world curbed the true scope of retention and recollection. Historically, to say that a record is indefinitely retained did not mean that it was instantly available, as it does today. The file went in the cabinet, to be stored in case needed in the future. But today, record retention enables data-mining; the file goes in the database as the template against which searches are run and comparisons can be made on a daily, or even multiple times daily, occasion.

The computerization of information into databases -- whether genetic, biometric, biographical or geographical -- enables the activation of previously passive collections of acquired knowledge. Thus, it is not enough to say “law enforcement has always collected this data”; fair analysis requires further consideration of how technology has changed what that means in terms of how the collected data is used. The Court in *Smith* wrongly analogized an inquiry into a sex offender registry to “a visit to an official archive,”²⁰⁸ because the “official archive” would not have -- as did the registry -- a current photo of the individual along with current information about his address, workplace, or other biographical characteristics. Moreover, the registry might get thousands of visitors a day, whereas the archive could not manage that many in a year.

In short, the economies of restraint are different for the technological world than for the physical one. 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.”²⁰⁹ Websites can be maintained at relatively small expense. DNA collection, storage, and processing are becoming cheaper every day, and with automation the expense will continue to drop precipitously. GPS monitoring costs as little as eight to ten dollars a day.²¹⁰ Biometric

²⁰⁷ *United States Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 764, 109 S.Ct. 1468, 1477, 103 L.Ed.2d 774, 790 (1989)).

²⁰⁸ *Smith*, 538 U.S. at 181.

²⁰⁹ Ronald Corbett, Gary T. Marx, *Critique: No Soul in the New Machine: Technofallacies in the Electronic Monitoring Movement*, JUSTICE QUARTERLY, Vol. 8 No. 3 Sept. 1991, at 400.

²¹⁰ This, of course, is compared to the estimated forty to one hundred dollars daily it requires to incarcerate someone.

technologies require only an initial capital investment. And many technologies have built within them mechanisms for recouping their minimal cost: jurisdictions increasingly require solvent defendants to pay for their own electronic tracking devices,²¹¹ or else charge a nominal fee for records searches performed online.²¹²

In part because technologies cost less per person to implement, they can be used against a greater volume of individuals and for a longer period of time. For the cost of one incarcerated body, the government can track ten wearing GPS bracelets. Instead of deploying a large team of officers responsible for searching and identifying randomly selected persons, biometric techniques allow rapid identification of known suspects so that resources can be concentrated on particular areas or trouble spots. In the time it takes for a detective to interview one witness, a DNA database might yield suspects in a wide array of cases. Because technology is efficient, its methods can be deployed in greater volumes. Similarly, once ensnared in a technological restraint, few durational restrictions limit the extent to which the harm can be suffered. Jail terms are limited and finite, but the Internet lives forever. A photograph or DNA sample can trigger scrutiny indefinitely, both in terms of the length of time to which the person is vulnerable to intrusion, and the frequency with which that intrusion occurs.

Technological costs also tend to level out, or even diminish, over time. The state incurs its most significant expense in processing the DNA sample, creating the online index, scanning the biometric image or affixing the GPS bracelet affixed. Once that is done, the cost of continued monitoring and restraint is significantly diminished. Whereas the jail cell costs the state the same on day one as it does on day one thousand, technology tends to front load its capital outlay, and then coast along with only minor upkeep or expenditures.

Thus, for instance, many of the above techniques already can and do operate for the lifetime of the individual, or even beyond life. Both registration statutes and GPS tracking requirements have typically set forth lengthy compliance periods, ranging from ten years to life. Other online indexes may remain until deliberately taken down or altered. The hoarding of biometric or other such data is at present largely unregulated, and thus such information could arguably be kept in perpetuity. DNA statutes authorize indefinite retention of the expressed genetic profile, and even the biological sample containing the entire genome of the person. Indeed, there is no reason why the information need be purged even upon the death of the individual; rather, there is a strong incentive to keep it across successive generations (so that it may be used, for example, to conduct “familial searches” to find children or relatives who allegedly perpetrated a crime).

In sum, technology gives law enforcement the ability to control great numbers of persons, for a long period of time or even indefinitely, and usually at a cheap price.²¹³ Thus, it does not replicate the conditions of physical world, it alters them.

IV. A NEW LANGUAGE OF LIBERTY.

²¹¹ A number of states require tracked individuals to pay for their tracking, including Alabama, ALA. CODE § 15-20-26.1, Arkansas, ARK. CODE ANN. § 12-2-923, Georgia, GA. CODE ANN. § 42-1-14; Michigan, MICH. COMP. LAWS § 791.285, and South Carolina, S.C. ANN. § 23-3-540. The same is true of many SCRAM programs, *see Keeping Watch*, *supra* note X (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).

²¹² *See supra*.

²¹³ Corbett, *supra* note X, 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”).

“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...?”²¹⁴

Until recently, controlling dangerous persons required acquisition of control over their physical bodies. But in these modern times, the state is increasingly capable of using technology to create a virtual prison capable of regulating a person almost as comprehensively as the traditional kind. And, of course, it has every reason to do so, since the costs all around will be cheaper.

Presently, however, there is little to prevent the state from constituting this virtual prison not with lawfully adjudicated, individually culpable prisoners given determinate periods of sentencing or supervision, but rather with wholesale categories of individuals drawn broadly and indefinitely and without regard to any individualized findings. Rather than simply substitute for physical incapacitation, technological incapacitation will serve as a net into which increasingly greater numbers of persons are drawn. And rather than operate as an effective and efficient means of safeguarding persons from “dangerous” individuals, technology will become a crudely wielded tool by which segments of the population are stamped “dangerous” and subjected to different standards of privacy and liberty.

This Article attempts to identify several respects in which particular characteristics shared by technological regulations raise concerns not presently recognized in legal doctrine, in order to enrich the conversation about the potential harms wrought by such technologies. Although crafting a legal regime capable of creating finer distinctions between permissible and impermissible uses of surveillance technologies exceeds the scope of this Article, this section attempts to identify some general principles to consider as new technologies continue to undergo legal challenge.

First, it is essential that courts amplify the understanding of the range of interests that technological regulations can cognizably infringe. Corporeal harms serve as poor points of comparison for technological intrusions. Demands for an actualized, demonstrable injury overlook the very real injury incurred in being singled out for exposure to harm. In addition, the requirement that all harms emanate directly from the state ignores the role that the state can play in generating or facilitating harm by a third party. Thus, for example, it is not enough to require proof that the individual’s DNA sample will be misused by the government, when the harm is the very risk of misuse, and by any party. Nor would it be enough to claim that the taking of the DNA sample is the only moment of intrusion; rather, the retention and maintenance of the profile and biological material would constitute an ongoing incursion.

At the same time that the standard by which the harm is assessed is broadened, the standard by which the government’s need or determination to implement the technology should be narrowed. Rather than rely upon speculative assessments that a particular technology achieves a particular goal, courts should demand particular evidence both of the purpose of the technological intrusion and of its capacity to achieve that purpose. Thus, it would not be enough to say that GPS monitoring prevents crime; it would be necessary to specify, for example, what kinds of crime are prevented and at what rate of efficacy.

²¹⁴ *Olmstead v. United States*, 277 U.S. 438, 571 (1928) (Brandeis, J., dissenting).

Second, courts should require that there be both balance and nexus between the purpose of the act and its method of implementation. This inquiry would consider both the general question of balance and nexus between the technique and its implementation, as well as the individualized inquiry into the technique and its implementation against the particular individual. Thus, if the purpose of the registration acts is to alert the public to the fact of conviction, then that interest should be balanced against the potential harm (assessed as above) to the individual of widespread public dissemination. Moreover, in order to add the requirement that the individual provide current personal demographic information, the state would need to show a demonstrated interest in demanding such information.

The ultimate measure of a particular regulation's validity, both as a general matter and in a particular case, should vary according to the procedural safeguards that attend its use and the tightness of the nexus between its purpose and application. At one end of the spectrum would lie methods of surveillance that impose minimal harms and operate for short periods of time, against narrowly drawn classes of persons, with procedural safeguards that ensure that a particular individual both falls within the applicable class and will not suffer significant harm from that particular technique either alone or in combination with other lawful regulations. At the other end of the spectrum are techniques that impose significant burdens, operate indiscriminately and indefinitely, against broadly drawn classes of persons, with few procedural opportunities to redress misapplication, and in concert with other techniques impose oppressive conditions on individual liberty.

This kind of nuanced inquiry better balances the harms that technological regulations can impose against the desirability of using such regulations to prevent or control crime. Present doctrine, which places too much stock in an all-or-nothing determination that a particular technique is "regulatory" or "punitive," or infringes an expectation of privacy or does not, provides too crude of a test. For instance, there might be techniques that raise concerns when applied retroactively, and yet need not require full criminal process prior to implementation. Or a technology might be unjust when applied with little procedural protection for an indeterminate period, but fairly implemented with those protections for a shorter duration. Requiring courts to choose between classifying a technique as punitive (thereby accepting the most stringent procedural safeguards) versus regulatory (thereby granting carte blanche in its implementation), or finding a liberty interest or expectation of privacy versus not recognizing one, serves neither the interest of individual liberty nor the interest of public safety.

The foregoing aims only to sketch preliminarily some thoughts about the manner in which the implementation of technological restraints on dangerous persons might operate. What is clear is that, absent some amplified notion of what procedural safeguards ought to attend the use of such regulations, individual liberty will be seriously placed in jeopardy. This outline intends only to carve out some possible terrain between the elaborate structures of criminal process that most physical deprivations of liberty trigger, and the empty wasteland upon which technological regulations currently sit.

In undertaking this effort, I hope not only to improve the ways in which we view liberty and state power in a technological society, but also to ensure that, to the extent that technology segregates the "dangerous" from the rest of us, those classes are finely and accurately drawn. Otherwise, we may find our society coarsely segregated into two classes of citizenship. The elite will be those invisible to the public eye, and free from the worry of arbitrary suspicion and intrusion. The unlucky others, though nominally free, will in fact be heavily fettered by constant scrutiny. Most troubling, the likely denominator for classification -- contact or generalized

suspicion generated in the criminal justice system -- has been demonstrably and repeatedly shown to skew along racial, political, and socioeconomic lines.²¹⁵

Equally as troubling, the repercussions of these tools of surveillance amplify in this age of information. Some general label of dangerousness may matter less when it is restricted by person-to-person contact, but in a global society it can seriously inhibit freedom. More and more, individuals are constructed as compilations of abstract data in “digital dossiers.”²¹⁶ So labeled, it no longer is plausible to move towns or switch jobs, or to stop driving or cease going to the supermarket. Isolation, whether by the government official that always seems to pull over your car on the highway or by the employer who can find your entire history on the internet, may vastly impair the ability of an individual to get a job, find a residence, and live independently and freely. Unlike when the state imprisons an individual, and therefore assumes the obligation to provide him with some measure of shelter, sustenance, and protection from harm -- however poorly it performs these functions -- our fictional offender from above, who has trouble working or finding an apartment or even living without fear of random violence, will lack something that his incarcerated counterpart retains: the right to hold the state accountable for affirmatively providing for his shelter, livelihood, health, and safety.

CONCLUSION

Just twenty years ago, only six Supreme Court justices could agree that the Constitution countenanced the preventive detention of persons charged with probable cause of a narrow category of dangerous crimes, and found by a judge after an adversarial hearing to clearly and convincingly pose a danger to the community.²¹⁷ Today, eight justices agree that a statute requiring a person for the rest of his life to report to the government if he dyes his hair does not even invoke the Constitution’s protections at all. Judges around the country feel the same about requirements that individuals give biological samples for government storage and retention, or attach live tracking devices to human beings.

Justice Brandeis presciently urged long ago that the Constitution retain the “capacity of adaptation to a changing world.”²¹⁸ And just as new communication technologies forced Fourth Amendment doctrine to shift its focus to “people, not places,”²¹⁹ so too do new incapacitation technologies require renewed reckoning with our understandings of what it means to incapacitate.

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 it does, then it will be up to us to ensure that our ideals of liberty have kept pace with our innovations, and to release the vision of jail as the paradigmatic form of restraint. Otherwise, those ideals may themselves start to seem as old-fashioned as the prisons.

²¹⁵ See, e.g. Troy Duster, *Explaining Differential Trust in DNA Forensic Technology: Grounded Assessment or Inexplicable Paranoia?*, 34 J.L. Med. & Ethics 293 (2006) ; see also Jonathan Simon.

²¹⁶ Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083 (2002); see also Poster, *supra* note X, at 90 (“With databases, the individual is constituted in abstantia.”).

²¹⁷ *Salerno*, 481 U.S. 739 (noting flight risk also justifies detention).

²¹⁸ *Olmstead v. United States*, 277 U.S. 438, 473 (Brandeis, J., dissenting).

²¹⁹ *Katz v. United States*, 389 U.S. 347, 351 (1967).