Towards a Brighter Fourth Amendment: Privacy and Technological Change

Joshua S. Levy
NYU School of Law, joshlevy08@gmail.com

Follow this and additional works at: http://lsr.nellco.org/nyu_lewp

Part of the Law Enforcement and Corrections Commons, and the Science and Technology Commons

Recommended Citation
http://lsr.nellco.org/nyu_lewp/279

This Article is brought to you for free and open access by the New York University School of Law at NELLCO Legal Scholarship Repository. It has been accepted for inclusion in New York University Law and Economics Working Papers by an authorized administrator of NELLCO Legal Scholarship Repository. For more information, please contact tracythompson@nellco.org.
Towards a Brighter Fourth Amendment: Privacy and Technological Change

Joshua S. Levy*

Introduction

On November 13, 2010, John Tyner tried to fly from San Diego International Airport to South Dakota. Before he could board his flight, Transportation Security Administration (TSA) screeners instructed him to undergo a full body scan that renders naked, albeit grainy, images of passengers. Tyner refused. TSA screeners then insisted he face an “enhanced” pat down, which would include a “groin check.” Tyner again refused, crying “don’t touch my junk!” He never boarded his flight to South Dakota. TSA Director John Pistole has defended the full body scans and enhanced pat downs, arguing that they are necessary for national security and simply need to be better explained to the public.¹

Given the technological developments of the past few decades, it is unsurprising that the TSA expects complicity in serious invasions of privacy. Digital technology already affects “the way we shop, bank and go about our daily business.”² This has enabled private companies to track and aggregate credit card transactions, medical prescriptions, social networking postings and even real estate records.³ Over time, these technologies reduce the amount of privacy people subjectively experience in their daily lives, causing them to expect less privacy overall.⁴ Yet as the public outcry against enhanced airport screening shows, the government can go too far.⁵ Aside from viewing naked images of passengers, the government can track people by global

* B.A. 2008, University of Virginia (Highest Distinction); J.D. 2011, New York University School of Law (magna cum laude). I would like to thank Barry Friedman for his invaluable guidance throughout this research; without his help this Article would never have been written. I would also like to thank Katherine J. Strandburg for her insightful comments on an earlier draft of this Article.


position system (GPS),\textsuperscript{6} satellite technology\textsuperscript{7} or radio frequency identification,\textsuperscript{8} look into private residences with video surveillance\textsuperscript{9} and thermal imaging\textsuperscript{10} and even read personal emails.\textsuperscript{11}

The capacity of government surveillance “to spy on private conduct” has sparked an academic debate about whether courts or legislatures are better able to protect privacy in the face of new technologies.\textsuperscript{12} The academic consensus favors courts expanding Fourth Amendment protections against new government surveillance tools.\textsuperscript{13} A minority view contends that courts cannot keep pace with rapid technological change, so legislatures are better suited to protect privacy.\textsuperscript{14} However, statutory schemes can quickly become outdated, and legislatures are subject to lobbying by law enforcement interests.\textsuperscript{15} Since neither rulemaking institution is able to respond sufficiently rapidly to technological change, courts should take the “long view” of the Fourth Amendment by adopting bright line rules protecting core areas of privacy.\textsuperscript{16} This Article seeks to develop a framework of bright line Fourth Amendment rules that continue to provide privacy protection regardless of advancements in surveillance technology. Unlike specific constitutional or statutory privacy protections, which constantly lag and risk misunderstanding new surveillance technologies, bright line rules ensure that no body of government has to play ‘catch up.’ The bright line rules protect privacy regardless of the new technologies that law enforcement agencies adopt, ensuring that existing Fourth Amendment protections do not become increasingly vacuous. Given the extraordinary protective power of bright line rules, they should only be initially adopted for core areas of privacy that have always received heightened

\begin{footnotesize}
\begin{enumerate}
\item See MARK MONMONIER, SPYING WITH MAPS: SURVEILLANCE TECHNOLOGY AND THE FUTURE OF PRIVACY (2002).
\item See United States v. Mesa-Rincon, 911 F.2d 1433, 1437 (10th Cir. 1990).
\item See Sonia Arrison, New Anti-Terrorism Law Goes Too Far, S.D. UNION TRIB., Oct. 31, 2001, at B9 (“The law also expands Internet surveillance by making Carnivore, the controversial email wiretapping system official, even though there is a real danger that it over-collects information.”); COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, U.S. DEP’T OF JUSTICE, MANUAL ON SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS § III.B (2001), available at http://www.cybercrime.gov/sdsmanual2002.htm [hereinafter COMPUTER CRIME] (arguing that read e-mail stored on a server can be obtained with a subpoena and does not require a warrant).
\end{enumerate}
\end{footnotesize}
legal protection, namely, homes and human bodies. However, as the reach of surveillance technology grows and the social use of technology changes, they may need to be extended to new areas.

The Article is organized as follows. Part I demonstrates how technology decreases society’s privacy expectations and enables highly intrusive government surveillance. Part II discusses the academic debate surrounding the institutional capacities of courts, legislatures and law enforcement agencies to protect privacy. Part III argues that only bright line rules can adequately protect privacy against new technologies. It sets out bright line Fourth Amendment rules protecting homes and bodies that flow from longstanding legal principles as well as recent case law. It also defends the rules against possible legal and policy criticisms, and shows that they will induce the innovation and adoption of privacy protecting technologies.

I. Technology and Privacy

This Section shows how two technological trends serve to decrease privacy. First, the Section details how recent technological innovations, mostly digitalization and the internet, decrease society’s privacy expectations. Second, the Section analyzes new law enforcement technologies, such as data mining, thermal imaging, video surveillance, GPS and DNA typing, and their differential effects. This Section argues that the combination of these two trends magnifies the decrease in privacy. It defends this claim against those who argue that technology increases privacy and makes law enforcement surveillance less intrusive.

A. Privacy Expectations and Technological Change

The internet and digital recordkeeping have brought untold economic benefits to societies throughout the world, yet, as with all technologies, they are not without costs. While collecting and recording every webpage visit, credit card transaction and medical prescription enables more efficient commerce, it also removes any privacy or anonymity on the internet or in commercial dealings. Over time, such widespread, personalized data collection downwardly redefines privacy norms by diminishing the amount of privacy people subjectively experience in their daily lives. This process occurs gradually so that, at first, it seems to be “the inevitable price of progress,” but it then becomes “self-perpetuating.” For instance, employers often monitor employees’ e-mail. While these policies may provoke some initial opposition, once established they reshape privacy expectations to exclude some internet use and enable further “incremental encroachment[s],” such as monitoring which websites employees visit. The “internalization” by society of each successful encroachment—internet companies attempting to sell personal

17 See supra notes 2-4 and accompanying text.
18 See ROSEN, supra note 4, at 60-61.
19 Spencer, Reasonable Expectations, supra note 4, at 861.
20 See id. at 860-62.
21 Id. at 863.
information to third parties, media companies reporting lurid personal details and social networking and blogging sites—results in vast decreases in privacy expectations over time.

In this context, the free flow of information further diminishes privacy expectations. For instance, patients’ medical records are widely shared throughout the healthcare industry, mostly with those who have no medical need to access them. Large organizations also inadvertently disclose highly sensitive and personal material with alarming frequency. Accidental disclosures have ranged from credit reports to confidential medical information, and even children’s psychological records. These serious breaches of privacy are only among those acting in good faith. Criminals can hack business’ financial records or the Internal Revenue Service’s computers to engage in identify theft. As society adapts to this new, digitized world, it necessarily accepts that it does not have a “right to be let alone” in its commercial dealings, medical treatments or on the internet. So Scott McNealy, founder of Sun Microsystems, was speaking only partly in hyperbole when he declared: “You have zero privacy anyway. Get over it.”

Nonetheless, there are some who argue that technology increases society’s privacy expectations. They contend that technology such as cell phones and the internet enhance privacy by enabling individuals to communicate or shop from within the home instead of in public. This reasoning is flawed because it fails to appreciate the differences between physical and digital communications. While a person can theoretically be constantly followed in public,
digital communications can be cheaply tracked, stored and consolidated in databases.\textsuperscript{35} As a result, instead of increasing privacy by bringing previously public activities into the home, new technologies decrease communicative privacy even within the home.\textsuperscript{36}

B. Privacy and Law Enforcement Surveillance Technology

Since the Supreme Court found that citizens’ conversations in public telephone booths are protected from warrantless government wiretapping in \textit{Katz v. United States},\textsuperscript{37} the constitutional limits of government surveillance have depended on societal privacy expectations. Specifically, the Fourth Amendment protects areas and activities where a defendant has an actual or subjective expectation of privacy “that society is prepared to recognize as ‘reasonable.’”\textsuperscript{38} Therefore, as technology, facilitated by both the private sector and government, lowers the amount of privacy people come to expect in their daily lives, the Fourth Amendment provides increasingly less protection.\textsuperscript{39} In this “gray area of unsettled expectations,” law enforcement agencies have exercised their surveillance powers to the constitutional limit.\textsuperscript{40}

Consider digitized recordkeeping. Since private companies collect and store large quantities of personal data,\textsuperscript{41} police and prosecutors can freely access it during criminal investigations without first obtaining a warrant.\textsuperscript{42} Building on this concept, law enforcement agencies have developed their own databases, such as sex offender registries and no-fly lists, to track suspects and deny them certain liberties.\textsuperscript{43} Despite their lack of procedural safeguards,\textsuperscript{44} courts have


\textsuperscript{36} See, e.g., Laurie Thomas Lee, \textit{Can Police Track Your Wireless Calls? Call Location Information and Privacy Law}, 21 CARDOZO ARTS & ENT. L.J. 381, 382 (2003) (arguing that new technologies such as cell phones have become the consumer’s “ankle bracelet” because they enable government to monitor citizens’ movements more easily).

\textsuperscript{37} 389 U.S. 347, 353 (1967).

\textsuperscript{38} \textit{Id.} at 361 (Harlan, J., concurring).

\textsuperscript{39} See supra notes 17-31 and accompanying text.

\textsuperscript{40} Spencer, \textit{Reasonable Expectations}, supra note 4, at 844.

\textsuperscript{41} See supra notes 2-4 and accompanying text.


\textsuperscript{43} See Erin Murphy, \textit{Paradigms of Restraint}, 57 DUKE L.J. 1321, 1336-40 (2008) [hereinafter Murphy, Paradigms].
uniformly upheld these databases. Not content to simply mine data, police have warrantlessly tracked individuals using video surveillance, GPS tracking devices, satellite technology, radio frequency identification, facial recognition software and iris scanning technology. Police have even used thermal imaging devices to look into homes. Some of these surveillance technologies can reveal startlingly personal information that people do not wish exposed to the public. Society’s loss of privacy has even extended to the genetic level, as the government develops DNA databases to catch not only the individuals in the database, but their relatives as well. Thus, law enforcement surveillance reinforces the downward effect of technology on privacy.

There is a minority of commentators who think that improved police surveillance technology will increase privacy. They make two main arguments. First, they point out that some technology, most notably encryption, directly increases privacy. Second, they argue that technology enables more targeted and focused searches, especially in the digital realm, resulting

44 See Laura K. Donohue, Anglo-America Privacy and Surveillance, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1136-37 (2006) (discussing the federal government’s creation of lists forbidding or limiting airline travel by certain individuals but without developing any procedural safeguards to ensure the accuracy of the lists).
46 See, e.g., Cara Buckley, New York Plans Veil for Downtown, N.Y. TIMES, July 9, 2007, at A1 (describing a New York City plan to install cameras linked to license plate databases that could trigger barriers if cars banned from the area passed nearby).
47 See, e.g., People v. Johnson, 43 Cal. Rptr. 3d 587, 597-98 (Cal. Ct. App. 2006) (discussing potential uses of facial recognition software); see also David Lamb, One Last City is Scanning Faces in the Crowd, L.A. TIMES, Sept. 29, 2003, at A10 (reporting that Virginia Beach continues to use facial-recognition systems to scan for terrorists, felons with outstanding warrants and missing children).
49 See Kyllo v. United States, 533 U.S. 27, 38 (2001) (“The Agema Thermovision 210 might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider ‘intimate’…”).
50 See, e.g., United States v. Mesa-Rincon, 911 F.2d 1433, 1437 (10th Cir. 1990) (noting the intrusiveness of video surveillance “that recorded a person masturbating before the hidden camera”).
51 See Murphy, Paradigms, supra note 43, 1329-32 & n.36.
53 See Kerr, supra note 55, at 529-31 (noting that encryption “extends far greater privacy protection than the warrant requirement of the Fourth Amendment ever could” due to the near impossibility of decrypting complicated encryption keys); Simmons, Broader Perspectives, supra note 32, at 546-47.
in less intrusion. Both these argument miss the fact that technologies such as encryption and data mining are responses to privacy intrusions. Encryption is only necessary because hackers and government surveillance are capable of reading files and emails. Similarly, police have only developed targeted email search surveillance after initially using more intrusive searches. Therefore, privacy-enhancing technology will always lag behind privacy-intruding surveillance technology, leaving society’s reasonable expectations of privacy unprotected against government surveillance.

Such “response” technology will never fully “catch-up” to surveillance technology, in part due to economic incentives. In the private sector, technology companies regularly worry about “backlash” from consumers if they collect or utilize private data too aggressively. In numerous instances, companies have curtailed or even withdrawn innovations that upset their customers. While the private sector faces financial incentives to protect some measure of privacy, law enforcement faces no such incentives, since most surveillance activities are not visible to the public. As a result, law enforcement is capable of going too far and violating the very rights the Fourth Amendment was designed to protect.

II. Courts, Legislatures, Law Enforcement and Bright Line Rules

This Section explores the academic debate surrounding the institutional competences of courts and legislatures to make Fourth Amendment rules for new technologies. It adds to the debate by including academic work from economists and political scientists concerning public choice theory and the legislative process. The Section argues that neither courts nor legislatures can adequately keep pace with technological change. It then examines internal privacy regulation by law enforcement, a topic largely ignored by the mainstream academic debate. It argues that law enforcement agencies are the only bodies of government capable of protecting privacy at the same pace as technological advancement, since they are the ones adopting the new technologies. However, this Section concludes that law enforcement agencies have no incentive to protect privacy, so trusting them is tantamount to leaving the fox guarding the henhouse.

57 See Simmons, Broader Perspectives, supra note 32, at 563-64 (“[T]he government can use software that can sift through and copy only those messages with incriminating words or specific names, thus letting the innocent ones pass through without any human ever reading them.”); Kerr, Big Brother, supra note 55, at 648-54.
58 See Kerr, supra note 55, at 527.
59 See Kerr, Big Brother, supra note 55, at 651-52.
60 Simmons, Broader Perspectives, supra note 32, at 545.
62 See, e.g., Geoffrey A. Fowler & Emily Steel, Facebook Says User Data Sold to Broker, WALL ST. J., Oct. 31, 2010, at B3 (reporting Facebook’s swift response to a violation of its privacy policy by a data broker); A Special Report on Smart Systems: Sensors and Sensibilities, ECONOMIST, Nov. 6, 2010, at 15-16 (reporting that Pacific Gas & Electric withdrew “smart” utility meters after customer complaints of higher power bills).
64 See Stuntz, Pathological, supra note 15, at 533-34 n.118 (2001); Solove, Digital Dossiers, supra note 35, at 1158.
65 See, e.g., Simmons, Broader Perspective, supra note 32, 541-42.
A. Courts versus Legislatures

Most Fourth Amendment scholars favor an activist judiciary in Fourth Amendment law because, they argue, criminal suspects and defendants are disliked minorities who will never be able to vote themselves proper protections in a democracy.66 As a result, legislatures face little or no political pressure to protect the rights of the criminally accused, but face strong political pressure to ensure crime control.67 Therefore, the politically insulated courts must step in to protect crime suspects.68 Yet, commentators note with horror, the Fourth Amendment provides no protection to bank records,69 phone records70 or email,71 and does not protect against closed circuit television systems,72 data mining of transactional records,73 electronic databases74 or facial recognition software.75 They argue that courts should extend Fourth Amendment protection to new technologies, such as email and public video surveillance.76 Some even want to extend Fourth Amendment protection to anonymity and friendship.77 In short, they argue that “courts should be very active in shaping new criminal procedure rules,”78 lest they “abdicate all responsibility for the rules of high-technology surveillance.”79

66 See, e.g., Donald A. Dripps, Criminal Procedure, Footnote Four, and the Theory of Public Choice; or, Why Don’t Legislatures Give a Damn About the Rights of the Accused?, 44 SYRACUSE L. REV. 1079, 1079-81 (1993) [hereinafter Dripps, Criminal Procedure] (arguing that legislatures are “indifferent or hostile to the rights of the accused” to secure re-election in majoritarian politics); see generally JOHN HART ELY, DEMOCRACY AND DISTRUST 172-73 (1980) (arguing for a democratic process-based approach to Fourth Amendment law as a prophylactic against unequal treatment); United States v. Carolene Products Co., 304 U.S. 144, 153 n.4 (1938) (“[P]rejudice against discrete and insular minorities may be a special condition, which tends seriously to curtail the operation of those political processes ordinarily to be relied upon to protect minorities, and which may call for a correspondingly more searching judicial inquiry.”).
67 See, e.g., Dripps, Criminal Procedure, supra note 66, at 1079-81.
68 See 1 LAFAVE ET AL., CRIMINAL PROCEDURE § 2.01 (2d ed. 1999) (arguing that the courts are well-equipped to regulate criminal procedure rules because they understand the criminal process and are not subject to political pressures to deny basic liberties); ELY, supra note 66 at 172-73.
71 See Solove, Reconstructing, supra note 15, at 1281; Solove, Coexistence, supra note 6, at 769; Kerr, New Technologies, supra note 14, at 869 (“[N]o Article III court at any level has decided whether an Internet user has a reasonable expectation of privacy in their [sic] e-mails stored with an Internet service provider; whether encryption creates a reasonable expectation of privacy; or what the Fourth Amendment implications of . . . Internet surveillance . . . might be.”); but see United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that “a subscriber enjoys a reasonable expectation of privacy in the contents of emails”).
72 See SLOBOGIN, PRIVACY AT RISK, supra note 42, at 89-90.
73 See id. at 139-80.
74 See Murphy, Paradigms, supra note 43, at 1336-40.
75 See Simmons, Technology-Enhanced, supra note 55, at 729-30 & n.58.
76 See, e.g., Mulligan, Reasonable Expectations, supra note 13, 1586-93; Slobogin, Camera, supra note 13 (arguing courts should interpret the Fourth Amendment to recognize the right to be free from video surveillance in public, and suggesting courts should set up guidelines for the use of such surveillance).
78 Solove, Coexistence, supra note 6, at 776.
On the other side of the spectrum, Professor Orin Kerr has led a lonely fight to defend the legal status quo. He argues that courts lack the institutional competence to protect privacy against new technologies for three main reasons. First, courts do not sufficiently understand new technologies due to their lack of technological expertise and the limited records presented by the parties. Second, judicially created rules cannot adapt to technological change and, as a result, quickly become outdated. Third, legislatures value privacy highly since, unlike the rights of an individual criminal suspect, it is a public good. As a result, they have passed many comprehensive, flexible statutes protecting privacy, such as the Electronic Privacy Communications Act (ECPA) and the Computer Fraud and Abuse Act. Moreover, legislators can consult with “technologists” and “technology-savvy advisors” in an “open and interactive” process while crafting rules, and “can update them frequently as technology changes.” By engaging in proactive instead of reactive rulemaking, Kerr argues, legislatures provide both more certainty and flexibility than courts.

Mainstream commentators are quick to point out that certainty and flexibility inherently conflict. They contend that statutes are no better at keeping up with technological change, noting the many privacy gaps in existing statutory schemes, such as cell phones, video surveillance and emails on third party internet service providers (ISPs). As political scientists demonstrate, this necessarily flows from the structure of the legislative process. In instances of divided government, it is unlikely that the House, Senate and President will able to agree on legislative priorities. Moreover, federal law enforcement agencies are part of the executive branch, so legislation to curtail their powers will likely draw a presidential veto. Even in

80 See Kerr, New Technologies, supra note 14, at 875-82; Kerr, Congress, supra note 14, at 785-86.
81 See Kerr, New Technologies, supra note 14, at 859 (Judicially created rules . . . cannot change quickly and cannot test various regulatory approaches. As a result, judicially created rules regulating government investigations tend to become quickly outdated or uncertain as technology changes.).
82 The key aspects of public goods are that they are non-excludable in access and non-rival in consumption. Privacy is a public good since my enjoying privacy in no way diminishes your ability to enjoy your privacy. See, e.g., HUGH GRAVELLE & RAY REES, MICROECONOMICS (3d ed. 2004) (“The defining characteristic of a public good is that consumption of it by one individual does not actually or potentially reduce the amount available to be consumed by another individual.”).
83 See Kerr, New Technologies, supra note 14, at 850-52; Solove, Coexistence, supra note 6, at 753-60.
86 Kerr, Congress, supra note 14, at 784; Kerr, New Technologies, supra note 14, at 807.
87 See Kerr, New Technologies, supra note 14, at 806, 859-60, 872.
88 See Solove, Coexistence, supra note 6, at 767.
89 See id. at 763, 769; Solove, Reconstructing, supra note 15, at 1281; COMPUTER CRIME, supra note 11, at § III.B.
instances of unified government, a filibuster by the minority party in the Senate,\textsuperscript{92} or an ideological divide within a party, can result in legislative gridlock as well.\textsuperscript{93} It is unsurprising, then, that in the past 20 years between 78 and 97 percent of bills “died in committee” each year.\textsuperscript{94} In 1993, a year of unified government, the House passed just 2 percent of all bills introduced.\textsuperscript{95} Given such legislative torpidity, it is unlikely that privacy statutes will be able to keep up with the rapid pace of technological change.

Scholars also argue that even when legislatures do pass criminal procedure statutes, these laws will not adequately protect privacy, since legislators are susceptible to political lobbying by law enforcement interests for greater surveillance powers.\textsuperscript{96} Public choice theory posits that legislators act to redistribute resources from politically ineffective groups (which are typically large and heterogeneous) to politically effective groups (typically small and homogenous) in order to secure support for reelection.\textsuperscript{97} Whereas privacy is a public good that will be enjoyed by the dispersed population,\textsuperscript{98} law enforcement has a “concentrated interest” in reducing its regulation and increasing its resources.\textsuperscript{99} In this “classic public choice problem,” the concentrated law enforcement agency is able to marshal resources to lobby legislators for more power at the expense of the public’s privacy, because of its lower organization costs and more concentrated benefits.\textsuperscript{100} Kerr criticizes this view, claiming public choice theory does not apply to criminal procedure since there are no economic “rents” for law enforcement interests to capture.\textsuperscript{101} Yet this conception of economic rents is far too cramped. Larger budgets and more administrative power are private gains to law enforcement that do not flow to the rest of the society.\textsuperscript{102} Placing orders with companies that produce surveillance equipment can also help police secure lucrative private sector employment later.\textsuperscript{103} Moreover, security is also a public


\textsuperscript{93} See Sarah A. Binder, \textit{The Dynamics of Legislative Gridlock: 1947-96}, 93 AM. POL. SCI. REV. 519, 519 (Sept. 1999) (arguing that “intrabranch conflict—perhaps more than interbranch rivalry—is critical in shaping deadlock in American politics”).

\textsuperscript{94} CONGRESSIONAL BILLS PROJECT, TRENDS IN BILL SPONSORSHIP ACTIVITY (Univ. of Wash. 2004), http://www.congressionalbills.org/trends.html.

\textsuperscript{95} See id.


\textsuperscript{97} See MANCUR OLSON, \textit{THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS} (1965) (explaining advantages that concentrated interests, such as regulated industries, have over diffuse interests in the political process); see generally George Stigler, \textit{The Theory of Economic Regulation}, 2 BELL J. ECON. & MGMT. SCI. 1 (1971); Gordon Tullock, \textit{Some Problems of Majority Voting}, 67 J. POL. ECON. 571 (1959).


\textsuperscript{100} Id. See also Peter P. Swire, \textit{The System of Foreign Intelligence Surveillance Law}, 72 GEO. WASH. L. REV. 1306 (2004) (arguing that the expertise and institutional staffing of federal law enforcement enable strong lobbying against law enforcement regulations).


\textsuperscript{102} See Stuntz, \textit{Pathological}, supra note 15, at 534 (2001) (“If police and prosecutors want some new criminal prohibition, they likely want it because it would advance their goals.”).

good, so Kerr concedes that law enforcement can argue for privacy reductions with “myopic claims of the public interest in solving crimes . . . .”104 As a result, law enforcement interests are often highly influential among legislators.105 Perhaps the best evidence of law enforcement lobbying is in the federal privacy statutes themselves: they nearly all lack exclusionary rules, which, as even Kerr admits, renders them unable to deter privacy violations by law enforcement.106

Lastly, although commentators claim courts can use experts and amici briefs to understand new technologies,107 they are more persuasive when criticizing legislatures than defending courts.108 The oral arguments in City of Ontario v. Quon,109 a recent Fourth Amendment decision by the Supreme Court, provide an excellent example.110 Chief Justice Roberts began the judicial confusion by wondering, “[W]hat is the difference between a pager and e-mail?”111 He, along with Justice Kennedy, then admitted that they thought simultaneous text messages might jam one another.112 Later, Justice Scalia and Chief Justice Roberts expressed astonishment that text messages travel through communications companies and not directly between mobile devices.113 This led Justice Scalia to wonder if text messages were printable.114 Justice Alito entered the fray shortly thereafter by asking whether text messages can be deleted.115 This question was perhaps more embarrassing for the lawyer who did not know the answer.116 Rather than produce a clear winner, the ongoing academic debate demonstrates the inability of both courts and legislatures to adequately protect privacy from constantly improving government surveillance.

B. Law Enforcement and Privacy Regulation

104 Kerr, New Technologies, supra note 14, at 885.
105 See Dripps, Criminal Procedure, supra note 66, at 1079-81 (1993); Kerr, New Technologies, supra note 14, at 885; Stuntz, Pathological, supra note 15, at 534.
106 See Solove, Coexistence, supra note 6, at 763 (“[T]here is no exclusionary rule to protect e-mail under the Wiretap Act, and the Stored Communications Act and Pen Register Act both lack an exclusionary rule.”); Orin S. Kerr, Lifting the “Fog” of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law, 54 HASTINGS L.J. 805, 807 (2003) (“Congress should restructure the remedies scheme of Internet surveillance law by adding a statutory suppression remedy for violations of the Internet surveillance statutes.”).
107 See Solove, Coexistence, supra note 6, at 772.
108 See Kerr, New Technologies, supra note 14, at 878-81 (describing criminal procedure cases where courts misunderstood technology, causing them to reach the wrong result); Kerr, Congress, supra note 14, at 785-86 (same).
109 130 S. Ct. 2619 (2010).
110 It is worth noting that Quon is not a traditional Fourth Amendment case. Rather, it is a civil suit under both § 1983 and the Stored Communications Act. See id. at 2622. However, since much of the analysis concerns the plaintiff’s reasonable expectations of privacy, I will refer to it simply as a Fourth Amendment case.
112 See id. at 44.
113 See id. at 48-50 (“I thought, you know, you push a button; it goes right to the other thing.”).
114 See id. at 49 (“Can you print these things out? Could Quon print these -- these spicy conservations out and circulate them among his buddies?”).
115 See id. at 51.
116 See id. at 53 (“Honestly I’m not -- that’s not in the record, and the -- how that pager works as far as deleting, I couldn’t be certain that it would be deleted forever.”).
Largely ignored by the academic debate is law enforcement agencies themselves. Unlike courts and legislatures, law enforcement agencies will be able to understand and keep up with new surveillance technologies, since they often design them in-house and keep the underlying code secret. As a result, new surveillance technologies can be regulated by internal police guidelines the moment they are put into practice. These guidelines can be updated in response to changing technology or uses, as well as codified into formal regulations. Unlike courts and legislatures, law enforcement agencies can adequately protect privacy in the face of changing technology and improving surveillance.

But why would they? While privacy is a public good enjoyed by the diffuse public, law enforcement agencies are primarily interested in seeking prosecutions and, more importantly, convictions. This is surely easier with advanced surveillance technology. Developing or procuring new technologies can also enable police and prosecutors to obtain bigger budgets, or secure lucrative private sector employment. While elected District Attorneys may face some political pressure to protect privacy interests, this is likely to be limited since much law enforcement activity is not visible to the public, the public wants convictions and most law enforcement officers are not elected. Although federal law enforcement agencies, most notably the FBI, have adopted some privacy regulations, they have only done so in the wake of highly publicized scandals with intense public pressure. Moreover, most federal law

121 See Kerr, New Technologies, supra note 14, at 884-85.
122 See Stuntz, Pathological, supra note 15, at 534 (arguing that law enforcement agencies wish to “prosecute the range of cases” and “win the cases they bring”).
123 See id.
124 See e.g., Lipton, Antiterror, supra note 103.
125 See Stuntz, Pathological, supra note 15, at 533-35 & n.118.
127 See Intelligence Activities and the Rights of Americans (Vol. 2), Final Report of the Select Committee to Study Government Operations with Respect to Intelligence Activities, 5-15 (Apr. 26, 1976) (reporting extensive abuses by the FBI’s COINTELPRO “to ‘disrupt’ groups and ‘neutralize’ individuals deemed to be threats to domestic security including civil rights groups and leaders).
enforcement activity is not visible to the public, and the vast majority of policing is conducted by state and local authorities who face political pressure to get convictions. Thus, trusting law enforcement agencies to hold the line on privacy protection is to give the wolf the keys to the henhouse. It is a cruel twist of irony that the bodies of government best able to act proactively and rapidly in response to surveillance technology have little incentive to do so.

III. Bright Line Rules

This Section argues that, given the institutional limitations of government, bright line Fourth Amendment rules are the only way to adequately protect privacy against new technologies. It then sets out rules protecting homes and the human body as core areas of privacy that have received longstanding legal protection. It concludes by analyzing the policy implications of these rules and their impacts on technological innovation.

A. Bright Line Rules and Technology

For decades, legal thinkers have debated the merits of rules versus standards in the law. Although Fourth Amendment law has traditionally relied on a totality-of-the-circumstances approach, lately it has taken a formalist turn. The reasons for this are threefold: certainty, scarce judicial resources and technology. It is indisputable that bright line legal rules provide great certainty to those regulated. In the Fourth Amendment context, such rules enable police to know precisely how far they can intrude while conducting an investigation and, importantly,

---

128 See Stuntz, Pathological, supra note 15, at 544 & n.153 (“[F]ederal prosecutions are less than five percent of total prosecutions.”).
131 See, e.g., Thornton v. United States, 541 U.S. 615, 616 (2004) (noting the “need for a clear rule, readily understood by police officers”); Atwater v. City of Lago Vista, 532 U.S. 318, 347 (2001) (“[W]e have traditionally recognized that a responsible Fourth Amendment balance is not well served by standards requiring sensitive, case-by-case determinations of government need, lest every discretionary judgment in the field be converted into an occasion for constitutional review.”).
where they cannot intrude.\textsuperscript{133} Clearly delineated rules can also prevent the demoralization of police and prosecutors, since evidence will not be suppressed due to Fourth Amendment standards decided \textit{post hoc};\textsuperscript{134} improved morale may well result in better police protection.\textsuperscript{135} Additionally, since the Warren Court incorporated the exclusionary rule against the states,\textsuperscript{136} courts have been inundated with Fourth Amendment cases.\textsuperscript{137} Legal rules can be an efficient way to quickly adjudicate Fourth Amendment issues in the face of scarce judicial resources.\textsuperscript{138} Finally, and most importantly for purposes of this Article, since new technologies can intrude on citizens’ privacy,\textsuperscript{139} bright line rules can limit the “power of technology to shrink the realm of guaranteed privacy.”\textsuperscript{140}

Despite their advantages, bright line rules entail significant legitimacy costs. First and foremost they are inherently inflexible, which can lead courts to incorrect results in particular cases.\textsuperscript{141} Incorrect or unjust results risk severely damaging the institutional credibility of the judiciary.\textsuperscript{142} Second, bright line rulemaking is legislative in nature and, therefore, risks damaging the Court’s legitimacy.\textsuperscript{143} In order to ameliorate these costs, courts should only engage in bright line rulemaking for uncontroversial areas that have traditionally received the highest privacy protections. “[T]he Court has given weight to such factors as the intention of the Framers of the Fourth Amendment, the uses to which the individual has put a location, and our

\begin{itemize}
  \item \textsuperscript{136}See Mapp v. Ohio, 367 U.S. 643 (1961).
  \item \textsuperscript{137}See Donald A. Dripps, \textit{The Fourth Amendment and the Fallacy of Composition: Determinacy Versus Legitimacy in a Regime of Bright-Line Rules}, 74 MISS. L.J. 341, 349-350 (2005) (“[T]he sheer scale of activity regulated by Fourth Amendment jurisprudence grew overnight by, roughly speaking, an order of magnitude.”); Peter F. Nardulli, \textit{The Societal Cost of the Exclusionary Rule: An Empirical Assessment}, 1983 AM. BAR. FOUND. RES. J. 595, 595-96 (finding that motions to suppress illegally seized physical evidence are filed in 5 percent of criminals cases and that defendants win 17 percent of these motions).
  \item \textsuperscript{139}See \textit{Kyllo}, 533 U.S. at 33-34 (“It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.”); see also supra notes 17-65 and accompanying text.
  \item \textsuperscript{140}\textit{Kyllo}, 533 U.S. at 34. See generally Anthony Amsterdam, \textit{Perspectives on the Fourth Amendment}, 58 MINN. L. REV. 349, 399 (1974) (arguing that the Framers intended the Fourth Amendment to grow over time).
  \item \textsuperscript{142}See, e.g., Christopher E. Smith, \textit{Bright-Line Rules and the Supreme Court: The Tension Between Clarity in Legal Doctrine and Justices’ Policy Preferences}, 16 OHIO N.U. L. REV. 119, 123 (1989) (“[T]he Supreme Court is still confronted with cases in which the maintenance of bright line rules conflicts with desirable policies or simple justice.”).
  \item \textsuperscript{143}See \textit{Kyllo}, 533 U.S. at 51 (Stevens, J., dissenting) (“It would be far wiser to give legislators an unimpeded opportunity to grapple with these emerging issuers rather than to shackles them with prematurely devised constitutional constraints.”); Dripps, supra note 137, at 352-54.
\end{itemize}
Towards a Brighter Fourth Amendment: Privacy and Technological Change

societal understanding that certain areas deserve the most scrupulous protection from government invasion.” In addition to limiting themselves to traditional areas of privacy protection, courts should only adopt bright line rules for activities that are recurring in nature, clearly understandable and affected by rapid technological changes. The event must be recurring since developing rules entails upfront costs of scarce judicial resources, whereas standards incur costs in enforcement; so efficiency favors only promulgating rules for frequent, recurring events. Judges will only be able to develop such rules if they can fully understand the activities at issue. Yet, given the legitimacy costs of bright line rules, the Court should only invoke this power when “[t]o withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment,” leaving citizens “at the mercy of advancing technology.” In areas of rapid technological change, the inability (or unwillingness) of other areas of government to adequately protect privacy mollify any legitimacy costs rulemaking might entail.

Although technological change may diminish privacy in all areas of life, courts should proceed with caution given the institutional and legitimacy limitations they face. While this may not provide protection from all areas into which the government may intrude, this Article seeks to set out a framework of bright line Fourth Amendment rules for core areas of privacy that can later be expanded. There are two areas that satisfy all these requirements: homes and human bodies. The text of the Fourth Amendment explicitly refers to both “houses” and “persons,” and searches involving homes and bodies are mainstays of criminal investigations and have been for years. Since all judges have bodies and live somewhere, they surely understand the privacy and security interests at stake. These interests are constantly being changed as police develop technology that can see into homes and even bodies. Therefore, courts must proactively protect both homes and bodies with bright line rules to ensure that their traditional Fourth Amendment protections do not become increasingly empty due to technological advancements.

Conversely, other potential candidates for bright line protection, most notably automobiles and email, do not satisfy all the necessary criteria. Although automobile searches are recurring

---

145 See, Kaplow, supra note 138, at 572, 577.
146 See Kerr, New Technologies, supra note 14, at 863-64.
147 Kyllo, 533 U.S. at 28.
148 See supra notes 66-128 and accompanying text.
149 See supra notes 17-65 and accompanying text.
150 U.S. CONST. amend. IV.
151 See, e.g., Mapp, 367 U.S. 643 (requiring a search warrant for police to enter and search a house); Kyllo, 533 U.S. 28 (requiring a search warrant for police to use a thermal imaging device on a house); Schmerber v. California, 384 U.S. 757 (1966) (using a balancing test to determine whether the Fourth Amendment applies to blood tests); Winston v. Lee, 470 U.S. 753 (1985) (using a heightened balancing test to determine whether the Fourth Amendment applies to surgeries).
153 See supra note 1 and accompanying text.
Towards a Brighter Fourth Amendment: Privacy and Technological Change

Josh Levy

and easily understandable, a rule protecting the interior of a car breaks from decades of case law. The Supreme Court has consistently held that a police officer with probable cause has nearly free reign to search a car and all containers therein under the “automobile exception” to the warrant requirement, so long as the car is mobile. Additionally, the technology required to search the interior of a car has not significantly changed in decades. However, recent advances in GPS technology enable police to electronically track the location of automobiles. This has provoked a circuit split on whether around the clock GPS surveillance of automobiles triggers Fourth Amendment protection. Since the legal status of GPS tracking is currently in flux and automobiles have traditionally received very little Fourth Amendment protection, the exterior location of an automobile is not yet deserving of bright line rule protection. Nonetheless, it is a very promising future candidate.

Like automobile searches email is recurring in nature, but, unlike automobiles, it is subject to rapid technological change. It can also be analogized to paper mail, whose contents have received strong Fourth Amendment protection for centuries and can be considered “effects” within the text of the Fourth Amendment. Nonetheless, in cases involving ISPs, servers and encryption, “judges struggle to understand even the basic facts of such technologies . . . .” For example, a federal district court ordered a police officer to be physically present to supervise a search of an ISP, erroneously thinking this would protect privacy despite the officer’s lack of technological expertise. Similarly, in the first case to apply the Fourth Amendment to email, the Court of Appeals for the Armed Forces drew a distinction between America Online (AOL) email and “Internet” email, as if AOL were not part of the internet. Judges make such mistakes because they analogize from the physical to the digital, forcing them to rely on


155 See United States v. Chadwick, 433 U.S. 1 (1977) (holding that items in the trunk of a non-moving car are protected by the Fourth Amendment).

156 In light of this, the Court has developed a “remarkably detailed set of rules that govern every stage of traffic stops.” Kerr, New Technologies, supra note 14, at 862-63.


158 Compare United States v. Maynard, 615 F.3d 544, 555-68 (D.C. Cir. 2010) (finding that twenty-four hour GPS surveillance for four weeks is a search within the meaning of the Fourth Amendment), with United States v. Pineda-Morena, 591 F.3d 1212, 1216 (9th Cir. 2010) (finding that using a GPS tracking device to monitor movements for a prolonged period of time is not a search within the meaning of the Fourth Amendment), and United States v. Marquez, 605 F.3d 604, 609-10 (8th Cir. 2010) (same), and United States v. Garcia, 474 F.3d 994, 996-97 (7th Cir. 2007) (same).

159 See supra notes 17-31 and accompanying text.

160 See Ex parte Jackson, 96 U.S. 727, 733 (1877).


162 See Kerr, New Technologies, supra note 14, at 875-76.


164 See Kerr, Congress, supra note 14, at 785-86 (describing United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996)).
Towards a Brighter Fourth Amendment: Privacy and Technological Change

Josh Levy

“questionable metaphors to aid their comprehension,” without knowing “whether those metaphors are accurate, or whether the facts before them are typical or atypical . . . .”

In spite of these institutional constraints, one circuit has granted Fourth Amendment protection to email. As the social importance of email and other electronic communications grow, courts will likely have to extend Fourth Amendment protections to them. In the meantime, however, courts should avoid creating bright line rules, since judges’ failure to understand the relevant technologies risks creating a mismatch between privacy values and the effects of the resulting rules.

Admittedly, such judicial caution does not immediately solve many of the problems discussed above. Nonetheless, this Article seeks to create a framework for bright line Fourth Amendment rules and establish criteria for future expansion. While the strictness of bright line rules is their great strength in protecting privacy, courts should only engage in such rulemaking out of necessity. By adopting bright line Fourth Amendment rules for areas that most clearly deserve constitutional protection, courts can shape the contours of such rules and cement the bright line rule approach before expanding it to new areas as technological change and social use require. In the meantime, the Court should only adopt bright line rules protecting homes and bodies—core areas of privacy—come what may.

B. Bright Line Rule for Homes

This Subsection traces the longstanding importance and special legal protections granted to residences in common law, statutes and constitutional law as well as recent Fourth Amendment case law. It argues that the legal protections granted to homes flow from personhood interests in the home, so the Fourth Amendment can specially protect homes without violating the principle that “the Fourth Amendment protects people, not places.” It then sets out the details of the bright line rule with a limited plain view exception, and defends it against criticisms of underinclusiveness and overinclusiveness. This Subsection argues that the bright line rule will spur the innovation and adoption of new technologies that will enable thorough police investigations while protecting the privacy of the home.

1. Homes and the Law

165 Kerr, New Technologies, supra note 14, at 875-76.
166 See United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that “a subscriber enjoys a reasonable expectation of privacy in the contents of emails”).
167 See, e.g., Katherine J. Strandburg, Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change, 70 MD. L. REV. (forthcoming 2011) (manuscript at 26-27, on file with author) (analogizing from telephone wiretaps in Katz to email based on social use).
169 See supra notes 17-65 and accompanying text.
170 See supra notes 129-48 and accompanying text.
171 See Strandburg, supra note 167.
Virtually all areas of American law provide special protections in the home. Common law tort doctrine subjects accidents within the home to different liability standards than those that occur elsewhere. Similarly, contract law requires more stringent provisions for sales of real property than for other contracts. In substantive criminal law, many states have adopted “Castle Laws” that statutorily eliminate the duty to retreat for self-defense claims when attacked in the home. States have even granted homeowners special protections in debtor-creditor relations and foreclosure sales. Courts have extended the importance of the home to constitutional law as well. In Takings cases, the Supreme Court has treated even the smallest physical intrusions on a home as “perhaps the most serious form of invasion of an owner’s property interests.” Protection of the home is the sole reason for the Third Amendment. In the First Amendment context, the Court has recognized that “[a] special respect for individual liberty in the home has long been part of our culture and our law.” Accordingly, the Court has struck statutes prohibiting homeowners from displaying lawn signs and possessing obscenity in their homes, and upheld the rights of homeowners to prevent unwanted mail from entering their homes. The Alaska Supreme Court has even extended constitutional protection to the personal consumption of marijuana in the home.

The extra protections given to homes in all areas of the law have special significance in the Fourth Amendment context, where “the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion” is paramount. The Court has even extended such protections to places similar to homes. For instance, renters enjoy full Fourth Amendment protections, so long as the tenant complies with the rental contract. The Fourth Amendment provision for “going armed about the body” in the eighteenth century served to protect the homes in the colonial era; today, the right to keep and bear arms is the right to keep and bear arms in the home.

---

174 See Restatement (Second) of Torts § 332 (2010).
175 See Restatement (Second) of Contracts § 127 (2010).
176 See, e.g., CAL. PENAL CODE § 198.5 (West 2010) (presuming that a person in her residence who attacks an intruder does so out of self-defense); see also Barros, Home, supra note 173, 260-62 (“[T]he law privileges certain acts of self-help made in defense of the home that would in another context be criminal or tortious.”).
177 See Barros, Home, supra note 173, at 283.
178 Loretto v. Teleprompter Manhattan CATV, 458 U.S. 419, 435-38 & n.16 (1982). The Court in Loretto found the installation of a rooftop cable box whose dimensions are 18” x 12” x 6” constituted a government Taking requiring “just compensation.” See id. at 421, 438 n.16.
179 See Barros, Home, supra note 173, at 256.
181 See id. at 45.
184 See Ravin v. State, 537 P.2d 494, 503-04 (Alaska 1975); see generally ETZIONI, LIMITS, supra note 26, at 196 (arguing that “contemporary American society largely exempts from scrutiny most acts that occur inside the home”).
186 See Kerr, New Technologies, supra note 14, at 809-15 (arguing that Fourth Amendment doctrine loosely tracks property law).
Amendment even protects houseguests,¹⁸⁸ hotel guests¹⁹⁰ and tents.¹⁹¹ The reason for these broad constitutional protections is the constancy and importance of the idea of a residence.¹⁹² The home is “the sacred retreat to which families repair for their privacy and their daily way of living.”¹⁹³ This flows directly from the personhood interest in the home.¹⁹⁴ People’s personal well-being is tightly bound up with the space of the home,¹⁹⁵ and any encroachments entail a “psychic toll” to personhood.¹⁹⁶ This is supported by both empirical studies and even evolutionary biology,¹⁹⁷ and is widely accepted among legal scholars.¹⁹⁸ Since the special protections granted to homes flow from personhood interests, granting homes bright line Fourth Amendment protection is consistent with the principle that “the Fourth Amendment protects people, not places.”¹⁹⁹ While “new technology unmoors privacy from property,” people will

¹⁸⁸ See Minnesota v. Carter, 525 U.S. 83, 95-96 (1998) (Scalia, J., concurring) (finding that the Fourth Amendment protects house residents “when they rent it[] and even when they merely occupy it rent free – so long as they actually live there”)
¹⁸⁹ See Minnesota v. Olson, 495 U.S. 91, 98-99 (1990) (concluding that an authorized overnight guest has a reasonable expectation of privacy in the home he is visiting).
¹⁹⁰ See United States v. Nerber 222 F.3d 597, 600 n.2 (9th Cir. 2000) (“For Fourth Amendment purposes, a hotel room is treated essentially the same, if not exactly the same, as a home.”)
¹⁹¹ See United States v. Gooch, 6 F.3d 673, 677 (9th Cir. 1993) (“We have already established that a person can have an objectively reasonable expectation of privacy in a tent on private property.”).
¹⁹² See Barros, Home, supra note 173, at 276-77 & n.90 (“[H]omes are sources of feelings of rootedness, continuity, stability, permanence, and connection to larger social networks.”).
¹⁹⁵ See Radin, Property, supra note 194, at 960, 978, 1013 (“Our reverence for the sanctity of the home is rooted in the understanding that the home is inextricably part of the individual, the family, and the fabric of society.”).
¹⁹⁶ Kelly, Home Searches, supra note 194, at 6.
¹⁹⁸ See Stephen P. Jones, Reasonable Expectations of Privacy: Searches, Seizures, and the Concept of Fourth Amendment Standing, 27 U. MEM. L. REV. 907, 957 (1997) (“The most sacred of all areas protected by the Fourth Amendment is the home.”); James Q. Whitman, The Two Western Cultures of Privacy: Dignity Versus Liberty, 113 YALE L.J. 1151, 1215 (2004) (noting that American privacy law conceives of the home “as the primary defense”); Kelly, Home Searches, supra note 194, 7-8 (noting that the home has become the “gold standard” for Fourth Amendment protection); but see Stephanie M. Stern, The Inviolate Home: Housing Exceptionalism in the Fourth Amendment, 95 CORNELL L. REV. 905, 911-12 (2010) (arguing that the Fourth Amendment should protect substantive privacy interests, and overprotecting homes comes at the expense of substantive interests outside the home).
always need a place to live, and will always expect additional privacy there.\textsuperscript{200} It follows, then, to grant added constitutional protections to a person’s place of residence, regardless of its location or permanency.\textsuperscript{201}

In response to recent advances in police surveillance technology, the Court has begun to develop these principles into a bright line rule protecting houses from government intrusion. In \textit{United States v. Karo},\textsuperscript{202} Drug Enforcement Agency (DEA) agents used an electronic tracking device, a “beeper,” while investigating a narcotics ring.\textsuperscript{203} The agents placed the beeper in a container, without first obtaining a warrant, and used the beeper to track the container through several private homes.\textsuperscript{204} On the basis of the beeper evidence, police obtained a warrant to search a residence which contained a drug lab.\textsuperscript{205} The Court held that the DEA agents violated the defendant’s Fourth Amendment rights, because the tracking device enabled them to see the location of the container in a private house, which could not ordinarily be seen without a warrant.\textsuperscript{206} This marked a significant step towards the adoption of a bright line rule protecting the home from police surveillance.

The Court completed this move in \textit{Kyllo v. United States}.\textsuperscript{207} In \textit{Kyllo}, police parked on a public street and directed a thermal imaging device at the defendant’s home, without first obtaining a warrant.\textsuperscript{208} The device revealed that some parts of his house were unusually hot, likely evidence that the defendant was using heat lamps to grow marijuana.\textsuperscript{209} The police used the thermal image as evidence of probable cause to obtain a search warrant against the defendant.\textsuperscript{210} The subsequent search revealed that the defendant was, in fact, growing marijuana under heat lights in his house.\textsuperscript{211} The Court found that the thermal imaging device violated the Fourth Amendment because, as in \textit{Karo}, it revealed “information regarding the interior of the home that could not otherwise have been obtained without physical intrusion.”\textsuperscript{212} Yet the Court went even further, declaring that “the Fourth Amendment draws a firm line at the entrance to the

\begin{footnotes}
\item[201] \textit{But see} California v. Carney, 471 U.S. 386, 390-93 (1985) (finding that a mobile home is not a “home” for Fourth Amendment purposes because it can be “quickly moved”). However, the Court expressly declined to reach the issue of a mobile home “that is situated in a way or place that objectively indicates that it is being used as a residence.” \textit{Id.} at 394 n.3.
\item[203] \textit{See id.} at 707.
\item[204] \textit{See id.} at 708.
\item[205] \textit{See id.} at 709-10.
\item[206] \textit{See id.} at 714-15.
\item[208] \textit{See id.} at 29.
\item[209] \textit{See id.}
\item[210] \textit{See id.}
\item[211] \textit{See id.}
\item[212] \textit{Id.} at 40 (internal quotations omitted).
\end{footnotes}
house” and “[t]hat line . . . must be not only firm but also bright . . . .” 213 Although many scholars lauded Kyllo as heralding “a new era of Fourth Amendment jurisprudence,”214 in reality it simply reaffirmed the Court’s longstanding belief that the warrantless physical invasion of the home “by even a fraction of an inch” is constitutionally impermissible.215 Since the decision, lower courts have faithfully applied Kyllo to mean that the Fourth Amendment offers special protections to the home.216

2. Bright Line Rule and Exceptions

The Kyllo Court adopted a firm, bright line rule against warrantless government searches of a house; however, it is subject to a “plain view” exception.217 An object is in plain view (and, therefore, unprotected by the Fourth Amendment) if it can be seen from an area where the police have a right to be, using technology that is in general public use.218 This is best exemplified by United States v. Knotts.219 The facts in Knotts are remarkably similar to those of Karo, except for the crucial difference that the electronic tracking device never went into a home.220 The Court held that since the device only revealed what could have been seen without a warrant on a public road, it did not violate the Fourth Amendment.221 Thus, what can be seen in public with technology that is in “general public use,” even if it is in a house, is not protected by the Fourth Amendment.222

Such an expansive plain view exception may well swallow the bright line rule as technology advances. As the dissenters in Kyllo rightfully point out, the Court’s supposedly stringent protections “dissipate[] as soon as the relevant technology is in general public use.”223 They argue that the rule and the exception are contradictory, and the exception will destroy the rule, since the uncertainty of general public use will undermine the rule’s bright line nature.224

---

213 Id. (quoting Payton v. New York, 445 U.S. 573, 590 (1980)).
214 Melissa Arbus, Note, A Legal U-Turn: The Rehnquist Court Changes Direction and Steers Back to the Privacy Norms of the Warren Era, 89 VA. L. REV. 1729, 1769 (2003); see also David A. Sklansky, Back to the Future: Kyllo, Katz, and Common Law, 72 MISS. L.J. 143, 144-45 (2002) (describing Kyllo as a “likely touchstone[]” for future Supreme Court cases on the Fourth Amendment whose “expansive” reasoning will have “significance beyond its narrow holding and beyond its value as a curiosity”).
216 See, e.g., Loria v. Gorman, 306 F.3d 1271 (9th Cir. 2002); United States v. Tolar, 268 F.3d 530, 532 (7th Cir. 2001).
217 Kyllo, 533 U.S. at 28.
218 See California v. Ciraolo, 476 U.S. 207, 213 (1986) (“What a person knowingly exposes to the public, even in his own home or office, is not subject to Fourth Amendment protection.”); see also Arizona v. Hicks, 480 U.S. 321 (1987) (finding that serial numbers were not in plain view because they could not be seen without moving a turntable); Florida v. Riley, 488 U.S. 445 (1989) (finding that aerial inspection of property did not trigger the Fourth Amendment because a citizen could legally have flown in the airspace).
220 See id. at 279.
221 See id. at 285.
222 Kyllo, 533 U.S. at 39 & n.6.
223 Id. at 47 (Stevens, J., dissenting).
224 See id.
Therefore, the plain view exception must be narrowed in order to save the rule. Rather than incorporate general public use, the Court should return to an older conception of plain view, wherein an object or activity loses bright line Fourth Amendment protection only if it is in “plain view of an officer who has a right be in the position to have that view.”

Unlike the general public use exception, this narrower plain view exception protects privacy within the home regardless of technological advances.

In practice, the narrower plain view exception only applies to objects and activities that an officer can see with can see with her own eyes in public. In order to preserve the brightness of the rule and avoid line drawing problems, this exception must be construed very strictly to exclude any technology an officer uses to improve law enforcement surveillance. “[D]evices that allow government to see things it could never see before” within the home, such as thermal imagers, GPS trackers or hidden cameras, fall squarely within the bright line rule and require a warrant. However, even “technology that allows governments to conduct more traditional surveillance more efficiently,” such as binoculars or flashlights, must also fall within the bright line rule for homes to prevent a creeping general public use exception from swallowing the rule. In fact, many courts have already accepted that “any enhanced viewing of the interior of a home impair[s] a legitimate expectation of privacy,” and have found binoculars and telescopes to trigger Fourth Amendment protection. Perhaps the only technology that may pass muster is prescription glasses, since they are worn to aid normal vision not law enforcement surveillance. Therefore, activities inside the home are only unprotected by the bright line rule when an officer can see illegal activity “with the naked eye” from public property.

This fits well with the Court’s conception of the role of police in society. The Court has long held that police possess the same rights as “every citizen” in public places. This includes

---

226 The Court has construed ‘public place’ broadly through the “open fields” doctrine. See Oliver v. United States, 466 U.S. 170, 179 (1984) (finding no reasonable expectation of privacy in open fields for Fourth Amendment purposes); see also United States v. Dunn, 480 U.S. 294, 301 (1987) (deciding “[c]urtilege questions” based on proximity, enclosure, use and protection from observation).
227 See, e.g., State v. Ward, 617 P.2d 568, 573 (Haw. 1980) (finding a reasonable expectation of privacy unless the activities were exposed to the naked eye).
228 Simmons, Broader Perspective, supra note 32, at 541-42, 549.
229 Id. at 541, 543-44, 550.
230 See Kyllo, 533 U.S. at 47 (Stevens, J., dissenting).
234 Terry v. Ohio, 392 U.S. 1, 32-33 (1968) (Harlan, J., concurring).
interactions with uniformed police in streets and airports, as well as conversations with undercover officers. Although most states have criminalized using binoculars or recording equipment to see into people’s homes, undercover policing raises difficult issues in which officers may commit criminal acts that could include violating the privacy of the home. Nonetheless, the Supreme Court has repeatedly held that suspects give information or invitations into their home at their own risk, effectively exempting undercover police from the Fourth Amendment. If undercover officers who commit crimes “are immune from prosecution so long as their actions lie within the scope of their official undercover role,” surely the incriminating evidence they obtain from their dangerous work should not be excluded. Since the Supreme Court has granted undercover policing an exemption from all Fourth Amendment requirements, so too should it be exempt from the bright line rule protecting homes.

Although the bright line rule is subject to narrow exemptions for plain view and undercover policing, it is inviolable by new technological advancements. Regardless of changes in the social use of technology or the development of new police surveillance, the government will not be able to see into the home without first obtaining a warrant. However, the bright line rule is merely for triggering Fourth Amendment protection and, therefore, is subject to all recognized exceptions to the warrant requirement. For instance, an officer in hot pursuit of a suspect may still enter a home without a warrant, as can an officer who reasonably believes that evidence will be destroyed. An officer can even enter a home to render emergency aid, so long as she is not motivated by a desire to arrest a suspect or seize evidence. However, in the normal course of a police investigation, police may not look inside a home by any technologically enhanced

---

235 See id. at 34 (White, J., concurring) (“There is nothing in the Constitution which prevents a policeman from addressing questions to anyone on the street.”); United States v. Mendenhall, 446 U.S. 544, 551-54 (1980) (finding that “not every street encounter between a citizen and the police” is “secured by the Fourth Amendment”).


240 Joh, supra note 238, at 158.

241 See Warden, Md. Penitentiary v. Hayden, 387 U.S. 294 (1964); United States v. Santana, 427 U.S. 38, 43 (1976) (“[A] suspect may not defeat an arrest which has been set in motion in a public place . . . by the expedient of escaping to a private place.”).


243 See Brigham City, 427 U.S. at 402-03.
means without first obtaining a warrant. This modified bright line rule of *Kyllo* “captures the prevailing *zeitgeist* about law, technology and privacy.”

3. Underinclusiveness, Overinclusiveness and Technology Adoption

Like all bright line rules, the modified *Kyllo* rule can be criticized for being “at once too broad and too narrow.” The rule can be criticized as underinclusive for basing its protection of privacy on homes, which “tends to favor the interests of wealthier people.” The rich have nicer, bigger homes (and some poor do not have homes at all), so the rich not only have a larger physical space in which to enjoy privacy, but they are also likely to spend more time at home since it is more comfortable. Since the rule necessarily provides more protection to homes than to public places, it makes Fourth Amendment protection a function of wealth. Nonetheless, the Fourth Amendment does not protect equity; it protects privacy from unreasonable government intrusion. Just as the First Amendment provides greater protection to media companies since they communicate more, the Fourth Amendment affords more protection to those who are better able to keep their lives private. While this may be inequitable, it is not unjust. Moreover, providing stronger protection to homes does not diminish the constitutional protections afforded to others, while ensuring that existing Fourth Amendment doctrine is not rendered meaningless by technological change.

The modified *Kyllo* rule can also be criticized for being overinclusive. By giving so much Fourth Amendment protection to the home, the rule makes it harder for police to catch more sophisticated criminals, such as drug lords, mafia dons and white collar criminals, who can conduct their criminal activities within the privacy of their homes. Without the general public use exception, this is even more difficult at night, since the rule would bar police from using flashlights or binoculars to see into homes. However, technology that can reveal information about the interior of the home is no substitute for classic police work such as, *inter alia*, visual surveillance, undercovers, informants, wiretaps, paper trails and deals with knowledgeable lower

---

245 *Kyllo*, 533 at 46 (Stevens, J. dissenting).
247 See id. at 1270.
248 See id. at 1270-72.
249 See Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (finding that “the ultimate touchstone of the Fourth Amendment is 'reasonableness'”) (unanimous).
251 See ARISTOTLE, NICOMACHEAN ETHICS (Joe Sachs, trans.) (2002) (arguing that equals should be treated equally and unequals should be treated unequally).
252 See Stuntz, *Distribution*, supra note 246, at 1267 (“[T]he kinds of crimes wealthier people tend to commit require greater invasions of privacy by the police to catch perpetrators.”).
253 See Ric Simmons, *From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1334-35 n.142 (2002).
level criminals.\textsuperscript{254} As discussed above, the Supreme Court has specifically exempted undercover officers and police cooperators wearing a wire from Fourth Amendment protection under the third-party doctrine.\textsuperscript{255} Despite the restrictions on police investigations, the strictness of the modified\textit{Kyllo} rule can incentivize the innovation and adoption of new technologies that do not invade the privacy of the home.

A bright line Fourth Amendment rule protecting houses raises the cost to police of violating privacy in the home, thereby diverting police resources to other tactics.\textsuperscript{256} It also has the secondary effect of increasing demand for new technologies that do not intrude on houses by making new technologies relatively cheaper.\textsuperscript{257} These “substitution effects” create a market for surveillance technology that does not look into homes. For instance, police can use electronic tracking devices to follow contraband—ranging from drugs to guns to child pornography—to a suspect’s home without actually looking inside.\textsuperscript{258} Similarly, police can use electronic surveillance and software to monitor phone calls, emails and digital paper trails in order to catch white collar criminals.\textsuperscript{259} They can even watch criminals as soon as they step outside their home using video surveillance technology.\textsuperscript{260} By making invading the privacy of the home relatively more costly to police, the bright line rule incentivizes the adoption of these technologies and spurs the innovation of new privacy protecting technologies. The strictness of the bright line rule ensures that technology does not eviscerate the longstanding privacy of the home while channeling police surveillance into less intrusive means. The rule can even operate in tandem with future bright line rules to ensure that police adopt methods and technologies that truly minimize privacy intrusions.

C. Bright Line Rule for Human Bodies

This Subsection traces the longstanding importance and special legal protections granted to the human body by Anglo-American common law, statutes and constitutional law. It examines Twentieth Century bodily search cases to demonstrate that the Court has acknowledged the special importance of the human body in criminal procedure, and has steadily increased its protection under the Fourth Amendment. This Subsection argues that a bright line rule protecting the human body from warrantless searches is the logical extension of the Court’s bodily search jurisprudence. However, it breaks slightly from existing case law by arguing that

\textsuperscript{255} See supra note 239.
\textsuperscript{256} See Stuntz, \textit{Distribution, supra} note 246, at 1267 (“When the Fourth Amendment limits the use of a police tactic like house searches, it does two things: it raises the cost of using that tactic, and it lowers the relative cost of using other tactics that might be substitutes.”).
\textsuperscript{257} See id.
\textsuperscript{259} See Bennett, \textit{supra} note 254, at 67-71.
police searches that violate the human body should be per se unconstitutional in order to prevent technology and exigency from undercutting the rule's bright line nature. It then sets out the details of the bright line rule with a limited plain view exception, and defends it against criticisms of underinclusiveness and overinclusiveness. This Subsection concludes by arguing that the bright line rule will incentivize the innovation and adoption of new technologies that protect the human body, while still enabling police to investigate crime.

1. Human Bodies and the Law

For centuries, Anglo-American common law has treated bodily integrity as an “absolute right,” since “[n]o right is held more sacred, or is more carefully guarded, by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others . . . .” Accordingly, common law torts requires informed consent for doctors performing surgery, or even pursuing nonsurgical treatment, because it is “fundamental in American jurisprudence, that every human being of adult years and sound mind has a right to determine what shall be done with his own body.” Similarly, contract law treats waivers or limitations of damages for “injury to the person” as “prima facie unconscionable.” In substantive criminal law, “[a]ny touching, however, slight, may constitute an assault and battery, and some states treat the murder of a pregnant woman as a double homicide. The constitution is perhaps even more protective of the human body, granting First Amendment protection to both clothing and tattoos. Similarly, the Fourteenth Amendment forbids physical violence by any government actor. Finally, the legal protections granted to homes are derived from the inviolability of the person. As the most personal and

261 1 WILLIAM BLACKSTONE, COMMENTARIES *127, *129 (stating that an “absolute right[]” of an individual was “the right of personal security [which] consists in a person's legal and uninterrupted enjoyment of his life, his limbs, his body, [and] his health . . . .”). See also In re Cincinnati Radiation Litig., 875 F. Supp. 816-18 (S.D. Ohio 1995) (outlining Supreme Court decisions regarding the right to be free from unwanted bodily intrusions dating back to 1884).
268 See, e.g., N.Y. PENAL LAW §§ 125.00-125.05 (McKinney 2010).
270 See, e.g., Brown v. Mississippi, 297 U.S. 278 (1936) (holding that confessions obtained by violence violate the Due Process Clause of the Fourteenth Amendment).
271 See Radin, Property, supra note 194, at 997-1000; Kelly, Home Searches, supra note 194, at 6; Halliburton, Privacy, supra note 194, at 852-67; see generally JOHN LOCKE, TWO TREATISES OF GOVERNMENT (Peter Laslett ed., Cambridge University Press, 3d ed. 1988) (arguing that property rights are derived from people’s inherent right to their own labor).
permanent feature of human life, the body deserves, and has received, the highest legal protection.

In the criminal procedure context, the Court first addressed bodily intrusions in *Rochin v. California.* In *Rochin*, police illegally broke into a narcotics suspect’s bedroom, and violently attempted to retrieve two capsules from his mouth. After this failed, the police took the defendant to the hospital where a doctor forced an emetic tube into his stomach, which induced him to vomit the capsules. The two capsules contained morphine, which was introduced into evidence, and the defendant was convicted at trial. Although the California appeals court upheld the conviction, the Supreme Court struck it on Fourteenth Amendment grounds, finding that the actions of the police and the doctor “shock[] the conscience” and are “offensive to human dignity.” Although *Rochin* was decided under the Fourteenth Amendment since the Court had not yet incorporated the exclusionary rule against the states, it demonstrates the Court’s belief that the longstanding legal protections granted to the human body apply even to police investigations.

The Court next considered bodily searches in *Breithaupt v. Abram.* In *Breithaupt*, the Court upheld forcibly taking a blood sample from an unconscious suspected drunken driver. The results of the blood test were admitted as evidence of intoxication at the defendant’s trial, where he was convicted of manslaughter. The Court found that “the absence of conscious consent, without more, does not necessarily render the taking a violation of a constitutional right” since “[t]he blood test has become routine in our everyday life.” Although *Breithaupt* was also decided on Fourteenth Amendment grounds, the Court balanced privacy interests and public safety interests against drunk driving, essentially engaging in a Fourth Amendment reasonableness analysis. Although the Court backtracked on the protections granted to the human body in *Breithaupt*, it took a big step towards introducing the Fourth Amendment into bodily searches.

The dissents in *Breithaupt* are particularly notable, both for staying true to the law’s general treatment of the human body, and foreshadowing future directions in bodily search law. Chief Justice Warren argued that *Breithaupt* is indistinguishable from *Rochin*, since both involve

---

273 *See* id. at 166.  
274 *See* id.  
275 *See* id. at 166-67  
276 *See* id.  
277 *Id.* at 172, 174.  
278 *See* Mapp v. Ohio, 367 U.S. 643 (1961) (incorporating the exclusionary rule against the states).  
280 *See* id. at 433.  
281 *See* id.  
282 *Id.* at 435-36.  
283 *See* id. at 439-40.  
forcible extractions from the human body. He argued that police “must stop short of bruising the body, breaking the skin, puncturing tissue or extracting bodily fluids” when obtaining evidence from suspects. Justice Douglas, joined by Justice Black, similarly argued that the police violated “the sanctity of the body of an unconscious man.”

He found that:

“[I]t is repulsive to me for the police to insert needles into an unconscious person in order to get the evidence necessary to convict him, whether they find the person unconscious, give him a pill which puts him to sleep, or use force to subdue him. The indignity to the individual is the same in one case as in the other, for in each is his body invaded and assaulted by the police who are supposed to be the citizen’s protector.”

The dissents make clear that the Court is sharply divided on the disposition of the case, yet both the majority and dissents agree on the importance of privacy and dignity for the constitutionality of bodily searches. The dissents, anticipating future case law, essentially argue that the majority has insufficiently weighed privacy and dignity given the intrusiveness of the search on the specially protected human body.

The Court formally adopted the Fourth Amendment for bodily searches in Schmerber v. California. In Schmerber, the defendant was in the hospital recovering from injuries from a car accident. The police suspected that he had been driving drunk and asked for consent to a blood test. The defendant, acting on advice of counsel, refused. The investigating officer then ordered a physician to draw a blood sample. A chemical analysis of the blood sample revealed that the defendant was, in fact, drunk. Building on Breithaupt, including the dissents, the Court found that “[t]he overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State.” Nonetheless, the Court held that taking a blood sample did not trigger Fourth Amendment protection, since blood tests are “commonplace,” “routine” and “involve[] virtually no risk, trauma or pain.” It further reasoned that since “the percentage of alcohol in the blood begins to diminish shortly after drinking stops,” the officer had to act immediately, otherwise the evidence would be ‘destroyed.’

---

286 Id. at 442.
287 Id. at 444 (Douglas, J., dissenting).
288 Id.
289 See Rogers, Bodily Intrusions, supra note 284, at 1186.
291 See id. at 758.
292 See id. at 765 n.9.
293 See id. at 766.
294 See id. at 758.
295 See id. at 759.
296 Id. at 767.
297 See id.
298 Id. at 771 & n.13 (internal quotation omitted).
299 Id. at 770-71.
The Court’s opinion in Schmerber is notable in three respects. First, it analyzed a blood test as a “search” under the Fourth Amendment, thereby recognizing the inherent tradeoff between privacy and security. In doing so, it required a “clear indication” that evidence would be found, and that the government must obtain a warrant wherever practicable. Second, the Court included human dignity in its reasonableness analysis in light of the heightened legal protections afforded to the human body. Commentators have read this as an acknowledgment of the “sanctity of the defendant’s body.” Third, as in Breithaupt, the Court adopted a species of general public use exception, which included blood tests. The dissents in Breithaupt objected to this exception, noting that the stomach pump was “common and accepted” in Rochin. In Schmerber, Justice Fortas similarly argued in dissent that:

[T]he State, in its role as prosecutor, has no right to extract blood from an accused, or anyone else, over his protest. As prosecutor, the State has no right to commit any kind of violence upon the person, or to utilize the results of such a tort, and the extraction of blood, over protest, is an act of violence.

In response, the Court raised the standards for bodily searches under the Fourth Amendment in Winston v. Lee. In Winston, police investigating an armed robbery wanted to force the defendant to undergo surgery to remove a bullet lodged in his left collarbone. Hoping to tie the bullet to the gun the victim used in self-defense, prosecutors initially obtained a court order requiring the surgery. However, subsequent lower courts enjoined the threatened surgery. The Court also blocked the surgery in a unanimous opinion that commentators have read to mark a return to Rochin by implying a per se rule against surgical searches that require general anesthesia. Even prior to Winston, many states had effectively adopted this per se rule. For surgical searches requiring localized anesthesia, the Court held that:

---

300 See Rogers, Bodily Intrusions, supra note 284, at 1186-88.
301 Schmerber, 384 U.S. at 769-70.
302 See id. at 767.
304 See Schmerber, 384 U.S. at 771 & n.13; Breithaupt, 352 U.S. at 436.
305 Breithaupt, 352 U.S. at 413 (Warren, C.J., dissenting).
306 Schmerber, 384 U.S. at 778 (Fortas, J. dissenting) (internal citation omitted).
308 See id. at 755-56.
309 See id. at 765.
310 See id. at 756-57.
311 See id. at 757-58.
312 See Mandell & Richardson, Surgical Search, supra note 303, at 537, 546-47.
The reasonableness of surgical intrusions beneath the skin depends on a case-by-case approach, in which the individual’s interests in privacy and security are weighed against society’s interests in conducting the procedure . . . 314

When conducting this balancing, the Court directed lower courts to examine “the magnitude of the intrusion,” “the extent of intrusion upon the individual’s dignitary interests,” and “the community’s interest in fairly and accurately determining guilt or innocence” as factors for determining the “reasonableness” of the intrusion for Fourth Amendment purposes.315 Thus, Winston draws a “major-minor dichotomy” between a bright line rule and balancing for bodily searches.316

2. Bright Line Rule and Exceptions

The Court’s opinion in Winston reintroduced bright line rules into bodily search jurisprudence, as first suggested in Rochin.317 Yet by only providing bright line rule protection to some, but not all, intrusive bodily searches, the Court left its work unfinished. The Winston Court chiefly erred by proposing a legal principle “built with one foot in the law and one foot in medicine.”318 As medical technology advances, the line between general and localized anesthesia may become blurred, with one or the other (or both) becoming more common.319 Moreover, by grounding the constitutionality of bodily searches on whether they are routine or risky,320 the Court “simply postpones the time at which general anesthetic surgical searches . . . become safe enough to fall on the minor side of the major-minor dichotomy . . . .”321 Yet in the interim, warrantless bodily searches run the grave risk of killing hemophiliacs or violating suspects’ religious beliefs.322 Thus, the major-minor dichotomy, predicated upon common usage and riskiness, is much like the general public use exception for homes that must be abandoned in order to save the rule.323

Similarly, although the reasonableness test suggested by the Winston Court for non-general anesthesia searches has been met with acclaim in the legal academy, both when it was decided

314 Winston, 470 U.S. at 760.
315 Id. at 761-63.
316 Mandell & Richardson, Surgical Search, supra note 303, at 547 & n.11.
317 See Rochin, 342 U.S. at 173-74 (“It would be a stultification of the responsibility which the course of constitutional history has cast upon this Court to hold that in order to convict a man the police cannot extract by force what is in his mind but can extract what is in his stomach.”).
318 Mandell & Richardson, Surgical Search, supra note 303, at 549.
319 Cf. id. at 548 (analogizing the impact of medical technology on abortion law to surgical searches).
320 See Schmerber, 384 U.S. at 771 & n.13 (internal quotation omitted).
321 Mandell & Richardson, Surgical Search, supra note 303, at 547.
322 See E. John Wherry, Jr., Vampire or Dinosaur: A Time to Revisit Schmerber v. California?, 19 AM. J. TRIAL ADVOC. 503, 508-09 n.20 (1996) [hereinafter Wherry, Vampire]. It is worth noting that the Court did acknowledge these risks, if only in passing. See Schmerber, 384 U.S. at 771 (“Petitioner is not one of the few who on grounds of fear, concern for health, or religious scruple might prefer some other means of testing . . . .”).
323 See supra notes 217-33 and accompanying text.
and today,\textsuperscript{324} it is causing confusion among the lower courts. Circuit courts have struggled to grapple with forced catheterization, which “is more intrusive than a needle but less intrusive than a scalpel, making it hard to classify under an objective reasonableness inquiry.”\textsuperscript{325} Even the procedural history of \textit{Winston} itself is illustrative. The lower courts initially found a 1.5 centimeter incision to be justified, but then found a 2.5 centimeter incision to be unconstitutional.\textsuperscript{326} To prevent such arbitrary judicial decisionmaking, the Court should extend \textit{Winston}’s bright line rule against general anesthetic surgical searches to all bodily searches, whether physical or electronic, under the principles of \textit{Rochin}.\textsuperscript{327}

In order to prevent advancements in medical technology and “routine” use from undercutting the rule’s bright line nature,\textsuperscript{328} the rule for bodies must be “brighter” in two respects. First, the rule must trigger Fourth Amendment protection for any search that looks within the body. Second, such searches must be per se unconstitutional, even if the police first obtained a warrant or an exception to the warrant requirement applies. The first requirement is similar to the bright rule for homes,\textsuperscript{329} since routine use, much like general public use, will continually expand and risk leaving Fourth Amendment protection for bodies an empty doctrine.\textsuperscript{330} Additionally, both courts and police will be able to avoid making arbitrary judgment calls concerning the intrusiveness of bodily searches, so police will be better able to protect privacy while investigating crimes.\textsuperscript{331}

The second requirement is much stricter than the bright line rule for homes,\textsuperscript{332} because police have used exigency to force suspects to undergo medical procedures against their will without a warrant.\textsuperscript{333} In \textit{Schmerber}, the Court reasoned that since “the percentage of alcohol in the blood begins to diminish shortly after drinking stops,” a forced blood test without a warrant is justified to prevent the “destruction of evidence under the direct control of the accused.”\textsuperscript{334}

\textsuperscript{324} See, e.g., Jay A. Gitles, Comment, \textit{Fourth Amendment—Reasonableness of Surgical Intrusions}, 76 J. CRIM. L. & CRIMINOLOGY 972, 979 (1985) (“The Court’s decision to apply the \textit{Schmerber} ‘reasonableness’ test to surgical intrusions was well-founded.”); Ric Simmons, \textit{Can Winston Save Us from Big Brother? The Need for Judicial Consistency in Regulating Hyper-Intrusive Searches}, 55 RUTGERS L. REV. 547, 587-89 (2003) (arguing for extending the \textit{Winston} reasonableness test to all “hyper-intrusive” searches).

\textsuperscript{325} \textit{LeVine v. Roebuck} 550 F.3d 684, 687 (8th Cir. 2008) (quoting \textit{Sparks v. Stutler}, 71 F.3d 259, 261 (7th Cir. 1995)).

\textsuperscript{326} See \textit{Winston}, 470 U.S. at 756-57.

\textsuperscript{327} Cf. Mandell & Richardson, \textit{Surgical Search}, supra note 303, at 549 (arguing that “[t]he \textit{Rochin} standard is a defensible, independent constitutional rationale”).

\textsuperscript{328} \textit{Schmerber}, 384 U.S. at 771 n.13 (citing Breithaupt, 352 U.S. at 436).

\textsuperscript{329} \textit{See supra} notes 217-34 and accompanying text.


\textsuperscript{331} \textit{See supra} notes 324-27 and accompanying text; \textit{see also supra} notes 129-153 and accompanying text.

\textsuperscript{332} \textit{See supra} notes 241-43 and accompanying text.


\textsuperscript{334} \textit{Schmerber}, 384 U.S. at 769-770 (internal citations omitted).
use of the exigency exception to the warrant requirement applies to every case involving ingestion of alcohol or drugs,\textsuperscript{335} even the police actions in \textit{Rochin}, which “shock[ed] the conscience” of the Court, could be permissible under the \textit{Schmerber} standard.\textsuperscript{336} Thus, commentators have declared that “[b]lindly following \textit{Schmerber} as authorization for all non-consensual blood seizure for forensic purposes is, in this day and age, an outrage.”\textsuperscript{337} While abandoning the exigency exception to the warrant requirement for bodily searches would help prevent such police abuse,\textsuperscript{338} the \textit{Winston} Court recognized that some bodily searches, even if conducted with prior judicial approval, violate “personal privacy and bodily integrity” to a sufficient extent to violate the Fourth Amendment.\textsuperscript{339} In light of rapidly advancing medical technology and the inability of courts to keep up,\textsuperscript{340} it is imprudent for courts to attempt to draw lines regarding the commonality or intrusiveness of a medical procedure, or for police to attempt to decide whether an exigency is sufficient to justify a search. Instead, as the \textit{Schmerber} Court recognized in part, “fundamental human interests require law officers to suffer the risk that such evidence may disappear . . . .”\textsuperscript{341} Therefore, the proposed bright line breaks from both \textit{Breithaupt} and \textit{Schmerber} by finding any search that looks within the body, including, \textit{inter alia}, forced blood draws, vomiting, catheterizations or body scanners without consent, to be per se unconstitutional whether conduct with or without a warrant.

Since the history of bodily search case law spans both before and after the incorporation of the exclusionary rule against the states, it is necessary to distinguish between Fourth and Fourteenth Amendment violations in the operation of the bright line rule. For instance, a search conducted with the requisite level of suspicion in a “particularly offensive manner” likely violates the Fourteenth, but not the Fourth, Amendment.\textsuperscript{342} For the converse, consider a “brain wave recorder” that detects electrical impulses in the brain to determine mood, arousal, medications and pregnancy.\textsuperscript{343} Since there is no physical element, its use by police does not violate the Fourteenth Amendment. However, it violates the bright line Fourth Amendment rule by looking within the body.\textsuperscript{344} Under current Fourth Amendment law, the constitutionality of the brain wave recorder hinges on how a judge values “the individual’s dignitary interests,” assuming it was used with probable cause.\textsuperscript{345} Conversely, the bright line rule prevents judges

\textsuperscript{335} See supra note 333.
\textsuperscript{336} Rochin v. California, 342 U.S. 165, 172 (1952).
\textsuperscript{337} Wherry, \textit{Vampire}, supra note 322, at 540.
\textsuperscript{338} See id. at 517-525.
\textsuperscript{340} See supra notes 80-81, 107-16 and accompanying text; see also supra notes 162-65 and accompanying text.
\textsuperscript{341} Schmerber, 384 U.S. at 770.
\textsuperscript{342} United States v. Arnold, 523 F.3d 941, 946-47 & n.2 (9th Cir. 2008).
\textsuperscript{343} Colb, \textit{World Without Privacy}, supra note 200, at 889.
\textsuperscript{344} Others have also argued that government brain scans ought to violate the Fourth Amendment. See, e.g., Halliburton, \textit{Privacy}, supra note 194, at 867-68 (arguing that personal thoughts are personal property subject to Fourth Amendment protection); Colb, \textit{World Without Privacy}, supra note 200, at 891.
\textsuperscript{345} Winston, 470 U.S. at 761. The brain wave recorder also likely violates the Fifth Amendment privilege against self-incrimination. See Schmerber, 384 U.S. at 761 (finding that the Fifth Amendment protects evidence that is “testimonial or communicative”).
from having to make arbitrary judgment calls concerning technology they may not fully understand,\textsuperscript{346} while preserving the centuries old respect for bodily integrity against any advancements in police surveillance or medical technology.

Given the extraordinary strictness of the bright line rule for bodies, it must be subject to a somewhat broader plain view exception than the bright line rule for homes. While the plain view exception for homes only covers objects or activities visible in public to the naked eye,\textsuperscript{347} the exception for bodies also includes an adaptation of the Fifth Amendment privilege against self-incrimination.\textsuperscript{348} The Fifth Amendment protects defendants from being compelled to “provide the State with evidence of a testimonial or communicative nature,”\textsuperscript{349} which includes any communications that, “explicitly or implicitly, relate a factual assertion or disclose information.”\textsuperscript{350} Therefore, as the \textit{Schmerber} Court pointed out, the Fifth Amendment does not protect “against compulsion to submit to fingerprinting, photographing, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture.”\textsuperscript{351} Similarly, the bright line Fourth Amendment rule does not protect bodily emanations that are external to the bodily itself, such as sweat, saliva, voices and fingerprints. So long as such material is obtained by abandonment,\textsuperscript{352} consent,\textsuperscript{353} or the requisite level of suspicion for a person with reduced privacy expectations,\textsuperscript{354} police actions do not violate the bright line rule. Just as “the Fourth Amendment draws a firm line at the entrance to the house,” so too must it draw a bright line for the human body.\textsuperscript{355}

The plain view exception for bodies, much like the exception for homes, also includes anything in “plain view of an officer who has a right be in the position to have that view”\textsuperscript{356} that can be seen “with the naked eye” or prescription glasses.\textsuperscript{357} Therefore, public video surveillance,\textsuperscript{358} facial recognition software\textsuperscript{359} and iris scanning technology all fall within the

\footnotesize{\textsuperscript{346} See supra notes 80-81, 107-16 and accompanying text; see also supra notes 162-65 and accompanying text. 
\textsuperscript{347} See Harris v. United States, 390 U.S. 234, 246 (1968). 
\textsuperscript{348} See U.S. CONST. amend. V, cl. 3. 
\textsuperscript{349} Schmerber, 384 U.S. at 761. 
\textsuperscript{351} Schmerber, 384 U.S. at 764. 
\textsuperscript{352} For example, fingerprints or saliva left on a glass. See, e.g., State v. Piro, 112 P.3d 831, 834. 
\textsuperscript{354} See, e.g., United States v. Kelly, 55 F.2d 67, 69 (2d Cir. 1932) (holding that fingerprinting a suspect at the time of arrest is an appropriate means for identification). 
\textsuperscript{356} Harris v. United States, 390 U.S. 234, 246 (1968). 
\textsuperscript{358} See Simmons, Broader Perspectives, supra note 32, at 550; Kerr, New Fourth Amendment, supra note 260, at 953-55 (2009); Slobogin, Privacy at Risk, supra note 42, at 89-90. 
\textsuperscript{359} See Simmons, Technology-Enhanced, supra note 55, at 729-30; People v. Johnson, 43 Cal. Rptr. 3d 587, 597-98 (Cal. Ct. App. 2006) (discussing potential uses of facial recognition software); David Lamb, One Last City is Scanning Faces in the Crowd, L.A. TIMES, Sept. 29, 2003, at A10 (reporting that Virginia Beach continues to use facial-recognition systems to scan for terrorists, felons with outstanding warrants and missing children).}
plain view exception.\textsuperscript{360} The furthest this exception extends is visual body cavity searches. Although body cavity searches literally entail looking inside the body, they can only be conducted without a warrant on those with highly reduced privacy expectations, such as prison inmates.\textsuperscript{361} Moreover, so long as they only conducted with the naked eye, there is no risk of new technologies invading a constitutionally protected space. This allows for an addition to the plain view exception for bodies: drug sniffing dogs. Although dogs are an extension from plain view,\textsuperscript{362} they are unique for four reasons. First, the Supreme Court has repeatedly held that dog sniffs are not searches within the meaning of the Fourth Amendment.\textsuperscript{363} Second, they are “binary surveillance tools” that only reveal ‘yes’ or ‘no’ answers.\textsuperscript{364} Third, a dog sniff is particularly nonintrusive.\textsuperscript{365} Fourth and most importantly, barring astonishing feats of evolution, a dog cannot advance to further infringe on privacy interests.\textsuperscript{366} Therefore, drug sniffing dogs fall within the plain view exception.

3. Underinclusiveness, Overinclusiveness and Technology Adoption

Like all bright line rules, the body rule can be criticized for being “at once too broad and too narrow.”\textsuperscript{367} The rule can be criticized as underinclusive for not protecting against facial recognition software or video surveillance.\textsuperscript{368} However, such surveillance does not infringe upon the “individual’s dignitary interests in personal privacy and bodily integrity.”\textsuperscript{369} Even as technological aggregation makes new surveillance feasible,\textsuperscript{370} it only violates bright line Fourth Amendment protection if it impedes the “sacred . . . right of every individual to the possession and control of his own person. . . .”\textsuperscript{371} Moreover, extending Fourth Amendment protection to such technologies forces courts to make ad hoc judgments about how much aggregation is too


\textsuperscript{361} See Bell v. Wolfish, 441 U.S. 520, 560 & n.41 (1979) (holding that “visual body-cavity inspections” can be conducted with probable cause and less than probable cause for inmates).


\textsuperscript{363} See Place, 462 U.S. at 707 (finding that a “canine sniff is sui generis” and does “not constitute a ‘search’ within the meaning of the Fourth Amendment”); Illinois v. Caballes, 543 U.S. 405, 410 (2005) (“A dog sniff conducted during a concededly lawful traffic stop . . . does not violate the Fourth Amendment.”).

\textsuperscript{364} Simmons, Broader Perspectives, supra note 32, at 564. See also Place, 462 U.S. at 707 (finding that “a canine sniff by a well-trained narcotics-detection dog” will only reveal “the presence or absence of narcotics, a contraband item”); Illinois v. Caballes, 543 U.S. 405, 408-409 (2005).

\textsuperscript{365} See Place, 462 U.S. at 707.

\textsuperscript{366} The exception does not extend to machines that reveal the same binary information, because they can advance to further intrude into bodily privacy.

\textsuperscript{367} Kyllo, 533 at 46 (Stevens, J. dissenting).

\textsuperscript{368} See Murphy, Paradigms, supra note 43, at 1332-36; Slobogin, Camera, supra note 13 (arguing that courts should interpret the Fourth Amendment to recognize the right to be free from video surveillance in public, and suggesting that courts should set up guidelines for the use of such surveillance).

\textsuperscript{369} Winston, 470 U.S. at 761.

\textsuperscript{370} See Simmons, Technology-Enhanced, supra note 55, at 727-28.

\textsuperscript{371} Union Pacific Railway Co. v. Botsford, 141 U.S. 250, 251 (1891).
much, thereby creating police uncertainty concerning privacy rights. By drawing a bright line at the human body, courts can ensure that technology does not erode bodily privacy protections while creating clear rules for police to follow while investigating crime.

A more serious underinclusion criticism concerns DNA evidence. DNA can be obtained as a condition of incarceration, or simply from a soda can. Once it is entered into state and national databases, it can be used to trace an individual to crimes ranging from petty thefts to rapes that occurred decades earlier. However, so long as the DNA is not forcibly collected in an intrusive manner, DNA typing does not violate the bright line rule because of the adapted Fifth Amendment exception. Just as chemically testing a lawfully obtained blood sample for alcohol is not a testimonial communication protected by the Fifth Amendment, testing a lawfully obtained DNA sample for identification is merely a bodily emanation not protected by the Fourth Amendment.

This does not disturb the privacy protections of the bright line rule for bodies for three reasons: the type of DNA collected, the status of the persons from whom DNA is collected and the procedural safeguards in place. The government only collects and tests “junk DNA” that is “not associated with any known physical or medical characteristics,” but “differs from one individual to the next.” Therefore, it is only useful for “purposes of identification,” not unlike a dog sniff, thereby significantly limiting privacy violations. DNA is only forcibly collected for those convicted or indicted of crimes, that is, those with fewer privacy rights. Modern DNA collection techniques require just six cells of hair, skin or saliva that can be painlessly obtained from a cheek swab. For mere suspects, DNA must be collected either by consent or abandonment. Moreover, DNA databases contain “an array of statutory safeguards to foreclose the possibility of abuse,” including criminal sanctions. Finally, extending bright line Fourth Amendment protection to DNA typing would require judicial regulation of a rapidly

---

372 See, e.g., Murphy, Paradigms, supra note 43 at 1329-32; State v. Piro, 112 P.3d 831, 834 (Idaho Ct. App. 2005) (upholding DNA testing of a water bottle retained by officers after the defendant was offered a drink while in custody).

373 See Erin Murphy, The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence, 95 CAL. L. REV. 721, 732-44 (2007) [hereinafter Murphy, New Forensics] (noting the importance of DNA typing to the criminal justice system, charting its expansion into smaller crimes as costs have fallen and explaining how DNA databases facilitate “cold hits” to enable conviction in the absence of any other evidence).


375 United States v. Weikert, 504 F.3d 1, 3-4 (1st Cir. 2007) (internal quotation omitted).

376 Id.

377 See, e.g., id. at 3 (upholding DNA sample requirement for those on supervised release); United States v. Pool, 621 F.3d 1213, 1214-15 (9th Cir. 2010) (upholding DNA sample requirement for those indicted but not yet convicted as a condition of bail).

378 See Murphy, New Forensics, supra note 316, at 733. A cheek swab would fall within the plain view exception to the bright line rule since it can be seen in public with the naked eye.

379 See Murphy, Paradigms, supra note 43, at 1332 & n.45.

evolving forensic science. Not only would any judge-made rules perpetually lag behind scientific developments, but judges could also impede criminal investigations or even harm privacy interests if they fail to understand how new DNA typing techniques work.

The rule can also be criticized as overinclusive. Breithaupt emphasized “[t]he increasing slaughter on our highways,” demonstrating that the Court saw blood tests as an important way to police drunk driving. The Schmerber Court was similarly worried about the unenforceability of drunk driving laws without forced blood tests. Under the bright line rule, drawing blood without consent would be per se unconstitutional, even though a suspect’s blood alcohol level may drop significantly by the time a police officer was able to obtain a warrant. Yet technology has provided a solution. Rather than force suspects to undergo blood tests, police can, instead, administer Breathalyzer tests. As the Court later noted:

Unlike blood tests, breath tests do not require piercing the skin and may be conducted safely outside a hospital environment and with a minimum of inconvenience or embarrassment. Further, breath tests reveal the level of alcohol in the employee’s bloodstream and nothing more.

Although the police use Breathalyzers to measure blood alcohol level within the body, the crucial distinction is that officers administering breath tests are only looking outside the body. Like fingerprints or saliva, a person’s breath is a bodily emanation that can be obtained without violating the bright line rule for bodies. By contrast, the police in Kyllo violated the Fourth Amendment by measuring heat levels inside the home itself, not those outside in public. Although this distinction may seem facile, it based upon centuries of Anglo-American law. While measuring a person’s breath violates no recognized legal principles, forcing a needle into a person’s body “is an act of violence,” a battery, by the state.

---

381 See Murphy, New Forensics, supra note 373, at 732-44 (charting the progress and expansion of DNA typing).
382 See supra notes 162-165 and accompanying text.
384 See Schmerber 384 U.S. at 771. Interestingly, some studies have called into doubt the reliability of blood tests as forensic tests for alcohol. See, e.g., Carol A Roehrenbeck, Blood is Thicker Than Water: What You Need to Know to Challenge a Blood Alcohol Result, 8 CRIM. JUST. 14 (Fall 1993).
385 See Schmerber, 384 U.S. at 771 & n.13. But see Wherry, Vampire, supra note 322, at 519-20 (arguing that “some alcohol will remain detectable in the blood system for 3.6 to 6.6 hours”).
388 See TAYLOR, supra note 386 at § 8.1.
390 See Kerr, New Technologies, supra note 14, at 834-35 (arguing that Kyllo “is rather mystifying from the standpoint of physics”).
391 Schmerber, 384 U.S. at 778 (Fortas, J. dissenting) (internal citation omitted).
Had the *Schmerber* Court adopted the proposed bright line rule, then police forces nationwide would have been strongly incentivized to adopt Breathalyzers.\(^{392}\) Today, technology has even reached the point that blood alcohol levels can be determined from a person’s sweat.\(^{393}\) As technology evolves, police will be able to enforce the law while better protecting privacy in all areas of bodily search law, not simply drunk driving and blood tests. For drug swallowing cases, rather than forcibly inducing vomiting,\(^{394}\) police can simply wait for the suspect to excrete the drugs.\(^{395}\) For bullet removal cases, the very fact that a suspect refuses to have a bullet removed from his body is highly probative of guilt.\(^{396}\) Although body scanners are per se unconstitutional under the bright line rule, law enforcement can still conduct traditional pat-downs and search luggage at the airport.\(^{397}\) Finally, the bright line rule creates a market for new law enforcement technologies that do not violate the constitutionally protected human body. By incentivizing the innovation and adoption of less intrusive bodily search techniques, the bright line protects core Fourth Amendment rights while avoiding overbreadth.

### Conclusion

Under current law, the constitutionality of body scanners in airports under the Fourth Amendment is an easy case;\(^{398}\) it should not be. Body scanners use “low intensity X-ray beams” to peer into airline passengers’ bodies to detect nonmetallic objects.\(^{399}\) Such government intrusion violates centuries of protections granted to the human body in all areas of law. A bright line Fourth Amendment rule protecting bodies not only prevents such government intrusions, but also encourages law enforcement to find alternative means to provide security. Moreover, the clarity of the rule ensures compliance regardless of future technological developments while creating a market for surveillance technologies that do not violate protected areas of privacy.

The technology adoption mechanism brings the relationship between the Fourth Amendment and technology full circle. As the internet and digitalization downwardly redefine privacy norms, police and prosecutors magnify this effect by developing increasingly intrusive surveillance technologies. Yet neither courts nor legislatures can adequately keep up with this rapid pace of technological change, and law enforcement agencies have little incentive to protect

\(^{392}\) *Cf.* Stuntz, *Distribution, supra* note 246, at 1267 (“When the Fourth Amendment limits the use of a police tactic . . . it raises the cost of using that tactic, and it lowers the relative cost of using other tactics that might be substitutes.”).

\(^{393}\) *See* Murphy, *Paradigms, supra* note 43, at 1334-35.

\(^{394}\) *See* Rochin v. California, 342 U.S. 165, 166 (1952).


\(^{397}\) *See, e.g.*, United States v. Edwards, 498 F.2d 496, 500-01 (2d Cir. 1974) (upholding pat-downs and hand searches of carry-on luggage in airports).


\(^{399}\) *Id.* at 3.
privacy. Therefore, the only way to sufficiently protect society’s remaining privacy interests is to cabin off core areas of privacy with bright line Fourth Amendment rules. These rules not only ensure citizens’ privacy regardless of new technological developments, they also give law enforcement certainty when conducting investigations. By increasing the relative costs of invading the privacy of the home and the human body, the bright line rules create demand for non-invasive surveillance technology that will spur its innovation and widespread adoption. Bright line rules ensure a virtuous cycle of technological improvement, effective law enforcement and protected privacy interests. Although courts should begin by adopting bright line rules for homes and bodies, more constitutional privacy protection may be needed in the future. As technology continues to improve and redefine society’s interactions, courts and commentators will constantly have to reevaluate the appropriateness of current Fourth Amendment rules.