ENDING THE ZERO-SUM GAME: HOW TO INCREASE THE PRODUCTIVITY OF THE FOURTH AMENDMENT

RIC SIMMONS*

* Professor of Law, Moritz College of Law at The Ohio State University. Portions of this Article were presented at the South East American Law School conference in August, 2012. Thanks to my fellow panelists Renée Hutchins, Michael Mannheimer, and Laurent A. Sacharoff for their thoughts and feedback on my presentation. Thanks also to Professor Mary Leary for comments on an earlier draft.

INTRODUCTION

Every criminal procedure student learns on the first day of class that Fourth Amendment policy represents a zero-sum game: a constant struggle between the individual privacy of citizens and the needs of law enforcement.[1] The job of the courts is to mediate that struggle, to be referees in the "game" of cat-and-mouse between the police officer and the criminal. Before the Fourth Amendment was ever written, the parameters of the "game" were well-established when Benjamin Franklin declared, "[t]hey who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety."[2] The implication is clear: there is, and always will be, a trade-off between liberty and security, and the only way to get more security is to forfeit some liberty.

Judges frequently refer to criminal investigations as a competitive enterprise, in which the job of the courts is to maintain the status quo between both sides. The Supreme Court has repeatedly stated that the purpose of the Fourth Amendment is to act as a safeguard against the law enforcement officer "engaged in the often competitive enterprise of ferreting out crime."[3] Most recently, the concept of ensuring a fair competition between opposing sides has been on display in the cases involving the government's use of Global Position System (GPS) tracking devices. Judges opposed to these devices argue that their use unfairly tips the balance in favor of the government because the devices are so inexpensive that surveillance becomes too easy[4] and because the usual countermeasures one

1. In game theory, a "zero-sum game" is a situation in which a participant's gain (or loss) of utility is exactly balanced by the losses (or gains) of the utility of the other participant.

2. 1 BENJAMIN FRANKLIN, MEMOIRS OF THE LIFE AND THE WRITINGS OF BENJAMIN FRANKLIN 270 (London, Henry Colburn 1818).

3. Lo-Ji Sales, Inc. v. New York, 442 U.S. 319, 326 (1979) (quoting Johnson v. United States, 333 U.S. 10, 14 (1948)); United States v. Chadwick, 433 U.S. 1, 9 (1977) (quoting *Johnson*, 333 U.S. at 14).

4. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 963–64 (2012) (Alito, J., concurring in the judgment).

employs against government surveillance become worthless.[5] In a recent article in the Harvard Law Review,[6] Professor Orin Kerr claimed that "the basic dynamic of Fourth Amendment law resembles a zero-sum game,"[7] arguing that the fundamental principle driving Fourth Amendment jurisprudence over the past hundred years has been the courts' desire to maintain an "equilibrium" between police power and civil liberties.[8]

In reality, however, the "competition" between law enforcement and criminals is not zero-sum. In order to see why, we need to see the criminal justice system not as a *competition*, but instead as an *industry*. In the decades since the beginning of the law and economics movement,[9] there has been surprisingly little application of economic principles to criminal procedure.[10] Richard Posner's foundational textbook *Economic Analysis of the Law*, for example, devotes only five of its 716 pages to

---

5. *See* United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, J., dissenting) ("You can preserve your anonymity from prying eyes, even in public, by traveling at night, through heavy traffic, in crowds, by using a circuitous route, disguising your appearance, passing in and out of buildings and being careful not to be followed. But there's no hiding from the all-seeing network of GPS satellites that hover overhead, which never sleep, never blink, never get confused and never lose attention."); *see also* United States v. Garcia, 474 F.3d, 994, 998 (7th Cir. 2007) ("There is a tradeoff between security and privacy, and often it favors security.").

6. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).

7. *Id.* at 543.

8. *Id.*

9. The Law and Economics movement is generally thought to have begun with the publication of two groundbreaking articles in the early 1960's: Ronald Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960) and Guido Calabresi, *Some Thoughts on Risk Distribution and the Law of Torts*, 70 YALE L.J. 499 (1961).

10. *Cf.* Craig S. Lerner, *The Reasonableness of Probable Cause*, 81 TEX. L. REV. 951 (2003); Steven Penney, *Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach*, 97 J. CRIM. L. & CRIMINOLOGY 477 (2007); Hugo M. Mialon & Sue H. Mialon, *The Effects of the Fourth Amendment: An Economic Analysis*, (Emory Law Sch. Pub. Law & Legal Theory Research Paper Series, Paper No. 06-3, 2006), *available at* http://papers.ssrn.com/abstract=755035; Andrew Song, *Technology, Terrorism, and the Fishbowl Effect: An Economic Analysis of Surveillance and Searches*, (Berkman Ctr. For Internet & Soc'y, Working Paper No. 73, 2003), *available at* http://papers.ssrn.com/abstract= 422220. *See generally* Frank H. Easterbrook, *Criminal Procedure as a Market System*, 12 J. LEGAL STUD. 289 (1983) (discussing law and economics with regard to the trial aspects of criminal procedure, such as prosecutorial discretion, plea bargaining, and sentencing). There have also been a number of articles using economic principles to determine the effect of the exclusionary rule. For an example, see Myron W. Orfield, Jr., *The Exclusionary Rule and Deterrence: An Empirical Study of Chicago Narcotics Officers*, 54 U. CHI. L. REV. 1016 (1987).

criminal procedure.[11] Perhaps this is because criminal procedure, unlike tort law or contract law, deals with fundamental rights, which are less amenable to cost-benefit analysis.[12] But the mere fact that the Fourth Amendment protects fundamental rights does not mean that we cannot apply economic principles to evaluate it. Fourth Amendment law is about balancing privacy rights with the needs of law enforcement, and economic principles can inform that analysis.

Our goal in applying these economic principles to Fourth Amendment law is to increase the efficiency of the criminal justice system—that is, to maximize output while minimizing costs. This focus on efficiency does not mean that we are indifferent to the constitutional rights of our citizens. To the contrary, the potential infringement of these rights is one of the costs that we are seeking to minimize. Another cost, more easily measured, is the tangible monetary cost incurred by law enforcement organizations (and thus ultimately by society as a whole) to undertake a given type of surveillance.[13] The output that we are seeking is crime control, or more specifically in the Fourth Amendment context, the identification of those who are guilty of a crime and collection of evidence that can be used to demonstrate their guilt.[14] Roughly speaking, the more money we spend, or the more willing we are to infringe on our own freedoms, the more output we receive in terms of identifying the guilty and recovering incriminating evidence.

Once we apply economic analysis to this question, however, we can see that there are two reasons why Fourth Amendment doctrine could in fact be a positive-sum game. First, advances

---

11. RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW (6th ed. 2003). Posner briefly discusses plea bargaining, *Terry* stops, the exclusionary rule, and coerced confessions. *Id.* at 577–80, 712–16.

12. Penney, *supra* note 10, at 478–79.

13. Throughout this Article I will use the word "surveillance" to cover any method of investigation carried out by law enforcement officials, from accessing a Department of Motor Vehicles database to wiretapping a telephone to strip-searching a suspect. This rather awkward terminology is required because the term "search" has a very particular meaning in Fourth Amendment jurisprudence as a method of surveillance that implicates the Fourth Amendment to the degree that it requires probable cause or a warrant. *See* Katz v. United States, 389 U.S. 347, 350–53 (1967).

14. Of course, more efficient crime control is not just about identifying the guilty; it also entails collecting evidence that can exonerate the innocent.

in technology can increase the effectiveness of surveillance in catching criminals without reducing the privacy rights of ordinary citizens—that is, it is possible to increase the output without increasing the cost.[15] Second, changing norms and attitudes may decrease the value of certain kinds of privacy to individuals, causing the cost of certain types of surveillance to decrease. This can work in the other direction as well: When criminals, rather than police, take advantage of technological advances, the output of the system will decrease even if costs are held constant. Likewise, societal norms could change to make certain types of privacy more valuable, thus increasing the cost to the system. In these situations, the criminal justice system becomes a negative-sum game.

Another advantage of applying economic tools is that the application helps identify potential trade-offs in the system between different costs. For example, more money spent on training police could result in less infringement on constitutional rights while maintaining the same level of output (that is, the same level of gathering evidence and apprehension of criminals). More controversially, we may be able to maintain the same level of output by adopting newer types of surveillance that are less expensive but result in greater infringement on our privacy rights. It may well be that this latter trade-off is one that many people will never want to undertake, as even a savings of millions of dollars is not worth even a slight loss of privacy rights. But an economic analysis of the question at least makes that choice more transparent.

Once we have identified the productivity of different forms of surveillance, we can take steps to encourage more productive types of surveillance and discourage the less productive ones. This can be accomplished by adjusting the legal standard of suspicion that law enforcement is required to demonstrate before engaging in different methods of surveillance, from no suspicion at all, to reasonable suspicion, to probable cause, or to something even higher. If a certain surveillance method is

15. *See* United States v. Knotts, 460 U.S. 276, 284 (1983) ("Insofar as respondent's complaint appears to be simply that scientific devices such as the beeper enabled the police to be more effective in detecting crime, it simply has no constitutional foundation. We have never equated police efficiency with unconstitutionality, and we decline to do so now.").

very productive—that is, if it produces a high level of success with a low cost in terms of resources and infringements on our privacy—then we should encourage law enforcement agents to conduct the surveillance by removing any constitutional or statutory restrictions on the activity. And if a certain method of surveillance is particularly unproductive, we should require law enforcement agents to demonstrate a high level of suspicion—probable cause or greater—before being allowed to engage in that activity.

Part I of this Article will sketch out a basic formula for analyzing the productivity of different surveillance methods by measuring the cost of the inputs and the benefits of the outputs. Part II will apply this formula to different methods of surveillance to see how certain methods of surveillance are more productive than others, and will look for ways to increase the productivity of surveillance generally. The Article concludes by offering some suggestions for changing the way we regulate surveillance techniques to maximize the efficiency of the process.

I. APPLYING ECONOMIC ANALYSIS TO FOURTH AMENDMENT DOCTRINE

Until quite recently, scholars had done very little to apply economic principles to questions of criminal procedure.[16] Those that did tended to focus on the post-arrest aspects of criminal procedure—for example, how to regulate plea bargaining or prosecutorial discretion to produce an optimal result.[17] In 2003, Professor Craig Lerner provided the first serious attempt to apply economic principles to the Fourth Amendment when he

16. There has been a substantial amount of law and economics work in the substantive criminal law area—for example, using economic tools to determine the proper sanction for certain crimes. *See, e.g.*, Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968); Richard A. Posner, *Optimal Sentences for White-Collar Criminals*, 17 AM. CRIM. L. REV. 409 (1980). Other scholars have argued for privatization of the criminal justice system. *See, e.g.*, BRUCE L. BENSON, TO SERVE AND PROTECT: PRIVATIZATION AND COMMUNITY IN CRIMINAL JUSTICE (1998). Some scholars have applied econometric principles to determine the effects of certain criminal law doctrines such as the exclusionary rule. *See, e.g.*, Raymond A. Atkins & Paul H. Rubin, *Effects of Criminal Procedure on Crime Rates: Mapping Out the Consequences of the Exclusionary Rule*, 46 J.L. & ECON. 157 (2003).

17. *See, e.g.*, Easterbrook, *supra* note 10.

proposed a formula for determining whether probable cause exists in a certain case.[18] Professor Lerner chose as his starting point the famous Learned Hand formula from tort law, which is used to calculate whether a party has been negligent. Under Hand's formula, a party is negligent if the burden, or cost, of taking precautions to prevent an accident (B) is less than the probability of the accident occurring (P) times the social loss of the accident (L). In mathematical terms, if B < P * L, then the defendant was negligent.[19]

Professor Lerner adapts the formula and applies it to the probable cause context by proposing that a search would be reasonable if the social cost of the search in terms of the intrusion on privacy (C) is less than the social benefit (B) of the search multiplied by the probability of the search being successful (P).[20] In mathematical terms: If C < P * B, then the search is reasonable and probable cause exists.[21] Professor Lerner fine-tunes his formula with a few more variables,[22] but this basic principle remains the foundation of his argument.

---

18. Lerner, *supra* note 10, at 1019–22.

19. *See* United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947).

20. Lerner, *supra* note 10, at 1019–20.

21. *Id.*

22. Professor Lerner would reduce the social cost (C) by the factor "(1-P)," because he argues that the Supreme Court has determined there is no constitutionally recognized privacy intrusion if the search is successful. *Id.* at 1020. This factor, however, seems to misinterpret the Supreme Court doctrine in this area. The Supreme Court has held that if the surveillance can detect *only* information about illegal activity, then the surveillance does not infringe on any constitutionally protected rights—for example, a drug sniffing dog that tells the police nothing about the object of the search other than the fact that contraband is or is not present. *See, e.g.*, Illinois v. Caballes, 543 U.S. 405, 408–09 (2005). But this doctrine does not mean that a certain type of surveillance does not infringe on any constitutionally protected rights in every case in which the police find contraband. If the police search a suspect's house and find narcotics, the search still infringed on the suspect's rights—and definitely impacted the Fourth Amendment—because the police saw a lot of other private information while looking for the narcotics. Under Professor Lerner's revised formula, there would be no privacy intrusion and the social cost of this search would be zero.

Professor Lerner would also increase the social cost (C) by the factor "m," which he calls a "privacy multiplier," in order to "reflect the fact that not all seemingly identical searches are in fact identical, at least in the subjectively experienced intrusion on one's privacy." Lerner, *supra* note 10, at 1021. For example, Professor Lerner argues that an African-American person who is pulled over for the tenth time that year may subjectively feel a greater infringement than a white person who is pulled over for the first time. *Id.* As I note below, I am in favor of a using a

Professor Lerner intentionally deviates from established Fourth Amendment doctrine in one very significant way: He considers both the likelihood of success of the surveillance and the severity of the crime being investigated as factors in determining whether probable cause exists.[23] In other words, the social benefit "B" in his formula is not a constant, but a variable—it will be higher if the police are investigating a rape or a murder, and lower if they are investigating a petty larceny or a simple assault. It will also be higher if the search is very likely to uncover evidence of a crime, and lower if it is a mere fishing expedition that has a small likelihood of producing useful information. Consequently, under Professor Lerner's standard, a court may find probable cause to support an intrusive search (with a high "C") if the police are investigating a particularly severe crime or had a good chance of uncovering evidence. On the other hand, under this formula, a court would conclude that there was no probable cause to support the same search if the alleged crime were less severe or the likelihood of success was low.[24] This approach is consistent with Professor Lerner's economic analysis methodology: To weigh the costs and benefits of a particular course of action, it is important to have a realistic—as opposed to a formalistic—evaluation of the likely "benefits." Professor Lerner also argues that this approach is supported both by common sense and by the "reasonableness" language of the Fourth Amendment.[25] Indeed, a number of other scholars have proposed that courts take into account the severity of the crime at hand in assessing Fourth Amendment "reasonability,"[26] though this approach has gained very little traction with the courts.[27]

We will use Professor Lerner's formula as the starting point for our analysis. The principle is simple: Every type of surveillance has a cost and an expected benefit. Professor Lerner uses

---

more generalized "cost to society" rather than trying to calculate a specific subjective cost for each individual. *See infra* notes 32–42 and accompanying text.

23. Lerner, *supra* note 10, at 1015.

24. *Id.* at 1020 ("[t]he expected social benefit of a successful search increases if the crime under investigation is, say, aircraft privacy rather than tax fraud.").

25. *Id.* at 1019–20.

26. *See, e.g.*, Akhil Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 801–02 (1994).

27. *See, e.g.*, Dunaway v. New York, 442 U.S. 200, 207–12 (1979).

this formula in order to determine whether probable cause exists in a particular case. If the expected benefit exceeds the expected cost, there is probable cause, and a search should be permitted.[28] Our focus, however, is somewhat different. We are not attempting to create a minimum standard for when a type of surveillance should be permitted; instead, we are attempting to maximize the efficiency of searches that do occur. Once we determine which type of searches are the most efficient, we can devise legal rules that encourage more efficient searches and discourage the less efficient ones.[29]

Therefore, our formula should take the form of an equation in which the resources and costs (C) are the inputs to the system and the benefits (B) are the output.[30] To make the equation balance, we will add a variable X to the left side of the equation to act as the conversion rate between the costs and the benefit. In economic terms, X is the "productivity" of the system—if X is high, we receive a large amount of output in exchange for a small amount of input. If X is low, we receive a small amount of output in exchange for a large amount of input.[31] Our equation thus begins rather simply:

$$(C * X) = B$$

---

28. Lerner, *supra* note 10, at 1019–20.

29. Essentially Professor Lerner is engaged in the process of calculating productivity as well, although his ultimate goal is to determine a minimum level of productivity at which a surveillance method will be permitted. This minimum level will be termed "probable cause." Under Professor Lerner's theory, the minimum level is a productivity of "1" which occurs when the costs of the search equal the expected benefits of the search. Thus, this is the level at which he argues that judges should find probable cause.

30. The output of a system is defined as "[t]he various useful goods or services that are either consumed or used in further production." PAUL A. SAMUELSON & WILLIAM D. NORDHAUS, ECONOMICS 747 (18th ed. 2004). In our case, the output of the system is the identification of criminals and the collection of evidence.

31. I am using the term "productivity" in the most basic sense: as a simple ratio of output to input. For example, assume a factory produces $10,000 worth of widgets in an hour, using one hundred workers being paid $20 per hour, raw supplies at the rate of $2,000 per hour, and equipment and capital which depreciates at $1,000 per hour. Thus, the factory spends $5,000 each hour and produces $10,000 worth of products, and has a productivity ratio of 10/5, or 2. There are a number of ways to increase the productivity of the factory: If the workers can be trained at negligible cost to produce $15,000 worth of widgets per hour using the same equipment, the productivity would increase to a ratio of 15/5 or 3. Or, if cheaper raw materials were used, salaries could be cut (without sacrificing output), or new, cheaper equipment could be installed, the same $10,000 of output could be produced at a cost of $4,000, for a productivity ratio of 10/4, or 2.5.

The productivity, X, will vary depending on the type of surveillance that is being conducted. But in order to determine the productivity for each type of surveillance, we must first define the costs and benefits of the equation.

A. Costs of Surveillance

The cost of a given type of surveillance can be divided into two categories: (1) the amount of resources (money, time, and equipment) that are used in conducting the surveillance; and (2) the degree to which the surveillance violates privacy interests. The expenses of the first category, known as "administrative costs," are borne directly by law enforcement.[32] The costs in the second category are external—that is, they are borne not by the actor conducting the surveillance, but by those who are the subjects of the surveillance.[33] The degree to which the surveillance violates privacy rights encompasses many different factors: the level of physical intrusion onto the suspect, the number of people affected by the search, the amount of time the search takes, the intimacy of the intrusion, and whether the search was conducted in public or in private.

Quantifying the value of an invasion of privacy is a challenging exercise. Lack of privacy creates at least two types of tangible economic costs: avoidance costs and defensive costs.[34] Avoidance costs are the losses that occur when a lack of privacy causes individuals to refrain from some socially useful (but perhaps embarrassing) activities, such as buying condoms or visiting a therapist.[35] Defensive costs denote the money people spend to protect their privacy when they feel their privacy is at risk—such as encoding e-mails, building high fences over their yards, or driving to meet someone in person rather than speaking to him over the telephone.[36]

In addition to these tangible costs, surveillance has an intangible cost because privacy has value as an intrinsic good. Privacy allows us to engage in many activities which may not have eco-

---

32. Song, *supra* note 10, at 16–17.

33. In a strict economic sense, it is the presence of these externalities that requires government regulation of surveillance in the first place.

34. Penney, *supra* note 10, at 492–94; Song, *supra* note 10, at 11–16.

35. Penney, *supra* note 10, at 492–93; Song, *supra* note 10, at 11–14.

36. Penney, *supra* note 10, at 493–94; Song, *supra* note 10, at 14–16.

nomic value but which create utility for those who engage in them, whether it is sunbathing naked in one's backyard or saying intimate things to a spouse over the telephone. Privacy is also critical to our political system, as an increase in privacy fosters communication and interaction among those who hold political views which may be unpopular in a given place or time.

Calculating the value of a privacy interest is further complicated by the fact that our conception of privacy is a moving target that evolves over time. Two hundred years ago, citizens had a very different conception of privacy than we do today.[37] In certain aspects, modern citizens experience—and therefore expect—greater privacy than citizens did in the past. Two hundred years ago, most Americans worked in the open fields, travelled from one place to another by walking or riding on horseback while exposed to the world, and engaged in private conversations only when visiting each other in their homes. Today, many Americans have a private workspace, most travel insulated in a private car, and almost everyone expects to be able to have a private conversation with anyone else in the country at any time or place that they choose. In other ways, however, our expectation of privacy is lower today than in the past. For example, given the ubiquitous nature of electric light, we no longer expect the darkness of nighttime to hide our activities.[38] We also know that, at any time, planes and satellites (whether used by the government or a private company like Google) can see and record the exterior of our homes and private land, and perhaps even our own movements. We expect to see surveillance cameras in private businesses and even in public spaces.[39] We are also in a privacy revolution of sorts with regard to data, as we struggle to understand how the Internet, YouTube, Facebook, and other social media sources are changing our perceptions about what information should be kept private and what information is fair game for public exposure.

---

37. *See generally* Ric Simmons, *Why 2007 Is Not Like* 1984*: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence*, 97 J. CRIM. L. & CRIMINOLOGY 531, 537–40 (2007).

38. *See, e.g.*, Kerr, *supra* note 6, at 486–87.

39. For a more detailed discussion of how technology has increased our privacy, see Simmons, *supra* note 37, at 536–40.

The Supreme Court has acknowledged that our standard of privacy can change as technology and society change.[40] Most notably, in *United States v. Kyllo*, the Court held that using a thermal imager to detect heat coming out of a home violated the homeowner's reasonable expectation of privacy, in part because the thermal imager was "not in general public use."[41] This holding implies that as a piece of technology becomes increasingly prevalent, society will adjust its expectations of privacy regarding government use of that technology. This principle was at work long before *Kyllo*. Fifteen years earlier, the Court held in *California v. Ciraolo* that an individual does not have a reasonable expectation of privacy in any part of his curtilage that was visible from the air—even though the individual had erected a ten-foot fence to hide it from anyone on ground level—because "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed."[42] This certainly would not have been the outcome one hundred years before *Ciraolo.*

Different forms of surveillance will cost different amounts in terms of resources spent and privacy lost. Thus, another challenge in comparing the costs of different types of searches is the difficulty of making the conversion between administrative costs and privacy costs. For example, wiretapping a telephone for thirty days is relatively inexpensive in terms of administrative costs, but it carries a high cost in terms of infringing on the suspect's privacy. Staking out a suspect's home for thirty days has a high administrative cost, but a relatively lower cost in terms of privacy intrusion. We therefore need to update our formula to separate these types of costs:

$$(C_A + C_P) * X = B$$

In other words, any given type of surveillance will have an administrative cost (C_A) and a privacy cost (C_P), as well as a level of productivity that makes the search more or less effective. Thus, there could be a trade-off between administrative costs and privacy costs, and in deciding which type of search is preferable, we should consider all of the costs of the search. Sometimes more money could be spent to carry out a search

40. *See infra* Part II.B.2.

41. 533 U.S. 27, 40 (2001).

42. 476 U.S. 207, 213–14 (1986).

that is less intrusive, and in those cases, we should decide whether the trade-off is worth it. But before we can make those decisions, we must first consider the other side of the equation: the expected benefits of the search.

B. Benefits of Surveillance

The benefit of a search is a function of two factors: the chance that the surveillance will be successful multiplied by the societal value of a successful surveillance. Both of these factors require a bit more explanation. First, there are two different ways that a search can be "successful": gathering evidence that helps police identify the perpetrator of a crime, and gathering evidence that can be used to help convict the perpetrator in court. A given type of surveillance might provide either or both of these results, and may be successful in either category to a different degree. For example, confidential informants may help law enforcement agents learn the identity of the perpetrator, and may provide probable cause to arrest him, but would not be used to help convict the perpetrator in court.[43] Conversely, once a suspect is in custody, law enforcement may conduct a number of searches of the defendant's home, car, computer, or office in order to gain more evidence to use against him.

For the purposes of our analysis, there is no reason to distinguish between the two different types of "successful" surveillance. Rather, what we care about is the probability that the surveillance will be useful in convicting the correct person in court, however that might happen. Thus, we can gauge the "successfulness" of a surveillance on a scale of zero to one—"zero" meaning that the surveillance has absolutely no chance of providing any useful information leading to the conviction of the perpetrator, and "one" meaning that the search will, with absolute certainty, reveal information that will be sure to convict the correct perpetrator. Although in the real world there will be no method of surveillance that can reach this ideal probability level, there are some that come close. Dashboard cameras on police cruisers that are activated during drunk-driving arrests, for example, have a very strong chance of pro-

43. *See* McCray v. Illinois, 386 U.S. 300 (1967) (stating that the government may rely on confidential information to support probable cause for a warrant, but need not produce the confidential informant at the suppression hearing).

viding nearly incontrovertible evidence that a particular defendant committed the crime: There will be video evidence of erratic driving, video evidence of the defendant emerging from the driver's seat, and video evidence of his performance on the field sobriety tests.[44] On a more Orwellian level, covert video cameras in every home would be almost certain to succeed in identifying and gathering incontrovertible evidence of many crimes, from domestic violence to illicit drug use. Of course, the extraordinary cost of such surveillance—both in terms of the administrative costs and the infringement on privacy—makes this method of surveillance extremely low in productivity.

In evaluating the "success rate" of different types of surveillance, we should also consider another type of success: Certain types of surveillance—what we could call proactive surveillance—can prevent a potential crime entirely or halt a crime in progress. In contrast, reactive surveillance, even when successful, will serve only to apprehend or convict a criminal who has already committed a crime. For example, wiretaps on telephones and *Terry* stops are proactive surveillance techniques, which are more likely to identify potential criminals before they have committed a more severe crime.[45] Plainly visible video cameras in public parks or in private stores can deter potential criminals from committing the crime in the first place, because the potential criminals realize their chances of apprehension and conviction are prohibitively high.[46] On the other hand, reactive surveillance techniques do not provide this benefit: Searches of a home after an arrest are likely to only find evidence of a crime that has already been committed—that is, the crime for which the suspect was originally arrested. For that matter, surveillance for most low-level drug crimes does nothing to prevent more serious crimes from occurring[47]—the

44. *See Dash-cam video: Maitland Vice Mayor Phil Bonus wobbling after DUI stop*, ORLANDO SENTINEL, Oct. 11, 2012, http://www.orlandosentinel.com/videogallery/72789605/News/Dash-cam-video-Maitland-Vice-Mayor-Phil-Bonus-wobbling-after-DUI-stop.

45. They are still caught committing a lesser crime—conspiracy instead of murder, or possession of a firearm instead of armed robbery.

46. *See* Steve Chapman, *Do cameras stop crime? What has been learned in Chicago*, CHI. TRIBUNE, Feb. 20, 2011, http://articles.chicagotribune.com/2011-02-20/news/ct-oped-0220-chapman-20110220_1_cameras-crime-justice-policy-center.

47. Of course, basic deterrence doctrine leads us to expect that any successful surveillance that leads to the conviction of a criminal will deter that criminal and

drugs have already been sold or possessed, and the successful surveillance after the crime has been committed can lead only to an arrest of the perpetrators after the crime has already occurred. From these few examples, however, it is already obvious that although proactive surveillance provides an extra benefit, it frequently comes at a greater cost—the surveillance may affect larger numbers of innocent people (as with *Terry* stops) or the surveillance may be more intrusive (as with video surveillance).

As for the second category of benefits, the societal value of any successful surveillance is dependent upon the severity of the crime being investigated. Professor Lerner adopts this method in his original formula.[48] Other scholars, such as Akhil Amar, have argued that the "reasonableness" standard in the Fourth Amendment ought to take the severity of crime into account.[49] Although courts have not incorporated this factor into the definition of reasonableness, it is sensible to include the severity of the crime when conducting a cost-benefit analysis of any surveillance: The more severe the crime that is being investigated, the greater the societal benefit of the surveillance. For example, we would be more willing to bear a high-cost surveillance to gather evidence in a terrorism investigation than we would to gather evidence in a shoplifting investigation.

Determining the severity of the crime being investigated is actually one of the easiest aspects of our project, because the criminal justice system already provides us with an unambiguous ranking of each crime on the books. Thus, we can use the expected sentence after conviction as a proxy for the severity of the crime: The higher the expected sentence, the greater the societal benefit in a successful search.

Given this definition of "benefits," we can now rewrite our formula as follows:

$$(C_A + C_P) * X = E(S_1) + P(S_2)$$

In this formula, "E" is the percentage chance that the surveillance results in successfully providing information that will

---

others from committing the crime in the future, but that type of indirect crime prevention is true for every type of surveillance. Proactive crime surveillance is a more direct method of deterring crime altogether or preventing a more serious crime from occurring.

48. *See supra* notes 10, 23–25 and accompanying text.

49. *See supra* note 26 and accompanying text.

lead to the conviction of the perpetrator (whether by correctly identifying him or by gathering admissible evidence against him), "P" is the percentage chance that the surveillance will proactively prevent a crime, "S_1" is the multiplier based on the seriousness of the crime for which the evidence is being gathered, and "S_2" is the multiplier based on the crime which is being prevented. In the case of a reactive search, P will be zero. In the case of many proactive surveillance techniques, S_1 and S_2 will be identical—for example, video cameras on street corners known for drug dealing both will gather evidence against drug dealers and help to prevent the crime of narcotics trafficking. In such cases, P and E will be inversely related—that is, the greater the chance is that the surveillance technique will prevent the crime altogether, the lesser the chance is that the surveillance technique will successfully gather evidence about the crime, because the crime is much less likely to occur. In other cases, S_2 will be a more severe crime than S_1, and the success in gathering information leading to arrest and conviction will directly affect the success of preventing the more serious crime. For example, a *Terry* stop might reveal a firearm carried by a suspect who was intending to rob a jewelry store later in the day. In those cases, P and E will be nearly identical.

II. APPLYING THE MODEL

Now that we have a rough formula in place, we can begin to search for areas where we can achieve an increase of productivity. These increases occur when we are able to decrease the variables on the left side of the equation while holding the right side of the equation constant, or when we increase the variables on the right side of the equation while holding the left side of the equation constant. We start with the first variable in the equation—the administrative costs of searches—to consider how technology can make surveillance less expensive for law enforcement.

A. Lowering the Administrative Cost of Surveillance

Before considering how technological advances can increase the productivity of surveillance, we must acknowledge that many new technologies have *decreased* surveillance productivity by making it harder to detect criminal activity. The best example of such a technological advance is the invention of tele-

phone in 1876. The telephone has probably done more to decrease the productivity of law enforcement surveillance than any other single device in history. Ever since the telephone became ubiquitous—and ever since Congress decided to prohibit warrantless surveillance of telephonic communications in 1934[50]—criminals have been able to use the telephone to shield their communications. They use it to plan with coconspirators, transfer funds from place to place, or facilitate interactions with "customers" for drug sales, prostitution, and gambling activities. Before the advent of the telephone, all of these communications either had to take place in person, requiring meetings in public places or travelling on public streets, or by writing (a much less efficient method which leaves a permanent record of the illicit transactions). Once these communications could be accomplished indoors, safe from the eyes of investigating officers, the cost of surveillance for many crimes increased substantially even as its success rate dropped significantly.

Over the past thirty years, the widespread use of computers and Internet communications has once again dramatically lowered the productivity of law enforcement surveillance. Courts (and Congress) are still working through the extent to which these activities implicate the Fourth Amendment,[51] but the ability of

---

50. The Supreme Court, of course, originally did *not* believe that surveillance of telephone communications required a warrant. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928). This was before the "reasonable expectations" test of *Katz v. United States*, but the Court did note in *Olmstead* that it if an individual "project[s] his voice to those quite outside" his house, it is not "reasonable" to conclude that the Fourth Amendment protects his communication. *Id.* Congress disagreed, however, issuing a blanket protection for all telephone communications with the Federal Communications Act of 1934. When the Court finally revisited the issue of protection for telephone communications in *Katz*, it held that individuals did indeed have a reasonable expectation of privacy in those communications, even if they were made from a public phone booth. *Katz*, 389 U.S. 347, 351 (1967).

51. *See, e.g.*, United States v. Heckenkamp, 482 F. 3d 1142, 1146 (9th Cir. 2007) (holding that an individual has a "reasonable expectation of privacy in his computer"). *But see* United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (holding that there was no reasonable expectation of privacy in "transmissions over the Internet or e-mail that have already arrived at the recipient"). The prime example of Congress's efforts in this domain is the Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.), which amended the Wiretap Act at 18 U.S.C. §§ 2510–2522 to include electronic communications. That Congress has continued to grapple with the Fourth Amendment implications of electronic surveillance is evidenced by the fact that it has significantly amended the ECPA four times in the last twenty years, in the Communications Assistance for Law Enforcement Act of

criminals to store, transfer, and encrypt data has certainly made surveillance of their activities more expensive and less successful.

But other forms of new technology have increased the productivity of surveillance by providing law enforcement officers with new tools to conduct their investigations. Many of these new technologies provide the same success rate as the traditional surveillance that they replace, but they represent an unambiguous improvement in Fourth Amendment productivity because they provide that identical benefit more cheaply than before. Nonetheless, some of these methods present a challenge for our analysis: They are less costly in a monetary sense but more costly in terms of their effect on our privacy. This category of surveillance technologies gives us the first test of our formula, because it requires us to measure two very different types of costs against each other.

1. Cheaper Surveillance That Is No More Intrusive

Many new technologies increase the efficiency of certain types of surveillance by lowering the administrative cost of the surveillance with no loss of benefit and no increase in the cost in terms of privacy. For example, computerized recordkeeping and modern data search techniques allow police officers to investigate many crimes instantaneously from the dashboard computer of their cars. If they suspect that a car they see on the road might be stolen, police officers can punch in the license plate number and quickly connect to the appropriate database. If they suspect that an individual whom they have pulled over has an outstanding warrant or a suspended driver's license, they can check local, state, and federal records within a matter of minutes.[52] Similar technology allows police to check the fingerprints of suspects to see if they have committed other

---

1994 (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001–1010), the United and Strengthening American by Providing Appropriate tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (2001) and its reauthorization in 2006, and the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FISA Amendments Act), Pub. L. No. 110-261, 122 Stat. 2436 (codified in scattered sections of 8, 18, and 50 U.S.C.).

52. *See* Declan McCullagh, *Police blotter: When can cops run license-plate searches?*, CNETNEWS, Sept. 15, 2006, http://news.cnet.com/police-blotter-when-can-cops-run-license-plate-searches/2100-1030_3-6116296.html.

crimes, or have outstanding warrants under different names.[53] For more serious crimes, DNA evidence can be gathered from crime scenes and compared against DNA of known suspects[54]—provided the police are able to acquire DNA from those suspects.

2. Cheaper Surveillance That (May Be) More Intrusive

Although many modern surveillance techniques represent an absolute increase on our productivity scale, others are more ambiguous: They are less expensive than the surveillance method they are replacing, but they have the potential to be more intrusive on our privacy. In other words, the new method of surveillance is cheaper but possibly more intrusive. Law enforcement agencies will be overly sympathetic to these surveillance methods, because the privacy costs of these methods is externalized (that is, the privacy cost is not borne directly by the law enforcement agency and is therefore not part of their internalized cost-benefit analysis). On the other hand, courts tend to be overly critical of these surveillance methods, ignoring the cost savings on the financial side and focusing only on the privacy costs, as the role of courts in interpreting the Fourth Amendment does not take financial costs into account. Our role in attempting to calculate and compare the productivity of different types of surveillance is to try to balance both types of costs against each other.

As noted above, some people may disagree with this goal because they believe that no amount of cost savings to law enforcement is worth any diminution of privacy rights. This position, although theoretically pure, will make it difficult to experiment with many new technologies, from DNA searches, to GPS tracking devices, to cameras in public places. Under the absolutist position, any new type of surveillance that has a danger of infringing on our privacy would be unacceptable, regardless of how much more efficient it is. The real question should be one

---

53. *See* Maureen Mespell, *Wireless Fingerprinting Shortens ID Time*, INCNOW, Aug. 28, 2012, http://www.indiananewscenter.com/news/local/Wireless-Fingerprinting-Shortens-ID-Time-167757455.html.

54. *See* Nicholas Wade, *FBI Set To Open Its DNA Database for Fighting Crime*, N.Y. TIMES, Oct. 12, 1998, http://www.nytimes.com/1998/10/12/us/fbi-set-to-open-its-dna-database-for-fighting-crime.html?pagewanted=all&src=pm.

of degree: How much more intrusiveness can be exchanged for cost savings? This question needs to be answered on a case-by-case basis, keeping both types of costs in mind.

Balancing the two very different types of costs could be tricky on the margins, but in extreme situations it is not so challenging. On one end of the spectrum, law enforcement agents could—at a relatively low administrative cost—covertly install microphones and video cameras inside the home and office of every individual they suspect of criminal activity. The rest of the investigation would simply involve watching and listening to the suspect's everyday movements until the agents acquired enough evidence to convict the suspect in court (or until they were convinced of his innocence, in which case they would simply covertly retrieve the devices and move on). Although this process would save money in terms of investigative resources, most people would be unwilling to trade off this amount of privacy in exchange for the cost savings to law enforcement.

On the other end of the spectrum is the DNA database mentioned earlier.[55] Currently, law enforcement agents collect a DNA sample from individuals who are convicted of a felony[56] and enter it into a national database. As of 2010, this database contained nearly eight million unique samples from offenders.[57] Law enforcement officers can search the database every time a DNA sample is recovered from a crime scene, a relatively inexpensive type of surveillance which has a significant chance of both identifying the perpetrator and providing powerful evidence in court. This surveillance technique does infringe on privacy interests—that is, there is a privacy cost to individuals whose DNA samples are stored in a federal database—but the privacy cost is small (and mostly affects convicted felons, who possess fewer privacy rights in the first place).[58] Thus, this is a trade-off that many individuals will be willing to make (indeed, it is a trade-off that we as a society have already made, with little public outcry) For their part, circuit courts have routinely held

55. *See supra* note 54 and accompanying text.

56. Candice Roman-Santos, *Concerns Associated With Expanding DNA Databases,* 2 HASTINGS SCI. & TECH. L.J. 267, 283 (2010) (noting all fifty states require DNA collection for at least some felonies).

57. *Id.* at 274.

58. *See, e.g.,* Florence v. Burlington, 132 S. Ct. 1510 (2012) (allowing strip searches of individuals who have been arrested).

that taking and storing DNA samples from convicted felons does not violate the Fourth Amendment.[59]

At some point, however, the intrusiveness of DNA collection may well outweigh the decreased cost and increased efficiency of this type of surveillance. Some states go beyond gathering evidence from convicted felons and include all those who are arrested for felonies,[60] or who are convicted of certain misdemeanors.[61] A recent federal law allows for DNA collection from undocumented immigrants, even if they are not suspected of any crime.[62] As more and more innocent individuals are swept up into the database, there may be a point at which the existence and use of the database becomes too intrusive to justify the cost savings.

In between the two extremes of covert video surveillance inside homes and gathering DNA from convicted felons lies a vast array of modern surveillance techniques. For example, law enforcement officers can use "pen register" devices to monitor and record the telephone numbers of all of the outgoing and incoming calls for a phone line, or the e-mail addresses of all of the outgoing and incoming e-mails for an e-mail service.[63] The Supreme Court has held that this conduct does not constitute a "search" under the Fourth Amendment,[64] although the surveillance is (very lightly) regulated by statute.[65]

---

59. *See, e.g.*, Sanchez v. Goord, 430 F.3d 652 (2d Cir. 2005); Padgett v. Donald, 401 F.3d 1273 (11th Cir. 2005).

60. Roman-Santos, *supra* note 56, at 283. Many of these states allow the individual to apply for expungement from the database if they are acquitted or the charges are dismissed, but few states expunge the record automatically. *Id.*

61. *Id.*

62. *Id.* at 283–84. Nonetheless, as of 2009, Immigration and Customs Enforcement was not collecting this information. *Id.*

63. Police officers use a "pen register" to record the phone number or email address of outgoing calls and emails, and a "trap and trace" device to record the phone number or email address of incoming calls and emails. These terms refer to the devices originally used on telephone lines. *See In Re* United States, 610 F.2d 1148, 1151 (3d Cir. 1979). In modern times, law enforcement officers install a "sniffer" onto an e-mail account, which involves a piece of software that only retrieves the "to" and "from" address lines of all incoming or outgoing e-mails—this is known as a "pen register" device. *See* ORIN S. KERR, COMPUTER CRIME LAW 499–500 (2d ed. 2006).

64. Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

65. *See* 18 U.S.C. §§ 3122(b)(2) (2006) (allowing law enforcement to install pen/trap devices and collect address information upon a showing that the "infor-

Pen registers are a very efficient way for law enforcement to learn with whom a suspect is communicating. In some sense, pen register devices merely neutralize the technological advantages that criminals have enjoyed since the invention of the telephone.[66] Once the telephone—and then e-mail, and then the cell phone—became commonplace, the surveillance method of following suspected criminals in public (in itself a relatively expensive activity) became far less fruitful. Pen register devices not only remove the advantage that criminals have had for the past century and a half, they are also far less expensive than personal surveillance.

But of course pen register devices carry a significant cost in terms of privacy. Although the Supreme Court has held that individuals do not possess a reasonable expectation of privacy in the phone numbers we dial[67] (and therefore presumably not in the addresses of the e-mails we send, or the IP addresses of the websites we visit[68]), most Americans would probably feel their privacy was infringed upon if they learned the government was recording this information about their communication habits.

Cameras in public places provide another example of the trade-off between financial cost and intrusiveness. Theoretically, these cameras do no more than record what could be observed by law enforcement officials personally observing the area. Thus, on one level, they are no more intrusive than a police officer strolling through a park or down a sidewalk. Each camera is able to provide the identical amount of surveillance as a live police officer, and at a small fraction of the cost. In fact, the camera will result in a higher level of return for our first measure of output, because it will provide law enforcement with a nearly incontrovertible record of what it sees. It cannot be impeached on cross-examination, nor will its memory fade.

---

mation likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency").

66. *See supra* note 50 and accompanying text. Criminals could communicate by mail, of course, but that was a relatively slow form of communication, and the address on the letter was also in plain view of any investigating law enforcement officer. *See Ex parte* Jackson, 96 U.S. 727, 727 (1877) (holding that the Fourth Amendment does not bar police from reading the addresses off of envelopes in the mail system).

67. *Smith*, 442 U.S. at 745–46.

68. *See* United States v. Forrester, 495 F.3d 1041, 1048–50 (9th Cir. 2007).

It is true there is some diminution in our second measure of output because the presence of a police officer is more likely to deter a crime from ever happening than the presence of a video camera, but a video camera provides some amount of deterrent value in itself. Thus, on first analysis, public video surveillance appears to offer an increase in surveillance productivity. Consider again our formula:

$$(C_A + C_P) * X = E(S_1) + P(S_2)$$

With public video surveillance, there would be a much lower C_A, an identical C_P, a slightly higher $E(S_1)$, and a slightly lower $P(S_2)$. On balance, replacing roving police officers with multiple video cameras appears to increase the productivity of surveillance—that is, to make the equation balance, X must increase dramatically.

But here, the calculations can become tricky. Although the installation of one video camera in a public park may be no more intrusive than an officer on foot patrol, what about the installation of ten video cameras around the park? What about the installation of enough video cameras to ensure that every square foot of the park is being monitored? What about installing video cameras to monitor every public place available—inside the lobbies of public housing, around the campuses of public universities, on poles next to public sidewalks and roads—all feeding into a master control room where police officers watch everything that is occurring in the city's public places? If one assumes that the cost to privacy is still constant—because this is no more intrusive than having thousands of police officers roaming the city and observing behavior—then the productivity of this type of surveillance is tremendous. There is almost no crime that can occur in any public place in the city without a permanent, nearly irrefutable record being made of the criminal activity. But the assumption about the cost being held constant becomes increasingly harder to accept as the video surveillance becomes increasingly ubiquitous.

The Supreme Court recently dealt with this problem in a slightly different context: tracking suspects in automobiles. Once again, under an initial analysis, this appears to be an area where technological progress has unequivocally increased the productivity of surveillance. Decades ago, police officers conducting this surveillance would personally follow suspects in a car. This was an expensive form of surveillance in terms of manpower. It also ran the risk of failure, either because the suspect would alter his behavior so as not to reveal criminal activ-

ity or because the police might lose the suspect during the surveillance. As electronic tracking became more feasible, police officers implanted "beepers" onto items that the defendant would place in his car.[69] These devices emitted a signal which allowed the police to track a car from a distance where they would remain undetected and yet ensure they would not lose the subject.[70] The use of the beepers represented a slightly higher administrative cost, but no greater infringement on privacy, and offered a much greater chance of successful surveillance. Thus, while C_A (the administrative cost) increased slightly, $E(S_1)$ (the percentage chance that the surveillance will provide information leading to the successful conviction of a perpetrator, multiplied by the seriousness of the crime) increased even more, while the other terms remained constant—again showing an increase in surveillance productivity.

As technology progressed, police began using GPS devices to track vehicles. Once these devices were covertly placed on a suspect's automobile, a police officer would not have to follow the suspect at all. Instead, the GPS device would record all of the suspect's movements and then report them electronically.[71] This lowered the administrative cost of the surveillance dramatically and offered an even greater chance of success in providing evidence of a crime because there was no chance of losing track of the suspect once the GPS device was in place and only a very small chance that the device would be detected.

As with video surveillance, however, there is a point at which many would contend that continuous GPS monitoring becomes *more* intrusive than its old-fashioned analogue. The Supreme Court discussed this very issue in *United States v. Jones*.[72] Government agents installed a GPS device to the undercarriage of the defendant's car and monitored her vehicle's movements for twenty-eight days.[73] A majority of the Court held that this action violated the Fourth Amendment because law enforcement physically intruded onto the defendant's property by attaching

69. *See* United States v. Karo, 468 U.S. 705, 708 (1984); United States v. Knotts, 460 U.S. 276, 278–79 (1983).

70. *See Knotts*, 460 U.S. at 278–79.

71. United States v. Jones, 132 S. Ct. 945, 947 (2012).

72. *Id.*

73. *Id.* at 948.

the device to her car.[74] But this holding merely dodged the most significant issue in the case: To what degree did the continuous monitoring of the defendant's vehicle intrude onto her privacy? Because the Court was analyzing this case for the purposes of the Fourth Amendment, Justice Alito's concurrence in the judgment stated this issue in terms of the *Katz* test: Did the continuous monitoring of the defendant's vehicle violate an expectation of privacy that society is prepared to recognize as reasonable?[75] For the purposes of our discussion, however, we need to rephrase the question somewhat to determine whether vehicular surveillance using a GPS device is a more productive search than personally following the car. Thus, we must compare the two types of surveillance and ask whether the decrease in administrative cost and the increase in the chance that the surveillance will successfully turn up evidence of a crime outweighs the increased cost in loss of privacy. In mathematical terms, if $-\Delta C_A + \Delta E(S_1) > \Delta C_P$, then the GPS surveillance is a more productive search than in-person surveillance.

Because of the difficulties in quantifying the cost to privacy and the chances of success, this is a difficult calculation. To make this calculation, a person has to answer a number of questions. How intrusive in fact is this type of monitoring? What is the "exchange rate" between this extra intrusiveness and the savings in administrative costs? What is the exchange rate between this extra intrusiveness and the more effective law enforcement that the surveillance provides? These questions involve subjective values, and so reasonable people will disagree as to the level of intrusiveness involved and the proper "exchange rates" for the equation. But by framing the question in this way, we can at least engage in a discussion which recognizes all of the important values at stake.

Unfortunately, this is not at all the way that the courts have been framing the discussion. For the judges analyzing this surveillance, there is only one value at stake: the level of intrusiveness. This is because under the *Katz* test, if the level of intrusiveness surpasses a certain level, the surveillance is a search.[76] The increased benefits of the surveillance (in terms of

74. *Id.* at 949–50.

75. *Id.* at 958 (Alito, J., concurring in the judgment).

76. *See* Katz v. United States, 389 U.S 347, 360–62 (1967) (Harlan, J., concurring).

increased chances of successfully gathering evidence) are ignored. And the decreased administrative costs of the surveillance are placed on the wrong side of the equation: Instead of *counterbalancing* the extra intrusiveness of the surveillance, they *contribute* to the perceived intrusiveness of the surveillance. In *Jones*, Justice Alito notes:

> In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap.[77]

The fact that GPS surveillance is dramatically easier and cheaper than traditional surveillance was relevant to Justice Alito only in one way: it tended to show that GPS surveillance violates society's reasonable expectation of privacy. The lower administrative cost made it more likely that the intrusiveness of the search would be unacceptably high, because "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[78]

As we will see below,[79] this analysis is flawed in that it does not take into account the possibility that society's reasonable expectation of privacy may change as GPS devices become widespread, just as it did when airplanes became commonplace.[80] But the more fundamental flaw in this analysis is that it

---

77. 132 S. Ct. at 963–64 (Alito, J., concurring in the judgment) (citations omitted).

78. *Id.* at 964. Interestingly, Justice Alito's analysis did not ignore the severity of the crime; he noted that for minor offenses, an individual would not expect the government to conduct such an extensive surveillance, but "prolonged GPS monitoring in the context of investigations involving extraordinary offenses" may be constitutional because society would expect such comprehensive surveillance for an "extraordinary offense" even if the police used nothing but traditional methods. *Id.*

79. *See infra* Part II.B.2.

80. *See supra* notes 41–42 and accompanying text.

is stuck in a zero-sum world, where courts must ensure that neither the police nor the criminals get an "unfair" advantage in the game of cops and robbers. Decisions by the lower courts reflect this same mentality. Judge Ginsburg of the D.C. Circuit, who wrote the lower court opinion in the *Jones* case,[81] noted that GPS devices should be more strictly regulated than visual surveillance precisely *because* they are so inexpensive:

> Continuous human surveillance for a week would require all the time and expense of several police officers, while comparable photographic surveillance would require a net of video cameras so dense and so widespread as to catch a person's every movement, plus the manpower to piece the photographs together. Of course, as this case and some of the GPS cases in other courts illustrate, prolonged GPS monitoring is not similarly constrained. On the contrary, the marginal cost of an additional day—or week, or month—of GPS monitoring is effectively zero. Nor, apparently, is the fixed cost of installing a GPS device significant; the Los Angeles Police Department can now affix a GPS device to a passing car simply by launching a GPS-enabled dart. For these practical reasons, and not by virtue of its sophistication or novelty, the advent of GPS technology has occasioned a heretofore unknown type of intrusion into an ordinarily and hitherto private enclave.[82]

Judge Kozinski of the Ninth Circuit voiced a similar objection to GPS monitoring in his dissent in *United States v. Pineda-Moreno*:

> A small law enforcement team can deploy a dozen, a hundred, a thousand such devices and keep track of their various movements by computer, with far less effort than was previously needed to follow a single vehicle. The devices create a permanent electronic record that can be compared, contrasted and coordinated to deduce all manner of private information about individuals. By holding that this kind of surveillance doesn't impair an individual's reasonable expectation of privacy, the panel hands the government the

81. The case name was *United States v. Maynard* at the circuit court level but was decided as *United States v. Jones* by the Supreme Court.

82. United States v. Maynard, 615 F.3d 544, 565 (D.C. Cir. 2010) (citations omitted).

> power to track the movements of every one of us, every day of our lives.[83]

These judges argue that at some point this surveillance becomes so inexpensive that it will give the police too much information, and the information will be recorded and coordinated too efficiently. This may be because, as suggested above, judges want to maintain a zero-sum game where neither the police nor the criminals are given an unfair advantage. But there is also a more legitimate justification for this argument: the theory that expensive surveillance methods are to some extent self-regulating, whereas cheaper surveillance methods are not, therefore requiring the courts to intervene. In other words, if a surveillance method is very expensive (such as following a suspect in person twenty-four hours a day for a month), police will not choose to undertake the surveillance unless they already have substantial evidence that the defendant is involved in serious criminal activity. If a surveillance method is relatively cheap (such as placing a GPS onto someone's car and then downloading data after a month), police will feel free to engage in that surveillance on the smallest level of suspicion, or perhaps upon no suspicion at all. Justice Harlan expressed this concern in his dissent in *United States v. White*.[84] In *White*, the Court held that an informer with an electronic listening device that transmitted a conversation to the police was the equivalent of the informer reporting all he heard to the police after the conversation was over, because in both cases the defendant was trusting his words to a third party.[85] In the plurality's analysis, the electronic device was simply an improvement, because it involved no further infringement on privacy rights, but instead provided a more accurate record and more effective evidence at trial.[86] Our own economic analysis agrees with the

---

83. United States v. Pineda-Moreno, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, J., dissenting); *see also* People v. Weaver, 12 N.E.2d 1195, 1199 (N.Y. 2009) ("The potential for a similar capture of information or 'seeing' by law enforcement would require, at a minimum, millions of additional police officers and cameras on every street lamp.").

84. 401 U.S. 745, 768 (1971) (Harlan, J., dissenting).

85. *Id.* at 751.

86. *Id.* at 752 ("If the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither should it protect him when that

plurality: The minor extra expense involved in using an electronic transmitter (or recorder) is more than evened out by the greater effectiveness of the evidence at trial. But Justice Harlan feared that the cheaper, more accurate electronic device would lead to more widespread—and therefore more indiscriminate—use of eavesdropping. He stated that the plurality was erroneously holding that "uncontrolled consensual surveillance in an electronic age is a tolerable technique of law enforcement, given the values and goals of our political system."[87] One of the "controls" that was missing was the expense and the risk of having a human informant testify at trial. This expense and risk would ensure that the police only used informants when they already had good reason to believe that the suspect was guilty. Under this argument, the administrative cost of surveillance performs a valuable "channeling" function, which naturally leads law enforcement to regulate its use.[88]

This argument has intuitive appeal, but in reality the relationship between the expense of the surveillance method and the level of intrusion it involves is too crude to be relied upon as a guide. Courts should not assume that cheaper surveillance necessarily means more widespread surveillance, nor that more widespread surveillance necessarily means that privacy is being infringed upon to the extent that a warrant should be required. Furthermore, courts should not ignore the fact that cheaper surveillance leads to a more productive surveillance method. In this sense, Justice Alito, Judge Ginsburg, and Judge Kozinski have the analysis backward: The fact that a certain surveillance method is cheaper, more accurate, and more efficient is a positive factor in evaluating this surveillance method, and—all else being equal—should lead courts to encourage its use.

This does not mean that the result in *Jones* was incorrect. It could very well be that the "mosaic" of information[89] provided

---

same agent has recorded or transmitted the conversations which are later offered in evidence to prove the State's case.") (citations omitted).

87. *Id.* at 785 (Harlan, J., dissenting).

88. Thanks to Professor Orin Kerr for pointing out this argument and suggesting this terminology.

89. The "mosaic" theory posits that although acquiring one small item of information may not constitute a "search," acquiring hundreds or thousands of similar items of information and piecing them together could give the police enough in-

by continuous GPS monitoring represents such a significant intrusion into our privacy that it outweighs both the considerable savings in administrative costs and the increase in a chance of a successful search. If so, GPS monitoring is a less productive method of surveillance and should be discouraged. Courts should answer this question not by simply assuming that a lower administrative cost for the method of surveillance potentially will lead to an unacceptable level of intrusion, but by examining the actual level of intrusion that is currently occurring when law enforcement engages in this method of surveillance. When courts use administrative cost as a proxy for intrusiveness and ignore the cost savings and increased effectiveness that accompany the lower administrative cost, they fail to take into account all of the necessary factors to properly reach that conclusion.

This analytical failure is even more significant because there is much unresolved gray area surrounding this issue. The "physical trespass" issue that guided the majority decision in *Jones*[90] is a relatively easy obstacle to overcome for the government. Law enforcement will either monitor suspects using the car's own GPS device[91] or program small drones to follow the car from the air—neither of which would run afoul of the majority decision in *Jones.* At that point, Justice Alito's analysis will almost certainly be the law that governs the extent to which law enforcement can use electronic devices to track vehicular movements. A vast middle ground exists between the one-trip electronic surveillance held to be constitutional in *Knotts* and the twenty-eight day continuous monitoring held to be a search in *Jones*. This middle ground will require a careful balancing of all the important interests at stake. In deciding these close cases, the courts will be considering only one factor in the equation—the intrusion on the driver's privacy. This will

---

formation to violate a suspect's reasonable expectation of privacy. *See* Bethany L. Dickman, Note, *Untying* Knotts: *The Application of Mosaic Theory to GPS Surveillance in* United States v. Maynard, 60 AM. U. L. REV. 731, 733 (2011); Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment,* 55 UCLA L. REV. 409, 421 (2007).

90. United States v. Jones, 132 S. Ct. 945, 949–53 (2012).

91. *Jones*, 132 S. Ct. 945, 964 (Alito, J., concurring in the judgment).

result in overly restrictive rules—and lower productivity—for this type of surveillance.

B. Surveillance Techniques Which Are as Effective but Less Intrusive

Another way to increase productivity is to develop surveillance techniques that provide the same level of output but cost less in terms of privacy costs. In general, law enforcement agencies will be indifferent as to whether to use these methods, or equally expensive but more intrusive methods because once again they are indifferent to the "savings" in terms of the cost to privacy.

1. Binary Surveillance

Binary surveillance refers to a surveillance method that only produces one of two results: positive (meaning that illegal activity has been detected) or negative (meaning that illegal activity has not been detected).[92] The surveillance provides no other information about the person or area being monitored, and so represents a relatively minor intrusion on the target's privacy. In fact, the Supreme Court has held that binary surveillance does not even count as a "search" under the Fourth Amendment because it does not infringe on an expectation of privacy that society is prepared to recognize as legitimate.[93]

A simple example of a binary surveillance technique is a field test for narcotics. If a law enforcement officer reasonably believes that a certain substance may be narcotics, she can legally seize a very small amount of the substance and mix it with certain chemicals.[94] If the substance tests positive for narcotics, the law enforcement officer knows that the substance is in fact con-

---

92. *See* Timothy C. MacDonnell, *Orwellian Ramifications: The Contraband Exception to the Fourth Amendment*, 41 U. MEM. L. REV. 299, 302 & n.15 (2010) (using the term "contraband exception," rather than "binary search," because a binary search may not involve contraband and therefore would be covered by the Fourth Amendment); Ric Simmons, *The Two Unanswered Questions of* Illinois v. Caballes*: How to Make the World Safe for Binary Searches*, 80 TUL. L. REV. 411, 424 (2005).

93. *See, e.g.*, Illinois v. Caballes, 543 U.S. 405, 409 (2005) (finding that conducting a drug sniff during a lawful traffic stop was not unreasonable search and seizure); United States v. Jacobsen, 466 U.S. 109, 123 (1984) (noting that "Congress has decided . . . to treat the interest in privately possessing cocaine as illegitimate"); United States v. Place, 462 U.S. 696, 707 (1983) (holding that subjecting luggage to a canine "sniff test" does not constitute a search under the Fourth Amendment).

94. *See* United States v. Jacobsen, 566 U.S. 109, 111–12, 117–18 (1984).

traband and that a crime has occurred. If the substance tests negative, the officer knows nothing about the substance other than the fact that it is not an illegal drug. Therefore, because the suspect has no legitimate interest in possessing contraband, assuming other procedural prerequisites are satisfied, the surveillance does not implicate the Fourth Amendment[95]—the officer either learns nothing at all about the defendant or learns that the defendant is engaging in illegal activity.

Under our analysis, binary surveillance would theoretically provide us with a very high level of surveillance productivity because the cost in terms of intrusiveness is almost nothing. In practice, however, there are a number of complications when applying our model to binary surveillance. First, simply because the surveillance does not implicate the Fourth Amendment does not mean it has no cost in terms of privacy intrusion. For example, a drug-sniffing dog that approaches an individual's belongings, home, or person represents some level of intrusion,[96] even if there is no chance that the surveillance will reveal any legitimate information about your possessions. Thus, the binary surveillance itself creates some privacy cost. Furthermore, many types of binary surveillance will lead to a more intrusive search. A drug-sniffing dog alerting to a suspect's car or suitcase will trigger a thorough physical search. If the drug dog has a very low false positive rate, then it would result only in a more intrusive search on those rare occasions when contraband actually was present. Thus, this extra privacy cost would be relatively low. But in practice this is not the case: According to some estimates, when drug dogs alert, they are correct only between 26% and 44% of the time.[97] Therefore, in

95. *Jacobsen*, 466 U.S. at 126.

96. *See, e.g.*, Jardines v. State, 73 So. 3d 34, 48–49 (Fla. 2011) ("Such a public spectacle unfolding in a residential neighborhood will invariably entail a degree of public opprobrium, humiliation and embarrassment for the resident, whether or not he or she is present at the time of the search, for such dramatic government activity in the eyes of many—neighbors, passers-by, and some in the public at large—will be viewed as an official accusation of crime. And if the resident happens to be present at the time of the 'sniff test,' such an intrusion into the sanctity of his or her home will generally be a frightening and harrowing experience that could prompt a reflexive or unpredictable response.") (citation omitted).

97. *See* Laurence Hammock, *Drug-sniffing dog's accuracy questioned*, ROANOKE TIMES, June 6, 2012, http://www.roanoke.com/news/roanoke/wb/309801 (finding that drug sniffs have only a 26% accuracy); Dan Hinkel and Joe Mahr, *Tribune*

calculating the total privacy costs of binary surveillance, the privacy cost of a physical search times the percentage chance that the dog has improperly alerted must be added to the equation.

Finally, there is one more element to our total privacy cost calculation: a *correct* positive alert will also result in a physical search. Thus, we must include the privacy cost of a physical search multiplied by the percentage chance that contraband actually is present. Although the Supreme Court has stated that individuals who possess narcotics have no legitimate expectation of privacy in the contraband they carry,[98] a physical search that finds this contraband will involve a significant level of intrusion and will reveal other information about the suspect that *is* protected.

Accordingly, the privacy cost of using a drug-sniffing dog is:

C_P(drug dog sniff) + (false positive rate)*C_P(physical search) + (correct positive rate)* C_P(physical search)

To measure the overall productivity of binary searches, we also need to determine the *administrative* cost of the surveillance and, on the other side of the equation, the expected benefits of the surveillance. In the case of drug-sniffing dogs, the administrative costs can be calculated relatively easily. An officer with a drug-sniffing dog costs more than an officer working alone—trained drug-sniffing dogs cost between $5,000 to $8,000 up-front and then approximately $600 per year to maintain.[99] Drug-sniffing dogs make up for this higher cost, however, with their ability to quickly scan through many suitcases or cars, allowing them to conduct their surveillance much more quickly than an officer would be able to working alone, searching by hand. Given this greater efficiency, a police officer with

---

analysis: Drug-sniffing dogs in traffic stops often wrong, CHI. TRIB., Jan. 6, 2011, http://articles.chicagotribune.com/2011-01-06/news/ct-met-canine-officers-20110105_1_drug-sniffing-dogs-alex-rothacker-drug-dog (finding that drug sniffs have only a 44% accuracy).

The Supreme Court is currently deciding whether a positive alert by a drug-sniffing dog is sufficient to provide probable cause, given this high false positive rate. *See* Harris v. State, 71 So. 3d 756 (Fla. 2011), *cert. granted sub. nom.* Florida v. Harris, 132 S. Ct. 1796 (2012).

98. *See Jacobsen*, 466 U.S. at 123.

99. *See* Ed Richter, *Sheriff unleashes drug-sniffing dogs, Tango and Kash*, PULSE J., Dec. 5, 2009, http://www.pulsejournal.com/news/news/local/sheriff-unleashes-drug-sniffing-dogs-tango-and-k-1/nM7Ds//.

a drug-sniffing dog can conduct an individual search for far less money than a police officer without a drug-sniffing dog.

Unfortunately, measuring the expected effectiveness of drug-sniffing dogs is challenging. Most of the existing studies focus on the chance of a false positive: that is, whether or not a drug-sniffing dog will alert when there is no contraband present. To measure the effectiveness of the drug-sniffing dogs, however, we need to know the rate of false negatives—how often the drug-sniffing dog does *not* alert when contraband is in fact present. Finally, we need to multiply the chance of a successful search by the severity of the crime—in this case, drug possession or drug trafficking, depending on the amount of contraband which is found.

Of course, quantifying all of this data would be nearly impossible. But this analysis is still useful because it allows us to make rough comparisons between different types of surveillance. In the context of investigating narcotics possession, we can use our model to compare the use of drug-sniffing dogs to the more traditional physical search for drugs to find which method has a higher productivity. Suppose a car has been pulled over, and the police wish to determine whether the car has narcotics inside. A traditional physical search will take a substantial amount of time, which increases both the administrative and privacy cost of the surveillance. The physical search will also reveal a large amount of protected information to the law enforcement officer—essentially the entire contents of the car—which further increases the privacy cost. On the other side of the equation, a thorough search is likely to turn up narcotics if in fact any exist, though the most serious crimes are more likely to remain undetected because drug traffickers are likely to go to greater lengths to hide their contraband.

A drug sniff, on the other hand, imposes a much lower administrative cost to the government and a much lower privacy cost to the suspect—a traditional search is carried out only if there is a positive alert by the drug-sniffing dog. Even if the false positive rate is over 75%, the use of the drug-sniffing dog still represents a lower privacy cost than a traditional search. And if a drug-sniffing dog is used, any narcotics that are present are more likely to be found: Frequently the dog will alert to a certain area, and law enforcement officials can concentrate their search on that area, conducting a more careful and com-

prehensive search than they would have done if a drug-sniffing dog had not been used.

This conclusion does not mean that drug-sniffing dogs should be used indiscriminately, without probable cause, on every car that police stop on the road or find in a parking lot. It means only that searches with drug-sniffing dogs are preferable to searches without them because the former are more productive—they carry a lower cost with a higher rate of return. Thus, we should encourage their use over other, less productive searches, such as physical searches. Indeed, the current laws reflect this reality: Dog-sniff searches conducted during lawful *Terry* stops are permitted without a warrant,[100] whereas physical searches of a car without a warrant require probable cause.[101] This provides police with an incentive to use searches with drug dogs as opposed to relying on physical searches.

Two other common examples of binary surveillance are hash value searches and gun detectors. "Hash value" searches are searches of a computer hard drive or other digital storage device in which a piece of software is used to examine every file stored on the drive. Every computer file has a unique identifier known as its "hash value," which is as individualized as a fingerprint.[102] The Federal Bureau of Investigation (FBI) maintains a database containing the hash value of every known computer file containing child pornography. Thus, a computer program could be installed into a suspect's hard drive and could sift through every digital file stored there, looking for a match with any of the thousands of known contraband hash values. If no match were found, the program would return no results, and the law enforcement officer monitoring the program would learn nothing about the suspect's computer other than the fact that it did not contain any known files of child pornography. If a match were found, the law enforcement officer would know with near-certainty that the suspect's computer did contain at least one such file.

The software searching for these files could be secretly downloaded into a suspect's computer as an attachment to an e-mail, or it could be attached to an internet service provider

100. *See, e.g.*, Illinois v. Caballes, 543 U.S. 405, 410 (2005).

101. *See* Carroll v. United States, 267 U.S. 132 (1925).

102. *See* KERR, *supra* note 63, at 316–17.

(ISP) to monitor all internet traffic to and from the suspect's computer. Alternatively, this surveillance technique could be conducted on a massive scale, one that makes the potential scale of public video cameras and GPS tracking devices look trivial. At a relatively low administrative cost, the government could install this binary "sniffer" software on all the major ISPs and monitor virtually all e-mail and Internet traffic in the country. Or, if the government wanted to search hard drives indiscriminately for contraband files, it could send out e-mails with "Trojan Horse" viruses that search through hard drives and send a report back to the government.[103]

Similarly, advances in X-ray technology and image recognition software will soon result in the production of binary gun detectors.[104] These portable devices would be able to see through clothing or the outside of containers and discern the shape of objects that are secretly being carried by individuals. To ensure that the search is binary, the devices would not display the shapes to the user; instead, software inside the device would match all of the shapes detected by the device to the shape of a handgun. If a match is found, the device would produce its only possible output: a flashing red light or a beep indicating that it had detected a gun, much like the output of a metal detector. Once again, there is a potential for widespread use of these devices—each individual device may be expensive, but on a busy city sidewalk, each device could be used to conduct surveillance on thousands of individuals in the course of a single hour.

For hash value searches and gun detectors, both the administrative cost and the privacy cost of each individual search is very low. The chance of a successful search, however, is also very low, especially if the surveillance is done indiscriminately. The crimes they seek to identify—possession of child pornography or possession of a firearm—are relatively serious offenses, and the effectiveness of gun detectors is enhanced by the fact that finding a gun could prevent a far more serious crime of violence. But even if these surveillance techniques are

---

103. *See* MacDonnell, *supra* note 92, at 345–46.

104. *See* MacDonnell, *supra* note 92, at 347–48; Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1344, 1353 (2002).

honed to the point where they are unfailingly accurate, there is still a problem of false positives in the legal sense. In the case of child pornography, the problem stems from the "knowing" mens rea requirement for possession crimes:[105] frequently an individual may have downloaded child pornography without being aware of it. Perhaps the suspect believed he was downloading adult pornography, or perhaps there are multiple users of the computer, only one of which is aware of the contraband on the hard drive.[106] In the case of gun detectors, the legal false positives are generated by the fact that many states allow individuals to carry concealed handguns. Thus, a positive alert by the gun detector may provide unequivocal evidence that the suspect is carrying a gun, but not unequivocal evidence that possession of the gun is illegal.[107]

As with drug-sniffing dogs, false positives lower the productivity of the search because they increase the privacy cost of the surveillance. Every time there is a false positive, the officer will conduct a more intrusive search—either a full search of the hard drive (in the case of the child pornography alert), or a physical search of the container or suspect himself (in the case of the gun alert). This means that in calculating the productivity of these binary searches, we must also consider the legal status of the item that is being detected as this status will determine how often a positive alert will actually result in a successful search.

2. *Diminishing Societal Expectations of Privacy*

Another way in which surveillance methods can become more productive occurs when the privacy cost of the surveillance is reduced because society's reasonable expectation of

105. *See* 18 U.S.C. § 1966A (2006).

106. To some extent, this is true for every type of surveillance. A successful surveillance simply means that evidence is found that could lead to conviction, not that the evidence on its own proves the defendant's guilt beyond a reasonable doubt.

107. These "legal false positives" are not really an issue for drug-sniffing dogs, for a number of reasons. First, unlike the contents of a computer hard drive, it is difficult for a suspect to claim that he did not know that he had drugs on his person or in his suitcase. Second, unlike possession of handguns, possession of narcotics is illegal in every state under almost any circumstance.

privacy has shifted.[108] Like other factors we have considered, this shift can work both ways: As certain technologies become more commonly used and as cultural norms change throughout the decades, some aspects of life that we originally considered public may now be reasonably expected to be private, whereas other aspects of life that we originally considered to be private can now be thought of as public. Our productivity calculation needs to take these changes into account, discouraging the use of surveillance methods whose heightened privacy cost has now made them less productive, while encouraging law enforcement officials to take advantage of lower privacy expectations in other contexts.

Frequently, this shift in what we reasonably expect to be private will be caused not by the *invention* of the new technology, but by its subsequent widespread use throughout society. It was not the invention of the airplane in the nineteenth century, but rather its ubiquitous use in the mid-twentieth century that led the Court to hold in *California v. Ciraolo* that an individual had no reasonable expectation of privacy in what could be seen from the air.[109] The Court highlighted this distinction in *United States v. Kyllo*, stating that using "a device that is not in general public use," in this case a thermal imager, violates expectations of privacy.[110] However, if, in the near future, we all carry thermal imagers on our smart phones and routinely point them at houses to see where heat is emanating, the occupants of those houses would presumably lose their reasonable expectation of privacy

---

108. Admittedly, this analysis depends upon a certain definition of "reasonable expectation of privacy"—specifically, that "reasonable expectation of privacy" is equivalent to the information that society as a whole legitimately expects should be kept private. In other words, "reasonable expectation of privacy" is a description (or approximation) of society's shared beliefs about privacy. Although this is the most commonly held view of what the Court means when it uses this term, others have proposed different possible definitions. *See, e.g.*, Orin Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 507–22 (discussing four different possible definitions: the "probabilistic" model, the "private facts" model, the "positive law" model, and the "policy" model).

109. 476 U.S. 207, 215 (1986); *see also* Kyllo v. United States, 533 U.S. 27, 33–34 (2001) ("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. For example, as the cases discussed above make clear, the technology enabling human flight has exposed to public view (and hence, we have said, to official observation) uncovered portions of the house and its curtilage that once were private.").

110. 533 U.S. at 40.

in that information, and law enforcement agents could freely use thermal imagers without a warrant.

Widespread use of new technologies can also *increase* society's reasonable expectation of privacy. In 1986, when the Internet was young and relatively unknown to the general population, Congress passed the Electronic Communication and Privacy Act (ECPA), which set rules for monitoring voice and electronic communication. Under the ECPA, voice communication received robust protection, and the ECPA provided a suppression remedy, mandating that all evidence obtained in violation of the ECPA be excluded from court.[111] But electronic communication did not receive the same level of protection.[112] Government officials did not need to meet the same standards to receive a warrant to intercept e-mails or access stored e-mails,[113] and if they did violate those rules, the ECPA did not require suppression.[114] At the time, legislators believed that the Internet was developing into a tool for commerce, which deserved less protection than the sometimes intimate conversations that occurred using the telephone.[115] Furthermore, e-mails easily could be intercepted by the government because they were transferred and stored by third-party ISPs. Thus, Congress reasoned, most people using the Internet would not expect the same level of privacy as they would when speaking on the telephone.[116]

These assumptions may have been true in 1986 when the ECPA was passed. But as the technology of electronic communication has become widespread—indeed, as it has become the primary method of interpersonal communication for a large number of Americans[117]—our reasonable expectation of privacy

---

111. *See* 18 U.S.C. § 2515 (2006).

112. *See* Michael S. Leib, *E-mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III's Statutory Exclusionary Rule and Expressly Reject a "Good Faith" Exception*," 34 HARV. J. ON LEGIS. 393, 406–09 (1997) (detailing the numerous ways in which electronic communication receives less protection under the ECPA).

113. *Id.*

114. *Id.* at 408–09.

115. *Id.* at 410.

116. *Id.* at 409–10.

117. *See* Kristen Purcell, *Search and email still top the list of most popular online activities*, PEW RES. CTR., INTERNET & AM. LIFE PROJECT (Aug. 9, 2011),

in electronic communications has shifted. Courts are now properly recognizing this shift and extending full Fourth Amendment protection to electronic communications, thereby overruling the ECPA's now dated judgment on the degree of privacy that should be afforded to this medium. Consider the Sixth Circuit's reasoning in the 2010 case of *United States v. Warshak*:

> The next question is whether society is prepared to recognize [defendant's expectation of privacy in his emails] as reasonable. This question is one of grave import and enduring consequence, given the prominent role that email has assumed in modern communication. Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. . . . By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities.[118]

The *Warshak* Court concluded that "the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."[119]

In terms of our formula, C_P (the privacy cost) is not constant for any given form of surveillance. It will increase or decrease as certain types of technology become more widespread (as in airplanes and perhaps, someday, thermal imagers), or as technology is used in different ways (as in the Internet).

But new uses of technologies are not the only way that reasonable expectations of privacy can change: Cultural and economic shifts can also change what we consider to be private. Today, we are in the midst of a significant cultural shift regarding our expectation of privacy for the information we share online and the information we share with private companies. Many younger Americans have grown up with the expectation that information about themselves will be shared through social me-

---

http://pewinternet.org/Reports/2011/Search-and-email.aspx (noting growth in e-mail usage among Americans).

118. 631 F.3d 266, 284 (6th Cir. 2010) (internal citations omitted).

119. *Id.* at 285.

dia sites, public blogging, or smart phone applications that reveal where they are at all times. Some scholars call this generation "digital natives,"[120] and surveys have shown that they consistently display less concern about keeping information about themselves private than the "digital immigrants" who did not grow up amid the ubiquity of information-sharing technology.[121] Other surveys have shown that digital natives are indeed concerned with privacy, but that they are less concerned about the type of information that is shared and more concerned about who has control of their information.[122] This generation has grown up in the era of massive corporate data collection, in which private companies like Google and Facebook and even retail stores collect information about customer preferences and then use it to target advertising or sell it to others.[123]

Eventually, these digital natives will become a majority of the population, and they will likely maintain their different—and in some ways more relaxed—attitudes about data privacy as they get older.[124] Thus, society's reasonable expectation of privacy will diminish, at least with regard to the personal and commercial data that digital natives are accustomed to sharing.[125] This inexorable shift has caused some scholars concern.

---

120. The terms "digital natives" and "digital immigrants" were coined by John Palfrey, Jr., *Case Commentary: We Googled You*, HARV. BUS. REV., June 2007, at 5.

121. *See* William McGeveran, *Disclosure, Endorsement, and Identity in Social Marketing*, 2009 U. ILL. L. REV. 1105, 1126 (2009); Kim Bartel Sheehan, *Toward a Typology of Internet Users and Online Privacy Concerns*, 18 INFO. SOC'Y 21, 30 (2002).

122. *See generally* Mary G. Leary, *Reasonable Expectations of Privacy for Youth in a Digital Age*, 80 MISS. L. J. 1033, 1044–48 (2011); Sonia Livingstone, *Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy, and Self-Expression*, 10 NEW MEDIA & SOC'Y 393 (2008).

123. Mary G. Leary, *The Missed Opportunity of* United States v. Jones*: Commercial Erosion of Fourth Amendment Protection in a Post-Google Earth World*, 15 U. PA. J. CONST. L. 331 (2012).

124. Teri Dobbins Baxter, *Low Expectations: How Changing Expectations of Privacy Can Erode Fourth Amendment Protection and a Proposed Solution*, 84 TEMP. L. REV. 599, 613 (2012).

125. *Id.* at 622 ("As [younger people] age, their privacy expectations may become the norm and reflect the views of an increasing share of the population. As discussed above, subjective privacy expectations among youth are diminishing even outside of regulated spaces such as schools. If these attitudes persist into adulthood, the expectations of society as a whole may shift and diminish over time. Consequently, 'society' may be less willing to accept that certain subjective expectations are reasonable. As youth continue to influence society, courts must be aware of the changes and make decisions regarding the reasonableness of pri-

For example, in a recent article, Professor Teri Baxter argues that the shift will "erode" Fourth Amendment protection.[126] Professor Baxter proposes legislative fixes or altering the "reasonable expectation of privacy" test itself.[127]

But Professor Baxter and others who propose solutions to this "problem" skip the first step of the analysis, which is to demonstrate that this shift in our reasonable expectation of privacy—and the resultant loosening of Fourth Amendment restrictions—is a problem to be solved in the first place. The implicit assumption in their argument is that the amount of privacy that we now enjoy from government searches is the optimal (or at least the minimum optimal) amount; thus, any technological or societal change which lowers this amount of privacy is negative. Their response is to change the law to freeze the existing levels of privacy in place.

But the "reasonable expectations" standard is meant to be a flexible one; it ought to adjust as the amount of privacy that we expect evolves. If as a society we become more willing to tolerate certain invasions of our privacy, the C_P, or privacy cost, of certain types of surveillance decreases, thus making those types of surveillance more productive. The level of intrusiveness of a surveillance method is not measured against an absolutist scale but against the subjective belief of the suspect and the reasonable belief of society. In other words, the changing expectations of privacy is not a problem to be solved but rather an opportunity to engage in certain kinds of surveillance more frequently because that type of surveillance is by definition no longer as intrusive as it used to be.

As an example, consider the surveillance of text messages by employers, as described in the recent case *City of Ontario v. Quon*.[128] In *Quon*, a city employer issued pagers to all of its workers, but notified its workers that it had the right to moni-

---

vacy expectations accordingly. Even if judges—particularly older judges—maintain heightened expectations of privacy, if the government can establish that large segments of society do not support those expectations, the judges will have to choose between their own beliefs and those of other, potentially larger, segments of society.").

126. *Id.* at 600.

127. *Id.* at 622–36.

128. 130 S. Ct. 2619 (2010).

tor the content of those texts at any time.[129] Later, the employer read through the plaintiff's texts and noticed that some of the texts were sexually explicit in nature.[130] The plaintiff then sued the city employer, alleging that when the city read his texts, it violated his reasonable expectation of privacy.[131]

The trial court and appellate court both found that the plaintiff had a reasonable expectation of privacy in the content of the texts that he sent using the government pager.[132] The legal question was a tricky one, requiring courts to interpret the fractured Supreme Court decision of *O'Connor v. Ortega*, where a state-run hospital conducted a search of the office and files of one of its employees.[133]

In *Quon*, the Supreme Court avoided the question of whether the plaintiff had a reasonable expectation of privacy in the context of his text messages. The Court explained that the *Katz* standard must remain a flexible one:

> Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. As one *amici* brief notes, many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency. Another *amicus* points out that the law is beginning to respond to these developments, as some States have recently passed statutes requiring employers to notify employees when monitoring their electronic communications. At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve.
>
> Even if the Court were certain that the *O'Connor* plurality's approach were the right one, the Court would have difficulty predicting how employees' privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reason-

129. *Id.* at 2625.

130. *Id.* at 2625–26.

131. *Id.* at 2626.

132. *Id.* at 2626–27. The courts differed, however, as to whether the city's search was reasonable. The lower court found that the reasonableness of the search depended upon the city's purpose in carrying out the search, and sent that question to the jury; the Ninth Circuit held that the search was unreasonable, regardless of the purpose. *Id.*

133. 480 U.S. 709, 710–13 (1987).

> able. Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.[134]

In other words, as technology and societal norms change, the C_P for a given type of surveillance also changes. Professor Baxter correctly points out that for many new technologies, this will result in a lowering of our expectation of privacy as the younger generation begins to replace the digital immigrant generation:

> Youth and young adults may believe that any expectation of privacy when using many forms of technology is unreasonable. This may reflect their greater understanding of the technology and the risks involved in using almost any technology. They may be familiar with successful attempts to hack into or access codes or accounts, and understand that few if any sites or accounts are truly secure. Consequently, they may consider any subjective expectation of privacy to be unreasonable.[135]

Professor Baxter means this to be a warning—as a dire consequence which must be avoided—and she proposes new tests to prevent this legal shift from occurring.[136] But nowhere is it written in stone that the contents of text messages on government-issued pagers must be protected by the Fourth Amendment. Indeed, the entire point of a flexible *Katz* test is that *nothing* about what the government is or is not allowed to search is written in stone. If in fifty years society no longer considers the content of text messages to be private, there is no reason to limit government surveillance of those messages.

---

134. *Quon*, 130 S. Ct. at 2629–30 (citations omitted).
135. Baxter, *supra* note 124, at 616.
136. *Id.* at 622–36.

Indeed, part of the reasoning in the *Jones* case involving GPS tracking of vehicles might also have to be revisited in the near future. Justice Alito (and three other Justices) concurred with the holding in the case because "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[137] That certainly was society's expectation thirty years ago, and it may still be the expectation today. But as GPS tracking in cars and phones becomes more ubiquitous, this is unlikely to be society's expectation ten years from now. Even today, Justice Alito's reasoning seems suspect: Should we really base society's current expectation of privacy on what law enforcement could accomplish back in the 1970s? Is it the job of the courts to freeze our expectation of privacy at a certain spot in time, and keep it at that level regardless of what the vast majority of individuals may come to believe is publically available information? If so, what era should we look to when we determine what the "proper" level of privacy is? Should it be 1967, when the *Katz* case was decided? Or, should it be 1791, when the Fourth Amendment was ratified? At any rate, the Court has made it clear in *Ciraolo* and *Kyllo* that the *Katz* test was *not* meant to freeze a certain expectation of privacy in place; instead, the standard was meant to adjust to new technological and societal changes.

Of course, this can work both ways. As noted above,[138] society's reasonable expectation of privacy in electronic communications has increased over the past few decades—a development that courts are now beginning to recognize. Likewise, we have seen an increase in society's reasonable expectation of privacy with regard to the third-party doctrine. In 1979, the Supreme Court held in *Smith v. Maryland* that we have no reasonable expectation of privacy in the telephone numbers we dial because we are voluntarily turning this information over to the telephone company.[139] In doing so, the Court applied an all-or-nothing approach to dis-

137. United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgment).

138. *See supra* notes 112–119 and accompanying text.

139. 442 U.S. 735, 743–44 (1979).

closure and privacy: Once an individual turns information over to anyone else, she is relinquishing any privacy rights to that information with regard to government surveillance. At least one member of the Court is ready to reject this approach: In *United States v. Jones*, Justice Sotomayor argued in favor of overruling this aspect of *Smith:*

> This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice Alito notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[140]

In short, society's expectation of privacy is a critical element in our productivity analysis, and if we do not keep up with how this expectation shifts over time, we run the risk of either overregulating certain surveillance methods based on outdated conceptions of what people wish to keep private, or underregulating other surveillance methods based on a misunderstanding of how intrusive people actually believe the surveillance to be.

C. Case Study: Surveillance at Airport Security Checkpoints

Airport security checkpoints provide an excellent opportunity to apply our productivity formula. Up until about a dec-

140. 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (citations omitted).

ade ago, law enforcement officials had essentially two different options at airport security checkpoints. They could conduct an initial physical search of every passenger, or they could use a magnetometer to scan every passenger for metal, and then conduct a more thorough physical search if metal was detected.

Based on our formula, it appears that frisking all passengers is the less productive of these two methods. Frisks carry a high cost in terms of intrusiveness. In a seminal article, Professors Christopher Slobogin and Joseph Schumacher surveyed over two hundred individuals by subjecting them to fifty different types of surveillance procedures and asking them to rate the intrusiveness of each on a scale of 1 to 100.[141] Frisks received an average score of 54.76, just below searches of newspaper offices.[142] In contrast, walking through a metal detector received a very low average "intrusiveness" score of 13.47, just above searching through foliage in a public park.[143] Moreover, the administrative costs of frisks are relatively high. Although frisks do not require any special equipment, individual frisks take longer to conduct than walking through a metal detector; therefore, more officers are required to conduct the same amount of surveillance in the same amount of time. On the other side of the equation, the success rate of frisks is substantial, but it is somewhat dependent on the level of intrusiveness of the frisk: The longer and more comprehensive the search, the more likely it is to uncover a weapon. Thus, it is hard to make productivity gains with this method because costs will inevitably rise as the expected benefits rise.

Magnetometers carry a much lower privacy cost because they do not involve any physical touching of the suspect and they reveal no private information other than the absence or presence of metal. They do have a significant false positive rate, in that they will frequently alert to the presence of innocuous metal as opposed to the presence of a dangerous weapon, and in these cases the suspect may be subjected to a

---

141. Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727, 733–37 (1993).

142. *Id.* at 738.

143. *Id.*

physical frisk. But the majority of people who are subject to this type of surveillance avoid a physical search, resulting in a low overall cost to privacy. The administrative cost of magnetometers is somewhat higher: The machines cost up to $15,000 and require multiple personnel to operate.[144] However, magnetometer surveillance is faster than physical frisks, so more suspects can be processed in the same amount of time. The success rate for magnetometers has varied over time as both law enforcement and criminals have been able to take advantage of new technologies. As soon as the technology of metal detection advanced to the point where widespread use of these machines became economically feasible, the productivity of surveillance at airport checkpoints increased substantially because magnetometers allowed for faster, less intrusive searches and nearly always detected the presence of weapons. But as the technology for weapons has evolved, criminals have been able to use weapons that are undetectable to metal detectors, such as ceramic knives or plastic explosives.[145] This in turn makes the magnetometers less productive, either because of a lower success rate; a need to resort to more intrusive physical searches on more individuals; or a higher administrative cost to develop and operate more sophisticated surveillance devices.

Today, there are many examples of more sophisticated surveillance methods. Law enforcement officers can swab the hand of every passenger and then test the swab for explosives to see if the suspect has handled explosives recently.[146] They can employ a magnetic imaging system, which uses millimeter wave detection to generate high-resolution images of a person's body.[147] Or they can use "puffer" machines, which blow air onto a person's body to dislodge and detect any small particles of explosives or gunpowder in the person's hair or clothing.[148] Each of these methods (or combination of methods) will

144. *Magnetometers, X-Rays, and More: Airport Security Technology*, FOXNEWS.COM, Dec. 29, 2009, *available at* http://www.foxnews.com/tech/2009/12/29/magnetometers-x-rays-airport-security-technology/.

145. *See Shoe Bomb Suspect 'One of Many'*, BBC NEWS, Dec. 26, 2001, http://news.bbc.co.uk/2/hi/uk_news/1729022.stm.

146. *Magnetometers, supra* note 144.

147. *Id.*

148. *Id.*

have its own distinct levels of administrative cost, privacy cost, and success rate, and thus its own unique level of productivity.

In most cases, the challenge is to ensure that law enforcement chooses the most productive method of surveillance. We usually cannot rely on law enforcement officials to naturally choose the most productive method, as generally they only care about the administrative cost and the success rate and will discount (or ignore) the privacy cost. Similarly, we cannot usually rely on the courts to choose the most productive method because courts will care only about the privacy cost, and will discount (or ignore) the success rate and the administrative cost. Neither institution has the incentive (much less the ability) to calculate the true productivity of each surveillance method. Therefore, I will argue in the conclusion that in most cases it is the legislature who much gather the necessary data, make the appropriate calculations, and then promulgate rules to regulate the choices of law enforcement.[149]

In the context of airport checkpoint surveillance, however, there is no need to ask the legislature to set these rules. Airport checkpoint surveillance is an outlier in terms of our model. Because of society's rapidly changing (and in this case, diminishing) reasonable expectation of privacy at airport checkpoints, the effective privacy costs of almost any surveillance method in this context are close to zero. After a wave of hijackings in the late 1960s, passengers on airplanes were willing to accept more intrusive searches in exchange for safer air travel.[150] Thus, the effective privacy cost of all airport searches dropped. After the terrorist attacks of September 11, 2001, a similar shift in public attitudes occurred, and the general population became willing to accept even more intrusive surveillance methods at airport checkpoints. Thus, although certain types of surveillance (taking off shoes and belts, walking through metal detectors, submitting to a pat-down), may carry a high privacy cost in other situations, the privacy cost for the identical method of surveillance at airport checkpoints is extremely low. Courts have recognized this reality, and (invoking the "special needs" doc-

149. *See infra* Conclusion.

150. *See* Ric Simmons, *Searching for Terrorists: Why Public Safety is Not a Special Need*, 59 DUKE L.J. 843, 851–55 (2010).

trine) have held that these searches are permissible under the Fourth Amendment.[151]

Although courts have not gone so far as to say that society has no reasonable expectation of privacy at airport checkpoints, the reality is that individuals boarding planes can no longer reasonably expect to avoid these searches. To use the terminology of our formula, C_P is close to zero for these searches:

$$(C_A + C_P) * X = E(S_1) + P(S_2)$$

If $C_P=0$, then the only variable left on the left side of the equation is C_A, the administrative cost, which law enforcement has both the ability and the incentive to calculate on their own. In other words, if society's reasonable expectation of privacy is so low that we do not have to worry about privacy costs, law enforcement officers will naturally choose the most productive method of surveillance. But this will rarely be the case. Usually, we need to create rules that will encourage (or force) law enforcement to choose the most productive surveillance method.

CONCLUSION

The stated goal of this Article was to determine the productivity of different methods of government surveillance by taking into account all the relevant costs and benefits of the surveillance. Once we have determined the most productive methods, however, we need a way to encourage law enforcement officers to use the more productive methods and avoid using the less productive methods. Left to their own devices, law enforcement officers cannot be counted on to use the most productive methods of surveillance because they are relatively insensitive to privacy costs. At any rate, they are ill-equipped to determine what those privacy costs actually are. Thus, we need to adjust the law governing surveillance to provide law enforcement officers with the proper incentive.

The simplest way of accomplishing this goal is by aligning the legal standard required to conduct a given surveillance method with the productivity of that method. Today we live

151. *See, e.g.*, United States v. Albarado, 495 F.2d 799, 806 (2d Cir. 1974); United States v. Cyzewski, 484 F.2d 509, 512 (5th Cir. 1973).

in a legal regime in which there are numerous different legal standards for different surveillance methods, some set by courts and some set by statutes. Many types of surveillance require no showing of suspicion at all on the part of law enforcement.[152] Some require a showing of "certified relevance"—little more than a ministerial approval by the courts.[153] Some require reasonable suspicion[154] or probable cause,[155] but allow the police officer to make that judgment on the spot, to be reviewed later by a neutral magistrate. Others require law enforcement to prove probable cause to a neutral magistrate before conducting the surveillance.[156] Still others require an even greater showing: probable cause in addition to proving that the surveillance is the only feasible means of conducting the investigation and that minimization protocols will be followed.[157]

Once we have calculated the productivity of each type of search, we should attach the lowest standards to the most productive searches and the highest standard to the least productive searches. As of now, the severity of the standard roughly tracks only one of the factors of productivity—the intrusiveness of the search—and ignores the others, such as the administrative cost, the likelihood of success, and the severity of the crime being investigated. Sometimes the standard is untethered from even the intrusiveness factor—for example, if the search is carried out in order to accomplish a "special need" distinct from criminal law enforcement.[158] A more sensible method of setting legal standards for surveillance methods would be to

152. If the surveillance is not a "search" under the Fourth Amendment and is not covered by any statutory restrictions, the government is free to conduct the surveillance with no showing of individualized suspicion. *See, e.g.*, United States v. Place, 463 U.S. 696 (1983).

153. This is the standard under the ECPA for gathering "non-content information" (such as address information) from real-time surveillance. *See* 18 U.S.C. § 3122(b) (2006).

154. This is the standard for a *Terry* stop. Terry v. Ohio, 392 U.S. 1, 30 (1968).

155. In some contexts police still must show probable cause, but they are allowed to conduct the search without first getting a warrant—for example, searches of automobiles. Chambers v. Maroney, 399 U.S. 42, 48 (1970).

156. Kyllo v. United States, 533 U.S. 27, 40 (2001).

157. This is the statutory standard for real-time interception of telephone or electronic transmissions. *See* 18 U.S.C. § 2518 (2006).

158. For example, roadblocks are meant to check for drunk drivers to protect the safety of motorists on the road. *See* Michigan v. Sitz, 496 U.S. 444 (1990).

align the standard to the overall productivity of the search and then to adjust the standard regularly as the productivity changes. New technologies can make the surveillance more successful, less intrusive, or less expensive; evolving standards of privacy can make the surveillance more or less intrusive; shifting legislative priorities can change the importance of certain types of crime. All of these factors can affect the productivity of a surveillance method.

Who should calculate the productivity for different methods of surveillance and set these standards? We have already seen that law enforcement, being relatively indifferent to the externality of the privacy costs, cannot be counted on to make the correct decision. For a number of reasons, however, the courts—which we generally rely upon to set the proper boundaries for government surveillance—are also an imperfect institution to make these determinations. First, their job is not to determine what is the *best* kind of search, but rather to set the outer limits as to what searches are permissible or impermissible. Second, just as law enforcement officers are insensitive to the privacy costs of their surveillance techniques, courts have devised tests that ignore a number of important factors in determining whether surveillance is permissible. For the most part, courts ignore the severity of the crime being investigated when evaluating a surveillance technique,[159] as well as the financial outlay required to conduct the surveillance.[160] But most importantly, we have seen that courts, like law enforcement officers, are unable to gauge accurately the level of intrusiveness of various types of technologies. They lack the investigative infrastructure required to understand how technologies function in practice and how often certain investigative techniques result in the successful apprehension of a suspect or the uncovering of evidence. Even in measuring intrusiveness—the one factor which they have been focusing

159. This is not true for every type of Fourth Amendment analysis. *See supra* notes 24–27 and accompanying text; Max Minzner, *Putting Probability Back into Probable Cause*, 87 TEX. L. REV. 913, 940 (2009) ("Currently, the Fourth Amendment is blind to the type of crime underlying the search.").

160. Had the caselaw evolved in a different way, courts may have considered these factors in determining whether a surveillance was "reasonable" under the Fourth Amendment. Instead, however, courts have chosen to essentially ignore these factors.

on for decades—they lack the ability to learn how a majority of society views certain different uses of surveillance technologies. This task is particularly challenging as society's views on privacy are evolving as quickly as new technologies are being invented. Thus, courts tend to refer merely to their own idea of what should or should not be private in lieu of examining any data as to what degree of privacy society is prepared to accept as reasonable.[161] When courts do attempt to tell us what "society" thinks is reasonable, they occasionally are spectacularly wrong—such as when the Supreme Court told us in *Olmstead* that a person who uses a telephone "intends to project his voice to those quite outside" and therefore does not deserve the protection of the Fourth Amendment.[162] Luckily, Congress stepped in to correct this mistake a few years later.[163] Later, the Court told us that we should not reasonably expect any amount of privacy in information that we turn over to third parties—even if the third party is a bank[164] or a telephone company,[165] and that disclosing the information the third party is a necessary element of modern commerce. This miscalculation regarding what society actually expects to be kept private could have disastrous results in the Internet age. Once again, Congress stepped in a few years later to realign the law with what a majority of Americans believed should be kept private.[166]

---

161. *See* Minnesota v. Carter, 525 U.S. 83, 97–98 (1998) (Scalia, J., concurring) ("In my view, the only thing the past three decades have established about the *Katz* test . . . is that, unsurprisingly, those 'actual (subjective) expectation[s] of privacy' 'that society is prepared to recognize as "reasonable,"' bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable. . . . [The Fourth Amendment] did not guarantee some generalized 'right of privacy' and leave it to this Court to determine which particular manifestations of the value of privacy 'society is prepared to recognize as "reasonable."' Rather, it enumerated ('persons, houses, papers, and effects') the objects of privacy protection to which the *Constitution* would extend, leaving further expansion to the good judgment, not of this Court, but of the people through their representatives in the legislature.") (citations omitted).

162. Olmstead v. United States, 277 U.S. 438, 466 (1928).

163. *See* Communications Act of 1934, Pub. L. No. 416-73D, § 605, (codified as amended at 47 U.S.C. § 605 (2006)).

164. United States v. Miller, 425 U.S. 435, 442–43 (1976).

165. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

166. *See* Electronic Communications and Privacy Act, 18 U.S.C. §§ 3121–3127 (2006) (regulating, among other things, surveillance information provided to third parties).

Even when courts are not spectacularly wrong, many of their judgments do not seem to line up well with what a majority of society *actually* reasonably believes ought to be kept private. Surveys have shown a significant amount of disconnect between the conduct that the Supreme Court believes violates a reasonable expectation of privacy and what individual citizens believe violates a reasonable expectation of privacy.[167] And as some scholars have noted, the Court does not seem very interested in empirical evidence on this issue.[168]

Luckily, neither law enforcement nor the courts are the primary source of surveillance regulation today. Over the past few decades, legislatures have taken a much more aggressive role in regulating surveillance. Today there are dozens of federal provisions that limit the use of technology by law enforcement, such as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III),[169] which regulates oral and wire communications; the 1986 Electronic Communications Privacy Act (ECPA),[170] which extends Title III to electronic communications; the Stored Communications Act (SCA),[171] which was part of ECPA and regulates government access to stored wire and electronic communications held by third-party ISPs; the Foreign Intelligence Surveillance Act of 1978 (FISA),[172] which sets out rules for electronic surveillance of agents of foreign powers; and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), which, among other effects, broadens the type of surveillance allowed under FISA and the ECPA.[173] All of these statues create a complex regime of surveillance regulation, so that when

---

167. *See* Slobogin & Schumacher, *supra* note 141, at 738–41. Professors Slobogin and Schumacher's article lists the "average intrusiveness" level for dozens of different types of surveillance based on a survey and then notes "frequent contrasts" between the survey results and the Supreme Court rulings on what constitutes a search. In areas ranging from the use of undercover officers to reviewing of bank records to seizures of luggage on buses, the Court has apparently misjudged the actual level of privacy that society considers to be reasonable.

168. *Id.* at 743.

169. *See* 18 U.S.C. §§ 2516–2518 (2006).

170. *See* Pub. L. No. 99-508, 100 Stat. 1848 (1986).

171. *See* 18 U.S.C. §§ 2701–2712 (2006).

172. *See* Pub. L. No. 95-511, 92 Stat. 1783 (1978).

173. *See* Pub. L. No. 107-56, 115 Stat. 272 (2001).

courts are evaluating the legality of a surveillance method—particularly if the surveillance method involves a relatively new technology—the court will frequently apply statutory rules rather than the Fourth Amendment.[174] Many scholars view the increasing involvement by Congress as a positive development, because the legislature is better equipped to determine the proper balance between the needs of law enforcement and the privacy rights of individuals.[175] Legislative bodies can act more quickly in response to changes in technologies and law enforcement needs, and they have the resources to learn what these changes are and how they affect surveillance methods.[176] In addition, measuring the productivity of surveillance requires a number of similarly important judgment calls that only legislatures are able to make. A legislature is uniquely qualified to calculate how intrusive a search is perceived to be by the general population. A legislature has the ability to hear from experts and gather information about the administrative costs of different methods of surveillance, as well as their likelihood of achieving success. Furthermore, a legislature is the very body that decides the severity of each crime, which is another factor in determining the benefit of any kind of surveillance.

Obviously, Congress is constrained by the courts' interpretation of the Fourth Amendment: If the Supreme Court decides that a particularly productive surveillance method requires law enforcement officers to obtain a warrant or demonstrate a similarly high standard of suspicion, Congress's ability to encourage that surveillance method is somewhat limited. But the Supreme Court has shown some willingness to defer to Congress on standards for surveillance methods, especially where Con-

174. Part of the problem with legislation in this area is that there are many different statutes covering many different situations. A broader, more comprehensive piece of privacy legislation would be easier to follow law enforcement to follow and easier for courts to implement.

175. *See* Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 853, 864–77 (2004). *But see* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 216 (1999) (arguing that courts must be counted on to apply consistent constitutional values to all types of surveillance).

176. Kerr, *supra* note 175, at 864–77.

gress has been willing to step in and take the lead.[177] This deference gives Congress the room it needs to redefine the way we think about surveillance regulation. It is time to move away from an intrusion-only based analysis and begin to consider all of the relevant factors of productivity when evaluating the desirability of surveillance methods.

177. For example, in a recent case, the Fourth Circuit warned against "wield[ing] the amorphous 'reasonable expectation of privacy' standard in a manner that nullifies the balance . . . struck by Congress in Title III," and affirmed that the "primary job of evaluating [new technologies'] impact on privacy rights and of updating the law must remain with . . . the legislature." United States v. McNulty (*In re* Askin), 47 F.3d 100, 105–06 (4th Cir. 1995). When the courts began looking for rules to regulate covert video surveillance, they showed even greater deference to Congress by adopting the exact standards that Congress set up to regulate wiretapping and holding that those same standards were mandated under the Fourth Amendment—essentially allowing the legislature to define the scope of Fourth Amendment protection in this area. *See, e.g.*, United States v. Torres, 751 F.2d 875, 885 (7th Cir. 1984) (explaining its intent to "borrow the warrant procedure of Title III, a careful legislative attempt to solve a very similar problem, and hold that it provides the measure of the government's constitutional obligation of particular description in using television to investigate crime").