Research Publication No. 2003-04
5/2003

Technology, Terrorism, and the Fishbowl Effect: An Economic Analysis of Surveillance and Searches

Andrew Song

TECHNOLOGY, TERRORISM, AND THE FISHBOWL EFFECT: AN ECONOMIC ANALYSIS OF SURVEILLANCE AND SEARCHES

Andrew Song[*]

Preliminary draft[**]

Abstract

The dual forces of terrorism and technology have eroded our understanding of privacy, confronting us with the difficult question, "What balance should we strike between privacy and public safety?" This paper offers an economic framework for analyzing when and to what degree privacy should be protected. It starts from the observation that surveillance can prevent and deter harm but creates disutility from loss of privacy, social costs from avoidance, defensive costs spent on protecting privacy, and administrative costs. The framework has several implications for law governing surveillance and searches. Specifically, with respect to Fourth Amendment doctrine, the framework suggests that courts should adopt different standards of scrutiny, engage in forum-based analysis, and give greater protection to hybrid rights involving speech and privacy.

Keywords: Privacy, Surveillance, Fourth Amendment.
JEL classifications: K14, K19

[*] Think Tank Affiliate, Berkman Center for Internet & Society at Harvard Law School; John M. Olin Fellow, Harvard Law School. I would like to thank Steven Shavell, John Palfrey, Vivek Mohta, and the participants in the Berkman Center Student Think Tank for comments. I am also grateful to the John M. Olin Center for Law, Economics & Business and the Berkman Center for Internet & Society at Harvard Law School for financial support.

[**]

Table of Contents

I. INTRODUCTION

Our understanding of privacy has been besieged by two forces: terrorism and technology. The terrorist attacks of September 11 vividly demonstrated the harm that terrorism can inflict and also our inability to prevent or deter the attacks given prior intelligence capabilities and efforts. In response, we unleashed a host of surveillance powers,[1] letting the dogs loose to hound the criminals, but instead of dogs, electronic devices. Since then, our nation been struggling to find a new balance between public safety and privacy. Like a tug of war, the government has pressed for more surveillance powers to combat terrorism and crime, while privacy advocates have sounded the death knell for privacy.

The second force that has besieged privacy is technology. Technological advancements tend to upset the natural balance of privacy with which we are accustomed by expanding the realm of surveillance that is possible. For instance, tiny cameras, the size of a stamp, can be sprinkled in a room, and soon with the help of software, they may be capable of transmitting high-quality images of any activity in the entire room.[2]

These two forces, terrorism and technology, are eroding the beach of privacy. The difficult question then becomes what balance should we strike between privacy and public safety? This question of finding a proper balance between privacy and public safety naturally lends itself to economic analysis, which often concerns itself with balancing of costs and benefits. Yet economic scholars have said little about privacy with respect to surveillance. One might think that economic analysis has little to contribute in this area because privacy and public safety are difficult to quantify. But this fact has not prevented economic analysis from making valuable contributions to the law of accidents, environmental regulation, and other areas.

This paper offers an economic analysis of privacy with respect to surveillance and searches. It provides an economic rationale for why privacy should be protected. The observation to be emphasized is that privacy provides an incentive to engage in desirable conduct, not just harmful conduct. Thus, the lack of privacy can inhibit socially valuable conduct. More importantly, the paper articulates a specific framework for determining when and to what degree society should protect privacy, thus offering some guidance as to what balance to strike between privacy and public safety.

The rest of the paper is organized as follows. Part II summarizes current law governing surveillance, focusing primarily on Fourth Amendment doctrine. Part III lays out the economic framework for analyzing privacy with regard to surveillance. Part IV offers a few remarks about assumptions in the framework. Part V examines the doctrinal implications of the proposed framework and offers several recommendations for reform. Part VI makes some concluding remarks. Lastly, a formal model of the framework is provided in the Appendix.

[1] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT") Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of U.S.C.).

[2] *See* Dan Farmer & Charles Mann, *Part Two: Surveillance Nation*, TECH. REV. 46, 48 (May 2003).

II. SUMMARY OF CURRENT LAW

I begin by briefly summarizing Fourth Amendment doctrine governing searches and surveillance. The Fourth Amendment has two distinct clauses. The first prohibits "unreasonable" searches and seizures.[3] The second requires that warrants authorizing searches shall be based on "probable cause" and described "particularly."[4]

Before inquiring whether a search is reasonable, courts first ask whether there is a "search" within the meaning of the Fourth Amendment. If the court finds that no "search" has occurred, the government is not constrained by the requirements of the Fourth Amendment. If there is a "search," the courts then ask whether the search is reasonable. A warrantless search is *per se* unreasonable.[5] However, there are numerous exceptions. Thus, the analysis shifts to the procedural requirement as to when a warrant is required. In the end, evidence that is obtained in violation of the Fourth Amendment will be suppressed.[6] This remedy is known as the exclusionary rule.

With respect to the antecedent question of whether a search has occurred, courts use a two-pronged test established in *Katz v. United States*.[7] First, the target must have manifested a subjective expectation of privacy, and, second, the expectation of privacy must be "reasonable."[8] The courts have struggled to articulate when an expectation of privacy is "reasonable." However, a few broad principles have emerged from the cases.

First, an individual does not have a reasonable expectation of privacy in areas that are open to public view. At one extreme, the search of an individual's home would violate a reasonable expectation of privacy. In *United States* v. *Silverman*,[9] the Court stated, "At the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[10] In *Dow Chemical Co. v. United States*,[11] the Court noted that "privacy expectations are most heightened" in the home.[12] In *United States v. Karo*,[13] the Drug Enforcement Administration, with the consent of the seller, installed an electronic tracking device on a container of ether, which can be used to extract cocaine from clothing. The buyer of the ether took the container to his house, and the agents followed him there. Later, they followed the container to another defendant's house and to various locations, which could not be observed by visual surveillance. Justice White, speaking for the majority, ruled that the use of the tracking device was a search because it verified that the container was in

[3] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." U.S. CONST. amend. IV.

[4] "[N]o warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id.*

[5] *See* Illinois v. Rodriguez, 497 U.S. 177, 181 (1990).

[6] *See* Mapp v. Ohio, 367 U.S. 643 (1961).

[7] *See* Katz. v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); California v. Ciraolo, 476 U.S. 207 (adopting the standard established in Justice Harlan's concurrence in *Katz*).

[8] *See* Katz, 389 U.S. at 360.

[9] 365 U.S. 505 (1961).

[10] *Id* at 511.

[11] 476 U.S. 227 (1986).

[12] *Id.* at 237.

[13] 468 U.S. 705 (1984).

the defendant's house, which could not be determined solely from visual surveillance from outside the house.

At the other extreme, there is no reasonable expectation of privacy in open fields, even if the land is private property.[14] In *Oliver v. United States,*[15] the defendant was growing marijuana in a field located more than a mile from his house. The field was private property in a highly secluded area and had a "No Trespassing" sign.[16] Nevertheless, the Supreme Court held that the defendant did not have a reasonable expectation of privacy because open fields do not provide the setting for "intimate activities."[17]

In between these two extremes, an individual has a reasonable expectation of privacy in "curtilage," the immediate area surrounding the home.[18] But "curtilage" is a term of art. To determine whether an area is protected curtilage, courts apply a four-factor balancing test: 1) the proximity of the area to the home, 2) whether the area is included within an enclosure encompassing the home, 3) the nature of the uses to which the area is put, and 4) the steps taken by the resident to protect the area from observation by people passing by.[19] In *United States v. Dunn,* the Court concluded that crossing several barbed wire fences on the defendant's 200-acre ranch and then a wooden fence that enclosed the front of a barn was not a search because the barn was 50 yards from a fence surrounding the defendant's home.

Second, an individual does not have a reasonable expectation of privacy in information that he "knowingly exposes to the public."[20] I will call this the *public exposure principle*. For example, it not a search for the police to use a "pen register" at a phone company to identify the phone numbers dialed from an individual's home because he exposes this information to the telephone company.[21] Through similar reasoning, lower courts have concluded that recording of conversations in electronic chat rooms is not a search even though the agent doing the recording is not a participant in the conversation.[22] In addition, it is not a search when police rummage through opaque garbage bags left on the curb of a street.[23]

However, it may be difficult to determine what exactly constitutes public view or public exposure. This problem often arises due to technological enhancement of the senses. The Court has held that the use of technology to obtain information that could not otherwise be obtained without physical intrusion into a constitutionally protected area constitutes a search if the technology is not in general public use.[24] For example, aerial surveillance of a fenced-in backyard from an altitude of 5000 feet is not a search because private and commercial flights are routine.[25] Similarly, aerial surveillance of a partially open greenhouse in a resident's backyard

[14] *See* Hester v. United States, 265 U.S. 57 (1924).
[15] 466 U.S. 170 (1984).
[16] *See id*.
[17] *See id.* at 176-179.
[18] United States v. Dunn, 480 U.S. 294 (1987).
[19] *Id.* at 301.
[20] *See* Katz, 389 U.S. at 351.
[21] *See* Smith v. Maryland, 442 U.S. 735 (1979).
[22] United States v. Charbonneau, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997).
[23] *See* California v. Greenwood, 486 U.S. 35 (1988)
[24] Kyllo v. United States, 533 U.S. 27, 34 (2001).
[25] California v. Ciraolo, 476 U.S. 207 (1986).

from a helicopter is not a search.[26] In *Kyllo v. United States*,[27] the Court held that use of a thermal imaging device targeted at a home was a search even though the device did not show any people or activity within the walls of the building.[28] In that case, the device was used to detect unusual heat emanating from certain rooms in which marijuana was grown.[29]

Third, an individual does not have a reasonable expectation of privacy in information obtained from one of the parties to whom the individual has voluntarily disclosed the information. I will call this the principle of *third party consent*. More specifically, recording of statements made to an undercover agent does not violate one's reasonable expectation of privacy.[30] Similarly, information disclosed to a government informant is not protected.[31] In *United States v. White*,[32] the defendant had a conversation with a government informant who carried a hidden radio transmitter. The recorded conversation took place in the defendant's home among other places, but Justice White held that the defendant did not have a reasonable expectation of privacy in the conversation because he assumed the risk that the party to the conversation would betray his trust.

III. THE FRAMEWORK

A. Prevention and Deterrence

Surveillance can benefit society in two ways. First, surveillance can be used to prevent harm through intervention. For instance, suppose the government were to routinely monitor users' emails. If a government agent came across an unencrypted communication revealing a high school student's plan to bring a gun to school and shoot his teacher and classmates, law enforcement could seize the gun before the teen has the opportunity to do harm to his fellow students.

The prevention of harm, however, is not limited to prevention of undesirable acts by individuals. Electronic surveillance can also affirmatively enhance public safety. For example, a municipality could employ video cameras at a public swimming pool to reduce incidents of drowning. Video cameras attached to computers may soon be capable of alerting lifeguards when a swimmer becomes immobile for more than a few minutes.[33] Thus, surveillance of swimming areas can affirmatively enhance public safety by reducing the incidents of drowning.

Second, surveillance can deter individuals from committing harm. Deterrence is achieved by increasing the probability of punishment through information gathered from surveillance. Unlike prevention, this information is not used until after the bad act has been committed even though the information may be gathered before the harmful act. For example, video cameras at ATM machines may not be able to prevent robberies because the police may be unable to act swiftly enough to intervene before the robbery takes place. However, surveillance

[26] Florida v. Riley, 488 U.S. 445 (1989).
[27] 533 U.S. 27 (2001).
[28] *Id.* at 30.
[29] *Id.*
[30] *See* Lopez v. United States, 373 U.S. 427 (1963).
[31] *See* Hoffa v. United States, 385 U.S. 206 (1966).
[32] 401 U.S. 745 (1971).
[33] *See* Ivan Amato, *Big Brother Logs On,* TECH. REV. (Sept. 2001).

may deter robbery because criminals know that they may be caught on camera. Even if the criminals wear masks, they may be identified by other characteristics, such as their height, build, and clothing.

Often, surveillance both prevents *and* deters harmful acts. In airports, for example, searches of passengers and their luggage may deter terrorists from attempting to hijack a plane because they know they might be caught before they can get on the plane. For those who cannot be deterred, however, passenger searches can prevent a terrorist with explosives from boarding a plane.

Lastly, surveillance can reduce the probability of harm to private parties, not just the general public. The harm could be to a corporation in the form of lost profits from employees who are shirking their duties and spending inordinate amounts of time surfing the Web at work. Employers might monitor their employees' Internet activity in order to prevent and deter employee shirking.

B. Privacy Disutility

1. Sources of privacy disutility

However, individuals may derive utility from privacy. If so, they will experience a loss in welfare from the loss of privacy caused by surveillance. I will call this "privacy disutility." Privacy disutility can be caused in several ways.

First, privacy disutility may result from the disclosure of information that an individual does not want exposed.[34] This is a loss of *informational privacy*." For example, an individual may feel violated if someone reads her personal diary. Alternatively, she may be embarrassed if someone read her emails that she wrote to her lover. Monica Lewinsky felt this way when prosecutors retrieved love letters from her home computer that she had written but never sent to President Clinton.[35] In general, an individual *A* experiences privacy disutility whenever information is revealed to *B* that *A* doesn't want *B* to know.

Second, the mere fact of monitoring can create privacy disutility even if no information is revealed in the process. This type of surveillance is an invasion of *attentional privacy* due to unwanted attention. For example, a young woman Rebecca may experience discomfort if she is being watched by her neighbor Tom, day in and day out, even if Tom doesn't learn any information about Rebecca. Tom may sit at his window with his binoculars and watch Rebecca's window even though Rebecca closes the curtains. The mere fact that Tom is watching makes Rebecca uncomfortable.

Of course, in this example, part of Rebecca's discomfort may also stem from her insecurity about her physical safety. Tom may turn out to be more than a peeper; he could be a dangerous stalker. But the privacy disutility is distinct from the threat of physical danger. A different context will help clarify the difference. Suppose that Rebecca walks into a museum,

[34] This, of course, assumes that we *know* that we are being watched, either at the time or after the fact. The issue of knowledge is discussed in more detail in Part IV.

[35] *See* ANDREW MORTON, MONICA'S STORY 215 (1999).

and she is accompanied by a large group of friends. She is not concerned about her physical safety because she is in a public place with many people and is with her friends. Sam, a stranger, begins to stare at her from across the room. He then follows her around from exhibit to exhibit, staying a distance, but continuing to gaze at her throughout her visit to the museum. She quickly leaves the museum with her friends because she is made distinctly uncomfortable by Sam's stare. This example illustrates how a mere unwanted gaze may cause discomfort. In fact, it is considered "rude" in our society to stare at strangers.

In practice, an invasion of informational privacy often accompanies an invasion of attentional privacy. There is often some information revealed in the process of surveillance whether the watcher intends to obtain information or not. To return to the example of peeping Tom, if Rebecca is not careful about closing the blinds, Tom might discover what kind of underwear that Rebecca wears, what pajamas Rebecca likes to sleep in, what kind of abs that Rebecca has (washboard or water cushion?). The exposure of these details may cause Rebecca privacy disutility in addition to the discomfort of being watched.

Third, even the mere presence of a third party can create privacy disutility. This is due to a loss in *physical privacy*. Consider the example of Mark and Sara, who are dating. Suppose Mark takes Sara to a candle-lit restaurant for dinner with a jazz trio playing George and Ira Gershwin melodies in the background. Afterwards, Mark drives to a bucolic spot with a breathtaking view of the city, so that they can talk through the night under the stars and watch the sun rise over the edge of the hill. One problem. Sara brings along her dog because she couldn't find anyone to house sit for her that night. The presence of the dog may ruin the date for Mark because, for him, the date is an experience that is intended to be shared between Sara and him only. The dog isn't "watching" what takes place on the date in any meaningful sense. The dog may just be blithely sitting in the back seat of the car, tongue drooping and tail wagging. However, the mere presence of the dog could ruin the date for Mark due to the lack of intimacy.

2. Reasons for privacy disutility

The previous examples illustrate various ways that privacy disutility can come about, but they do not explain the reasons that individuals value their privacy. Although the reasons are varied, a few useful observations can be made.

First, the utility from privacy can be direct or indirect. *Direct utility* refers to utility that individuals obtain from consumption of the good itself. For instance, I eat ice cream because I enjoy eating ice cream. My demand for ice cream is due to the intrinsic value of consumption. Similarly, privacy can confer direct utility in its own right, although commentators often overlook this fact.[36] Intimacy is an example. I derive utility from having intimacy with my significant other, intimacy meaning no more than privacy in this context. I may also derive utility from moments of solitude, solitude meaning no more than physical privacy. I find it soothing and peaceful to take walks in the park when no one else is around.

[36] Even privacy advocates attempt to justify why people value privacy, as if privacy has no value in itself. For example, Jeffrey Rosen has argued that privacy prevents us from being "judged out of context in a world of short attention spans." JEFFREY ROSEN, THE UNWANTED GAZE 8 (2d ed. 2001). Although his argument may be true, it only describes a type of derived demand for privacy.

The utility from privacy can also be indirect. *Indirect utility* refers to utility that individuals derive from a good to the extent that the good enables consumption of another good. For example, economists speak of utility from income, by which they mean the utility that can be derived from spending income on goods like ice cream and hot dogs.[37] Similarly, individuals may value privacy because it facilitates other benefits. The reasons for valuing privacy indirectly can be for good or bad reasons.

In some cases, individuals may value privacy because it helps them avoid sanctions for socially undesirable conduct.[38] The sanctions could be legal sanctions like imprisonment or social sanctions like disapproval by one's peers. Privacy enables individuals to avoid the consequences of behaving badly because other people do not know they have behaved badly. For example, a teen who plans to shoot his classmates will not want others rummaging through his emails because they might discover his malevolent plan. He would value the privacy of his emails because it helps him avoid being caught.

The fact that an individual wants to avoid sanctions for his conduct, though, does not necessarily mean the conduct is socially undesirable. That will depend, of course, on whether the sanctions are socially optimal or not. Even if we can assume that legal sanctions are optimally determined, it is hard to know whether social sanctions are optimal or not. An individual may be stigmatized by his peers for a number of reasons that are not socially desirable. For example, suppose in a particular law firm that working long hours is frowned upon by one's coworkers because the firm prides itself in being a lifestyle firm. Yet the net marginal productivity from working longer hours could very well be socially efficient. The converse situation could also arise. In another firm, it could be frowned upon by one's co-workers to leave the office before 8 pm. They may resent that the individual is leaving early while they have to stay late, or they might think he's not a team player. Yet the individual may be just as efficient working less hours, and staying late may not be cost-justified. In either scenario, the individual's desire for maintaining privacy concerning when he arrives or leaves the office may be, on balance, desirable.

In other cases, an individual may value privacy, not to commit undesirable acts at all, but to prevent undesirable acts from being done to the individual. We often think of this type of demand for privacy as *security*, but it is really the other side of the privacy coin. For example, Rebecca may not want her address and telephone information to be publicly available because an individual could use that information to stalk her.[39] Also, an individual may not want others to be able to intercept his Internet communications, which includes Web and email transmissions, because it contains sensitive financial data that can be used to commit identity theft. For example, he may transmit his credit card number and bank account information when he conducts financial transactions online.

[37] *See* WALTER NICHOLSON, MICROECONOMIC THEORY: BASIC PRINCIPLES AND EXTENSIONS 79 (6th ed. 1995).

[38] This point has been emphasized by Posner. *See* Richard. A. Posner, *Right of Privacy*, 12 GA. L. REV. 393, 394 (1978)

[39] Actress Rebecca Schaeffer was murdered by an obsessed fan who discovered her address from the California Department of Motor Vehicles. *See* JEFFREY ROSEN, THE UNWANTED GAZE 170 (2d ed. 2001).

For expositional clarity, I will not use the term "privacy utility" to refer to the indirect utility that an individual derives from evading sanctions for conduct that the surveillance is designed to ferret out. To return to the example of the high school shooter, the teenager will value the privacy of his emails because it helps him avoid getting caught for committing murder. If he is caught, he will be sanctioned and will suffer a loss, but I will not call this loss a form of privacy disutility. Certainly, the loss will affect the individual's utility, but it will be counted separately for analytical clarity.[40]

Note, however, that this definition of privacy utility does not mean that criminals cannot suffer privacy disutility. They can. For instance, the teenage shooter may still suffer privacy disutility to the extent that investigators read his personal emails that are unrelated to commission of the crime. This would be true if he obtains direct utility from the privacy of his personal emails. In addition, he may derive indirect utility from the privacy of his emails unrelated to the purpose of the investigation. Suppose that the teenager is gay and has not come out to his family or friends, and the investigators uncover emails that express his affection to a male classmate. If these documents became public as part of the court record, he would suffer privacy disutility from the exposure of this information to his family, friends, and acquaintances. The privacy utility is indirect because it depends on the way his family and friends treat him as a result of their ignorance.

3. Lack of privacy disutility

Of course, individuals may not always value their privacy in a given context. For example, some may not care if others know what kind of books they like to read, while others prefer to keep that information closely guarded because they regard it as personal. Some individuals may even derive utility from the lack of privacy. The "Jennicam" is an example. Jennifer Ringley, a twenty-one-year-old girl in Washington D.C., has a Web camera planted in her bedroom for anyone to watch twenty-four hours a day.[41] Reality TV shows are another example. Many eagerly flock to participate in shows like the "Real World" and "The Bachelor," allowing cameras to follow them around for several months of their lives or to film intimate moments and decisions.

However, two qualifications about the lack of privacy disutility are worth noting. First, the desire for privacy is *recipient-dependent*. In other words, the demand for privacy will depend on the identity of the observer or recipient of information. For example, Mark may willingly share intimate details about his life with his girlfriend Sara but would suffer privacy disutility if those same details were known by strangers. To some extent, all of us share information with family and friends that we do not want to share with the rest of the world. Individuals may even differentiate among friends, sharing information with closer friends but not with acquaintances.

Second, the demand for privacy is *purpose-dependent*. Individuals may be willing to reveal information if it is used for one purpose but not for other purposes. For example, an individual may have no reservations about revealing her age and weight to her doctor as part of a

[40] Formally, all this means is that I separate the two arguments in the individual's utility function. *See infra* Appendix.

[41] *See* ROSEN, *supra* note 39, at 50.

medical examination but may be embarrassed about revealing that information if she were dating that doctor (who is not *her* doctor). In other words, the demand for privacy will depend on whether the purpose is for medical diagnosis or for making judgments about physical attractiveness.

C. Social Costs of Avoidance

In response to a loss in privacy, individuals may alter their behavior to avoid or reduce their privacy disutility. They might respond in two ways. The first is to avoid the underlying behavior altogether due to the lack of privacy. The second is to undertake costly efforts to protect their privacy. This section will examine the effects of the first response, which I call *avoidance.* The next section will analyze the effects of the second response.[42]

Surveillance can inhibit individuals from engaging in certain activities. For instance, individuals may avoid engaging in activities that will subject them to a higher likelihood of being monitored if they experience privacy disutility from being monitored. In addition, they may avoid activities that will expose information that they would prefer not to be revealed to others. These activities in themselves may be socially desirable. Thus, surveillance can create a social loss by inhibiting these activities, what I will call "affected activities."

1. Externalities

The social costs from avoidance are likely to be large when there are *external benefits* to engaging in the activity. In such circumstances, individuals will choose not to engage in an activity if the marginal privacy disutility outweighs the marginal utility from engaging in the activity. However, the social marginal benefit from the activity may be greater than the private marginal utility to the individual. The result is that individuals will engage in a level of behavior that is less than socially desirable.

Consider monitoring of email for example. Carnivore (now known under the harmless pseudonym DCS 1000) is a software program that can be installed at an Internet Service Provider's facility.[43] It gives the FBI access to all electronic communications that cross the access point, not just communications to or from the target's Internet Protocol address. However, the program filters out and does not record any data that is not "relevant" to the investigation.

Suppose an FBI agent is investigating a group of terrorists who are critical of American foreign policy. The agent sets the Carnivore filter to capture emails with text strings containing words like "American foreign policy," "President Bush," and negative words like "stupid" or "imperialism." These terms are all arguably relevant to the investigation.[44] Now suppose that

[42] *See* Part III.D.

[43] Illinois Institute of Technology Research Institute, *Independent Review of the Carnivore System: Final Report* (2000)*, available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf (last visited Feb. 24, 2002).

[44] Put aside for the moment the potential for abuse in which the government exceeds its legitimate authority. For instance, the agent is not using Carnivore to find personal messages about sex for example.

there are several peaceful activists who are critical of the government's foreign policy but would prefer not to be monitored by the FBI for various reasons.[45]

To be concrete, suppose that an activist obtains a private benefit of $5 from criticizing America's initiation of war against Iraq. He considers whether to write an email articulating the reasons why America should not wage war against Iraq, pointing out the weaknesses in the evidence offered by the government as to Iraq's alleged capability to develop and use weapons of mass destruction. Suppose that each recipient of this email would obtain a net benefit of $5 from being better informed about the reasons for waging war against Iraq. However, the activist knows that there is a 70% chance that such an email would be intercepted by Carnivore. Further suppose that as a consequence, he would suffer privacy disutility of $10 from being placed on an FBI list.[46] In the end, the activist will choose not to write the email because his benefit of $5 is outweighed by the expected cost of $7.[47] However, it is socially desirable for him to write the email and send it to, say, twenty people because the social benefit would be $100, which outweighs the private cost of $7 to the individual. This example illustrates how surveillance can deter socially desirable conduct, namely the dissemination of information.

2. *Imperfect information*

The social costs from avoidance can be large even when there are no externalities present. It may be large when the subjects of surveillance have imperfect information about the benefits of engaging in an activity. For example, suppose a young teenager Jennifer is sexually active, and she feels uncomfortable about approaching her doctor to talk about safe sex because the topic is somewhat embarrassing and awkward. If we made condoms unavailable privately — for example available only upon request from a doctor — Jennifer might choose to forgo obtaining a condom because the perceived marginal benefit of obtaining the condom is not worth the marginal cost of privacy disutility. The perceived marginal benefit could be small because she has imperfect information and possible bad information about the danger of sexually-transmitted diseases (STDs) and relative effectiveness of condoms compared to other methods.

To be more precise, suppose that the probability that she will contract gonorrhea from her partner if she doesn't use a condom is 10%.[48] If she uses a condom, the probability is virtually 0%. Assume that the cost to her of contracting gonorrhea is $1,000, which reflects pain and suffering as well as the medical expenses she must bear to treat gonorrhea. However, because she has poor information about the prevalence of gonorrhea in the population, the effectiveness of condoms in preventing gonorrhea, and ineffectiveness of other "methods" of prevention, she estimates the probability of contracting gonorrhea from unprotected sex to be 0.01%. Suppose

[45] For instance, as a consequence of being monitored by the FBI, their names might be placed on a "no fly" list used to stop people at airports. *See* Eric Lichtblau, *Government's 'No Fly" List is Challenged in a Lawsuit*, N.Y. TIMES, April 23, 2003 at A17. Indeed, two peace activists, Rebecca Gordon and Janet Adams, who run a publication called War Times that is openly critical of the Bush administration's terrorism policies, were detained as they attempted to board a flight from San Francisco to Boston. *See id.* Officials claimed it was an honest mistake. *See id.* Still, a peace activist might be concerned that their activities might increase the probability of being placed on the FBI list, even if mistaken.

[46] *See id.*

[47] 70%($10) = $7.

[48] For expositional clarity, I do not consider the risk of pregnancy and other STDs, which the example could be extended to include.

the privacy disutility to her from visiting the doctor to request a condom is $15. Thus, she will choose not to obtain the condom because her perceived benefit is $10 while her expected cost is $15. Yet, the actual benefit of obtaining and using the condom is $100 because that is the expected harm she avoids by using the condom.

This example illustrates how the lack of privacy can inhibit socially desirable behavior such as obtaining a condom. Note that, in this example, the distortion of behavior is not due to the fact that Jennifer fails to internalize all of the social benefits of safe sex.[49] Rather, the distortion is due to the fact that the lack of privacy raises the cost of obtaining the condom and Jennifer has poor information about the benefits of using condoms. Of course, we could mitigate the extent of the distortion by attempting to directly disseminate information about the benefits of condoms, through aggressive advertising or sexual education classes in school.[50] Alternatively, or in conjunction with the dissemination of information, we could make condoms privately available, for example in public bathrooms, where an individual can purchase a condom anonymously. In this example, even if Jennifer were poorly informed, she would have obtained a condom if it were privately available because her perceived benefit of $10 would still have exceeded the expected cost of $0.[51]

The previous example can be extended to illustrate how the lack of privacy can inhibit individuals who have poor information from *seeking information*. Suppose Jennifer could have easily obtained information on the Internet about risks of gonorrhea and benefit of condoms, but she could not browse the Internet anonymously; each Web page that she visited and the contents of the page could be linked to her identity. In particular, suppose her parents log all Internet activity in their home,[52] and Jennifer would suffer privacy disutility of $50 if her parents found out that she was interested in safe sex. She doesn't know what she will learn on the Internet, but because none of her friends have ever had a sexually transmitted disease (at least they have never told her), she estimates the expected value of the information on the Internet to be $20. Clearly, she won't seek out information on the Internet because the cost of $50 outweighs her estimated expected benefit of $20. The actual expected value of the information on the Internet is $100 because the knowledge about gonorrhea and condoms could be used to reduce the probability of $1000 harm to her by 10%.

3. Non-communicative activities

Although many of the previous scenarios involve communication, social costs from avoidance are not limited to situations involving exchange of information. The condom example actually illustrates how the lack of privacy can chill non-speech, efforts to obtain condoms. Consider another example involving monitoring of swimming areas. Suppose that municipalities

[49] However, one could imagine that an individual might fail to internalize the benefits conferred to his or her partner from practicing safe sex. For instance, if the individual were male, he might fail to consider the full costs of pregnancy that his partner would have to bear.

[50] These measures are costly in themselves, although they may very well be cost justified.

[51] Realistically, the cost would not be $0. The purchase price of the condom plus the trouble of going to buy the condom might be $1 or $2.

[52] To simplify the analysis, assume that she can't obtain this information elsewhere. For example, her local public library and school use an imperfect filter that blocks all sites about sex, including web sites that discuss how to have safe sex.

installed 24-hour video camera surveillance of public beaches and lakes in order to reduce incidents of drowning. The video cameras would alert officials when it appears that a swimmer is in trouble, and a nearby lifeguard team could be dispatched to rescue the swimmer. However, the video surveillance could inhibit several beach-related activities: couples may be more reluctant to take intimate walks on the beach; individuals may be less willing to go fishing if the part of the value of fishing is the experience of being alone with nature; swimmers might not go skinny dipping, knowing that video cameras are present.[53] All these activities could be adversely affected by surveillance and do not involve speech.

For that reason, I prefer to avoid the term "chilling effect" when describing the inhibiting effect of surveillance on various activities, even though one could use that term. "Chilling effect" is often used in the First Amendment context to refer to the fact that uncertainty of liability or sanctions for harmful speech can chill socially valuable speech. As I have pointed out, though, the lack of privacy can inhibit much more than just speech. Therefore, I prefer the term "fishbowl effect" to refer to the inhibiting effect of loss of privacy. If we lived in a transparent glass bowl as goldfish do, we might end up doing what goldfish do — which is not much of anything. In other words, the fishbowl effect metaphorically conveys the fact that the lack of privacy can inhibit individuals from engaging in socially desirable activities.

4. *Number of activities*

The beach surveillance example also demonstrates that the social costs from avoidance will depend on the number of activities that take place in the area of surveillance. For instance, surveillance of beaches can affect fishing, skinny dipping, strolls on the beach, and so forth. By contrast, surveillance of ATMs can impact far fewer activities because individuals only go to ATMs to conduct financial transactions.

The social costs from avoidance will generally increase as the area subject to surveillance encompasses more activities, other things being equal. For instance, suppose that the city has a choice of conducting video surveillance on one of two beaches, which are identical in most respects (the area, the number of beachgoers, etc.). However, no one fishes at beach 1, whereas beach 2 is a popular destination for fishing. Surveillance of beach 2 will result in greater social costs of avoidance than surveillance of beach 1 as long as *some* fishermen experience privacy disutility from surveillance. The reason is that surveillance of beach 2 will inhibit fishing as well as all the other activities that take place on beach 1.

It is important to emphasize the caveat that other things must be held equal for the conclusion to be true. Surveillance of an area that encompasses only a single activity, like telephone conversations, could result in greater social costs of avoidance, than surveillance of an area that encompasses many activities, like on the beach. In that case, to make a meaningful comparison, the social cost from avoidance would have to be summed over all activities for each

[53] The overall effect on skinny dipping is more complicated because skinny dippers also obtain a benefit from video camera surveillance. Surveillance reduces the risk of drowning for them, so overall, they could be more willing to go skinny dipping. The net effect would depend on the expected harm from drowning weighted by the probability of drowning, the effectiveness of the surveillance in preventing drowning, and privacy disutility from the surveillance.

type of surveillance. The aggregate social cost from avoidance could not be determined solely on the basis of the number of activities.

D. Defensive costs

Rather than avoiding certain activities, individuals may take costly measures to protect their privacy. For example, individuals may encode their emails with 128-bit encryption, making it virtually impossible for unauthorized parties to read their emails without the proper decryption key. Some commentators have argued that this is an economic reason why the law should protect privacy. If parties can obtain their privacy in the end, but at higher cost, the law can reduce aggregate social costs by forbidding the invasion of privacy from the outset.[54]

However, the framework suggests the opposite conclusion: the ability of individuals to take defensive measures to protect their privacy can only reduce overall social costs of surveillance. The reason is that individuals will take defensive measures to protect their privacy if only if the cost of the defensive measure is less than or equal to their privacy disutility or private benefit forgone from avoidance.

To illustrate, consider the case of an individual who would be inhibited from engaging in a certain activity due to surveillance. Suppose that individual *A* would obtain a benefit of $30 from engaging in a particular activity but would suffer privacy disutility of $60 due to the presence of surveillance. If defensive measures are not technologically possible, he would choose not to engage in the activity, and his net benefit would be 0. However, suppose he could maintain his privacy at a cost of $20 by taking a certain defensive measure, like encrypting his email. Then, he will engage in the activity and enjoy a net private benefit of $10.[55] Compared to the welfare benchmark in the situation of no surveillance, the availability of defensive measures reduces social costs from $30 (costs of avoidance) to $20 (defensive costs).

Now consider an individual who would engage in the activity anyway despite the surveillance. Suppose that individual *B* would obtain a benefit of $80 from engaging in a particular activity, and his privacy disutility is $60 like *A*. Even if defensive measures were not available, he would choose to engage in the activity and would obtain a net benefit of $20. If he could take a defensive measure at a cost of $20, he would do so and lower his aggregate costs from $60 to $20. His net benefit would increase from $20 to $60 as a result.

In either case, the presence of defensive measures can only reduce overall social costs. In the case of individual *A*, the defensive measure reduces costs from avoidance. In the case of individual *B*, the defensive measure eliminates costs from privacy disutility.

[54] *See* David Friedman, *Privacy and Technology*, *in* THE RIGHT TO PRIVACY 186, 192 (Ellen Frankel Paul *et. al.* eds., 2000). Friedman gives an example involving rental of pornographic videos: "If I know the boss is monitoring my rentals from [the local video store], I respond by renting videos from a more distant and less convenient outlet. My boss is no better off [because] he is still ignorant of the fact. I am worse off by the additional driving time required to visit the more distant store." *Id.* In the end, the video renter ends up obtaining privacy but at much higher cost. Therefore, a regime that protects privacy can be socially preferable because it reduces overall costs.

[55] $30 – $20 = $10.

However, defensive measures also frustrate the benefits of surveillance. Terrorists can use encryption, for example, to thwart the effectiveness of surveillance in revealing their plot to bomb the World Trade Center. Thus, the overall social desirability of protecting privacy when defensive measures are available is indeterminate.

We can draw one general conclusion though. If the private benefit to criminals from committing a particular crime is much greater than the private benefit to innocent individuals from engaging in activities affected by the surveillance, then criminals are more likely than innocent individuals to take defensive measures because the probability that their benefit will exceed any given defensive cost is greater. Innocent individuals are less likely to take these costly defensive measures because the private benefit they derive from engaging in an activity is small. Thus, it is more likely to be cost-prohibitive for them to take these defensive measures. Such evidence would tend to favor greater protection of privacy because the surveillance would not be very effective in preventing or deterring harm but would tend to disproportionately inflict costs on innocent individuals in the form of privacy disutility or avoidance.

E. Administrative Costs

There are two types of administrative costs involved in searches and surveillance. The first type is the cost of gathering information ("collection costs"). This includes labor costs of employing agents to perform searches. It also encompasses costs of capital like X-ray machines and technological devices used in the search. The second type is the cost of processing the information gathered in the search or surveillance ("processing costs").

Take Magic Lantern for example. Magic Lantern is a program developed by the FBI that records all keystrokes on a particular computer.[56] The FBI has used an earlier version of Magic Lantern to obtain computer passwords. It can be installed remotely on a user's computer through the Internet and without the user's knowledge. The administrative cost of deploying Magic Lantern (the cost of conducting the surveillance) might be small; an agent might be able to deploy Magic Lantern from his computer in a matter of minutes, leave it on the target's computer for weeks, and retrieve it after a few days, again in a matter of minutes. But the processing cost might be large. Agents (or computers) must read through the transcript generated by Magic to identify the suspect's password among the strings of characters. The more information that is recorded in the surveillance, the more resources will be required to find the password in the alphabet soup. In general, it becomes more difficult to mine data for useful information as more information is swept up in the search.[57]

The two types of administrative costs are interrelated. The government can perform a focused search, which might increase the costs of collection but could lower the processing cost because less information is gathered. Alternatively, the government could perform an indiscriminate search, gathering a great deal of information at low cost, but incur higher processing costs later on when the government has to sift through the large amount of information.

[56] Bob Port, *Spy Software Helps FBI Crack Encrypted* Mail, DAILY NEWS, Dec. 9, 2001, at 8.

[57] Processing costs lead to the strategy in litigation where one party inundates the opposing party with discovery documents in order to drive up the opponent's costs. The strategy also makes it more difficult to find the smoking gun document in the haystack of paper.

Given limited resources, it is socially desirable to allocate resources to processing information that the government already possesses rather than collecting additional information if the two endeavors can yield the same benefit in prevention and deterrence. The reason is that the collection of more information incurs not only additional collection costs but also processing costs, whereas aggressively utilizing existing information incurs only additional processing costs. This may explain why the government has launched several initiatives to combine and coordinate existing government databases since September 11. For instance, the Terrorist Threat Integration Center now merges domestic and foreign intelligence on U.S. citizens as well as foreigners.[58] Similarly, the U.S. State Department has opened up its database on visa applications to local police departments.[59]

Unlike the other types of costs discussed earlier, administrative costs are incurred by the party undertaking the surveillance ("the surveillance actor"). Thus, the surveillance actor has the socially optimal incentive to minimize administrative costs. In general, the law will not need to provide the surveillance actor with proper incentives to minimize administrative costs, and these costs can generally be ignored when examining the level of privacy that the law should protect.

Nevertheless, the analysis of administrative costs is important in understanding the socially optimal level of surveillance. As technological advances lower the cost of conducting surveillance, the degree of surveillance that is socially desirable will also increase.

IV. REMARKS ON THE FRAMEWORK

A. *Illusion of privacy*

The framework above assumes that individuals are aware of the possibility of surveillance.[60] Several of the social costs can be avoided if the government could maintain an illusion of privacy, in which individuals think they have privacy when in fact they do not. For example, suppose the government conducted video surveillance of public parks using hidden cameras and did not disclose this fact to the public. Individuals would not suffer any privacy disutility if they were unaware of the presence of video cameras. Furthermore, there would be no avoidance. Couples would take walks through the park, hold picnics, suntan, go jogging as usual. Indeed, individuals would not alter their behavior in any way. They would act "naturally" because they are unaware that they are subject to surveillance.

Even though the illusion of privacy eliminates some of the social costs, it also eliminates some of the benefits of surveillance. As discussed earlier, one of the primary benefits of surveillance is to deter crime. An illusion of privacy forfeits the deterrent effect because individuals do not think they will get caught. For example, if individuals believed that there were no video cameras in the park, they might be inclined to mug someone or sell drugs in the park.

[58] Farmer & Mann, *supra* note 2, at 48.

[59] *Id.*

[60] However, it only assumes that individuals are aware of the *possibility* of surveillance. They may be uncertain as to whether they are in fact being monitored.

To be sure, the government can still use surveillance to prevent harm through intervention while maintaining an illusion of privacy. But a few caveats are worth noting. First, prevention will not be possible in many cases and, when possible, will be limited in its ability to avert the harm. For instance, if an individual attempts to mug someone in the park, and hidden video cameras alert the police, officers may not be dispatched quickly enough to stop the mugging before some harm is done.[61] Even if various plain-clothes policemen were stationed throughout the park, the mugger may injure the victim before the police can stop him. By contrast, if individuals are deterred, they will not commit the harmful act in the first place. Thus, individuals who can be deterred pose no risk of harm, whereas a prevention strategy runs the risk that those individuals will commit harm before the police can successfully intervene. In short, deterrence will often be pulling the most weight in bringing about the benefits.

Second, relying on prevention alone rather than prevention *and* deterrence will increase administrative costs. Prevention requires expenditure of additional resources in order to prevent the harm in addition to the administrative costs of implementing the surveillance itself. For instance, a certain amount of resources will be required to set up video cameras in the park. In addition, a police officer will have to be dispatched to stop each mugging. However, if individuals know that there are video cameras in the park, a potential mugger could be deterred from mugging someone in the park, and no additional enforcement expenditures would be required to avert the harm. Even if prevention could substitute for deterrence and achieve the same benefit as deterrence could, administrative costs would have to be higher, which could offset the cost-saving that the illusion of privacy was designed to achieve.

In addition to these caveats, as a practical matter, it will be difficult to maintain an illusion of privacy over the long term. For instance, suppose an individual goes skinny dipping at a beach, where she believes that no one is watching, and gets caught in a powerful undercurrent. A “stranger” who comes to her aid may be able to claim that it was coincidental when in fact the stranger is a lifeguard employed by the city to rescue swimmers on the beach, which is under secret video surveillance. This deception may work initially, but a hero can pull a Clark Kent only so many times before the truth is unveiled. Repeat swimmers may become suspicious of the privacy of the beach and not return to skinny dip, or those who have been rescued may share their stories with friends and family in the area, some of whom may also like to skinny dip.

Moreover, we should also question the social desirability of attempting to maintain an illusion of privacy. The discovery of government deceit may engender a more general distrust of the government. Individuals may begin to (rationally) suspect that there is some possibility of surveillance even when in fact there is none. The consequence is a loss in social welfare due to privacy disutility and avoidance, yet there is no corresponding benefit from an increase in public safety because there is no actual surveillance.

[61] Of course, the video cameras could be used to catch the criminal ex post, by tracking down the identity of the individual for example. But this, at most, will prevent the criminal from committing future harm by incapacitating the individual. The past harm cannot be undone and may go uncompensated. In this example, the mugger may have squandered the money already by the time he is caught.

In conclusion, in most circumstances, it will be socially desirable for the government to truthfully disclose the presence of surveillance when deterrence is possible, and the government will have a proper incentive to do so in order to reduce harm and administrative costs.

V. DOCTRINAL IMPLICATIONS

Even though the benefits and costs of surveillance may be difficult to quantify precisely, the framework offers several insights that can be used to enhance judicial or legislative decision-making. In this section, I will briefly analyze the implications for Fourth Amendment doctrine. In general, courts can use the framework to give concrete meaning to the "reasonable" expectation of privacy test. More specifically, the framework implies that courts should apply different standards of scrutiny, engage in forum-based analysis, and give greater protection to hybrid rights involving the First and Fourth Amendment.

A. A Reinterpretation of Reasonableness

Commentators have often criticized the reasonable expectation of privacy test because it is vague, subjective, and unpredictable.[62] To give concrete meaning to "reasonable" expectation of privacy, I suggest that the economic framework laid out here will be helpful. The usefulness of such a framework can be seen by way of analogy to the law of torts.

The doctrine of negligence requires that individuals exercise a degree of "reasonable" care.[63] The meaning of the term "reasonable" is vague as it is in Fourth Amendment jurisprudence. In tort law, commentators and courts have attempted to give a more precise meaning to the term using economic reasoning.[64] Judge Learned Hand adopted an economic interpretation of reasonableness in *United States v. Caroll Towing Co*. In that case, a barge broke away from a line of barges while it was being towed during the day. The barge owner sued the towing company for damages to the barge. Judge Hand held that the barge owner was negligent for failing to keep an employee on board the barge during working hours of the day when the accident happened. In deciding the case, Judge Hand articulated his famous formula: If the burden of precaution B is less than the probability of injury P times the harm L ($B < PL$), then the individual did not exercise reasonable care.[65] In essence, the Hand rule states than an injurer is liable when further precaution is cost-justified. The Third Restatement of Torts follows the same balancing approach to negligence:

> Primary factors to consider in ascertaining whether conduct lacks reasonable care are the foreseeable likelihood that it will result in harm, the foreseeable severity of the harm that may ensue, and the burden that would be borne by the actor and others if the actor takes precautions that eliminate or reduce the possibility of harm.[66]

[62] *See, e.g.*, WAYNE LAFAVE, 1 SEARCH AND SEIZURE § 2.1(d) (3d ed. 1996).

[63] *See* Brown v. Kendall, 60 Mass. 292 (1850).

[64] Richard Posner, *A Theory of Negligence*, 1 J. LEGAL STUD. 29 (1972).

[65] I do not suggest, however, that Judge Learned Hand's formula is the proper test for negligence.

[66] Restatement (Third) of Torts § 4.

I propose a similar economic interpretation of "reasonable" expectation of privacy. If the marginal benefit from the surveillance or search is outweighed by the marginal cost, the expectation of privacy should be deemed reasonable. To avoid unpredictability, however, courts should not engage in open-ended balancing on a case by case basis. Rather, they should engage in categorical balancing of the following sort laid out in the next sections.

B. Different Standards of Scrutiny

Different areas[67] should receive different levels of Fourth Amendment protection. Surveillance of protected areas should receive heightened scrutiny, perhaps akin to strict scrutiny; "unprotected" areas should receive minimal scrutiny; and areas in between should receive intermediate scrutiny.

The rationale for different standards of scrutiny is twofold. First, the expectation of privacy that is reasonable should depend on the degree of harm that the government is trying to prevent or deter. However, under the current test, individuals receive the same level of privacy protection whether the government is investigating tax fraud, a drug offense, or a terrorist bombing even though these types of criminal conduct have vastly different harms. By contrast, strict scrutiny would require the government to demonstrate a compelling state interest; intermediate scrutiny would require a "substantial" state interest; and minimal scrutiny would merely require a legitimate government interest (to prevent abuse). By demanding a more compelling governmental interest, higher standards of scrutiny require that the benefit from surveillance be greater when the social costs from surveillance are higher.

Second, the expectation of privacy that is reasonable also depends on the effectiveness of the method of surveillance in deterring or preventing harm. As in other areas of constitutional analysis, strict and intermediate scrutiny would require that no "lesser restrictive alternative" be available, "restrictive" in this context meaning restrictive of privacy. For instance, suppose a state statute authorized warrantless wiretaps of electronic communications when investigating suspected pedophiles. Assume for the moment that electronic communications would receive strict scrutiny. The government would then have to demonstrate that wiretaps are necessary to effectively investigate pedophiles and that a lesser restrictive alternative — like relying on underage individuals who have been accosted online by pedophiles to report these incidents — would not attain the same benefit.

To determine whether an area should receive heightened, intermediate, or minimal protection, courts should consider three factors: 1) the number of different activities that take place in the area subject to surveillance, 2) the nature of those activities, and 3) the social benefits conferred by those activities. The second factor serves as a proxy for the degree of privacy disutility, and the first and third factors reflect the social costs from avoidance.

C. Hybrid Rights

More specifically, surveillance of communicative activities should receive heightened protection as a categorical rule. The rationale is that the social costs from avoidance are likely to be greater due to the external benefits from the dissemination of information and imperfect

[67] By areas, I do not just mean physical areas but also areas of information, like telephone conversations.

information when seeking information. Doctrinally, what this means is that surveillance should receive heightened scrutiny when it implicates the hybrid rights of the First and Fourth Amendment.

There is support for recognizing such hybrid rights in the case law. In *Stanley v. Georgia*,[68] the privacy of the home was paramount to overturning a conviction for "possession of obscene matter." There, the government discovered obscene films in the process of searching the defendant's home for evidence of bookmaking. The Court held that the defendant could not be punished for possessing obscene material even though the sale and distribution of obscene material was not constitutionally protected.[69] The Court emphasized the privacy of the home in reaching its decision on First Amendment grounds: "Whatever may be the justification for other statutes regulating obscenity, we do not think they reach into the privacy of one's own home." Similarly, courts should emphasize the value of speech in reaching decisions on Fourth Amendment grounds.

For example, under the proposed rule, *Katz* would have been an easy case to decide. In that case, the FBI used an electronic listening and recording device attached to the outside of a public telephone booth to listen to a phone conversation in the booth. Because the surveillance of the telephone booth targeted communicative activities, the framework suggests that a court should apply strict scrutiny and deem the government's surveillance to be a "search" within the meaning of the Fourth Amendment. Thus, the FBI would have to obtain a warrant in order to conduct the surveillance.

D. Forum-based Analysis

The courts have historically given the home special protection against searches and surveillance.[70] The reason is that the sanctity of the home has "roots deep in the common law."[71] Heightened protection of the home makes sense from an economic perspective. Some of our most intimate activities take place in the home, and therefore, it is likely that individuals will experience greater privacy disutility from invasion of the privacy of the home. In addition, however, a greater number of activities take place in the home than in other forums. We sleep there, we eat there. We sometimes work, sometimes play, talk to our friends, and even maybe talk to ourselves. If more activities take place in the home, surveillance of the home will create a greater likelihood of inhibiting socially desirable activities.

By contrast, the Fourth Amendment offers no privacy protection in open fields. Again, this makes sense from the economic perspective. The types of activities that take place in open fields are not likely to be intimate activities. In addition, the number of activities that take place in open fields is fairly limited: growing vegetables, tending a flower garden, maybe target shooting.

More generally, the economic framework suggests that "general-purpose forums" should receive greater protection than "special-purpose forums" other things being equal. "General-

[68] 394 U.S. 557 (1969)

[69] *See* Roth v. United States, 354 U.S. 476 (1957).

[70] *See supra,* Part II.

[71] *Kyllo*, 533 U.S. at 34.

purpose forums" refer to forums in which many different activities take place. The reason for heightened protection of general-purpose forums is that surveillance of general-purpose forums is likely to impose greater social costs from avoidance because more activities take place in these forums. "Special-purpose forums" are forums that are limited to a few activities or even designated for a certain kind of activity. For example, stadiums are a special-purpose forum for watching sports games. Although many were disturbed by the video surveillance of the Super Bowl game in January 2001,[72] the economic framework elaborated here would imply that the law should have greater tolerance for surveillance of stadiums than surveillance of other areas like public parks or homes.

The economic rationale also implies that Internet traffic should receive heightened privacy protection. The Internet may not have the same historical significance as our homes. But more and more activities are taking place through the Internet. Individuals already use the Internet to do research, listen to music, manage financial assets, and make purchases. Someday, we may commonly use the Internet to watch TV, take classes, make friends online, and consult doctors and therapists. As more and more of our activities that we perform in real space shift to cyberspace, the economic theory of surveillance would suggest that Internet traffic should receive greater protection.

VI. CONCLUSION

Technological advances have consistently posed difficulty for the courts when analyzing privacy. Thirty years ago, the use of electronic listening devices in *Katz* forced the Court to re-evaluate its Fourth Amendment jurisprudence. The Court chose to abandon antiquated notions of privacy based on physical trespass. Eventually, the Court substituted the reasonable expectation of privacy test in place of the old doctrine. Yet, even today, *Kyllo* demonstrates that technological advances like thermal imaging still pose difficulties for the courts.

This paper has offered a new framework that reflects our intuitive notions about privacy, is consistent with many outcomes in prior cases, but renders the meaning of reasonable expectation of privacy more precise. Although I have only elaborated on the framework's implications for Fourth Amendment doctrine, the framework could be useful to other areas of law that regulate surveillance by the government, such as interpretation of federal and state wiretapping statutes. In addition, the analysis could be extended to private law affecting surveillance, such as invasion of privacy torts. The framework is applicable to any party who can benefit from surveillance: monitoring of employee emails by employers, "nanny cams" planted by parents to keep an eye on babysitters, searches of student lockers by the school administration. The purpose is to provide a general framework for analyzing privacy with respect to surveillance and for judicial and legislative decision-making as to what balance the law should strike between privacy and public safety.

[72] *See* Louis Sahagun & Josh Meyer, *Secret Cameras at Super Bowl Scanned Crowd for Criminals*, L.A. TIMES, Feb. 1, 2001, at A1.

VII. Appendix: A Formal Model

Some of the analysis in Part III can be rendered more precise in a formal model.

A. Prevention

In this section, I examine the optimal level of privacy when the government (or other entity) seeks to prevent some harm that cannot be deterred. For example, the harm may be due to accidents (swimmers drowning on the beach). The government chooses whether to undertake a method of surveillance that gathers a certain amount of information *x*. Let *h* be the harm that society would like to prevent and *p*(*x*) be the probability of harm. Assume that $p'(x) < 0$ and $p''(x) > 0$. In other words, the probability of the harm decreases as more information is gathered from surveillance but at a diminishing rate.

Suppose there are *n* different activities that take place in the area of surveillance ("affected activities"). An individual obtains a benefit *b* from engaging in an affected activity, where $0 \leq b \leq \bar{b}$. The probability density of *b* in the population is denoted *f(b)*. In addition, each affected activity can confer an external benefit *B* to others. However, an individual suffers a loss in utility, *l(x)*, due to a loss in privacy when engaging in an affected activity. It is assumed that individuals are risk neutral.

The administrative cost of gathering *x* is *c(x)*, where $c'(x) > 0$. In other words, the administrative cost of surveillance increases with the amount of information gathered. However, it is assumed that administrative costs do not increase with number of individuals who engage in affected activities. For example, if a beach is under surveillance by video cameras, a certain number of cameras will be needed to cover the area of the beach, but the number of cameras needed does not increase with the number of swimmers, fisherman, etc.

For each affected activity, an individual will derive utility $b - l(x)$ if he engages in the activity. If he does not engage in the activity, his utility will be 0. Thus, individuals will engage in an affected activity if and only if $b > l(x)$.

Social welfare is the social benefit from each affected activity less privacy disutility, summed over all individuals who engage in a particular affected activity, times the number of affected activities, less administrative costs and expected harm to society:

$$W = n\int_{l(x)}^{\bar{b}} [b + B - l(x)]\, f(b)\, db\ - c(x) - p(x)h\,. \tag{1}$$

The social problem is to choose the level of *x* to maximize (1). The optimal value of *x* will be called the optimal level of surveillance and will be denoted *x**. *x** is determined by the first-order condition of (1), which can be written as follows:

$$-p'(x)h = c'(x) + n\left[l'(x)\int_{l(x)}^{\bar{b}} f(b)db + Bf(l(x))l'(x) \right]. \tag{2}$$

The left side of (2) is the marginal benefit of increasing surveillance, which is equal to the marginal reduction in expected harm. The right side reflects the marginal cost of increasing surveillance. The first term on the right side is the marginal increase in administrative costs. The second term on the right side is the marginal increase in privacy disutility for those individuals who engage in affected activities plus the external benefits forgone due to those individuals who are inhibited from engaging in such activities, times the number of affected activities.

1. Relation of x to other variables.*

Observe that the optimal level of surveillance increases with the effectiveness of the surveillance in reducing the probability of harm, *p'(x)*, as well as the magnitude of the harm, *h.* The reason is that social welfare can be increased from the prevention of the harm.

The optimal level of surveillance is lower if marginal administrative costs $c'(x)$ are higher. The optimal level of surveillance is also lower if marginal privacy disutility from surveillance, *l'(x)*, is greater and if the number of individuals who engage in affected activities, represented by $\int_{l(x)}^{\bar{b}} f(b)db$, is larger because they will suffer privacy disutility.

Surprisingly, though, the optimal level of surveillance does not directly depend on the private benefit, *b,* of engaging in the activity except to the extent that an increase in the maximum possible benefit, $\bar{b}$, will increase the number of individuals who choose to engage in an affected activity and thus will suffer privacy disutility. The reason for this somewhat counterintuitive result is that individuals on the margin, *b = l(x)*, are deriving negligible net benefit from engaging in an affected activity, and increasing surveillance by a small amount results in negligible social loss even though those individuals are inhibited from engaging in the affected activity.

However, the optimal level of surveillance does depend on the external benefit, *B*, that is forsaken due to avoidance of affected activities. Specifically, *x** will be lower if the external benefit of these activities is larger. Moreover, the optimal level of surveillance decreases as the number of individuals who are inhibited by the surveillance, *f(l(x)) l'(x),* increases. Lastly, as the number of affected activities *n* increases, the optimal level of surveillance decreases.

2. Comparison to first-best behavior.

The optimal level of surveillance does not induce first-best behavior by parties in the sense that some individuals who should engage in affected activities do not — specifically, those for whom $0 < b \leq l(x)$. We can think of *l(x)* as a tax on engaging in an affected activity. Even though these individuals would derive a positive value from engaging in the activity, *b > 0*, the tax deters them from doing so.

B. Deterrence

In this section, I examine the optimal level of privacy when the government seeks to deter harmful acts.[73] Suppose that an individual can obtain a private gain, $g \in [0, \bar{g}]$, from committing a bad act, which causes harm *h*. If the individual is caught, he will be penalized with a sanction *s*. The cost to the public of imposing the sanction is *k* per unit of *s*. The probability that a harmful act will be detected and punished is *p(x)*, where *x*, as one will recall, is the amount of information gathered from surveillance. It is assumed that $p'(x) > 0$; the probability of detection will increase as more information is gathered. The remainder of the notation is the same as before.[74]

An individual will engage in an affected activity if and only if $b > l(x)$. If an individual commits the harmful act, his utility will be $g - p(x)s - l(x)$.[75] If he does not commit the harmful act, his utility will be 0. Thus, an individual will commit the harmful act if and only if

$$g > p(x)s + l(x).$$

Social welfare is the social benefit from engaging in an affected activity less privacy disutility, summed over all individuals who engage in the affected activity, times the number of affected activities, plus the private gain from committing the harmful act less harm caused and expected cost of imposing sanctions, summed over all individuals who commit the harmful act, less administrative costs of conducting the surveillance:

$$W = n\int_{l(x)}^{\bar{b}}[b + B - l(x)]\,f(b)\,db + \int_{p(x)s+l(x)}^{\bar{g}}[g - h - p(x)ks]\,u(g)\,dg - c(x)\,. \tag{3}$$

The first-order condition of (3) can be written as follows:

$$[h - p(x)s(1-k) - l(x)][p'(x)s + l'(x)]u(p(x)s + l(x))$$
$$= l'(x)n\int_{l(x)}^{\bar{b}} f(b)\,db + nBf(l(x))l'(x) + p'(x)ks\int_{p(x)s+l(x)}^{\bar{g}} u(g)dg + c'(x)\,. \tag{4}$$

The left side of equation (4) is the marginal benefit of increasing surveillance, which is equal to the net social benefit from deterrence of additional individuals. This includes the harm that is averted and the reduction in costs of imposing sanctions and privacy disutility from additionally deterred individuals. The right side is the marginal cost of increasing surveillance. The first term reflects the marginal increase in privacy disutility for those individuals who engage in affected activities times the number of such activities. The second term is the external

[73] The model presented in this section builds on Polinsky and Shavell (1984).

[74] *See infra* Appendix.A.

[75] The individual suffers privacy utility because it is assumed that engaging in the activity is necessary to commit the harmful act. For example, a shoplifter cannot shoplift without entering the store. A terrorist cannot hijack an airplane without boarding the flight.

benefit forsaken for each affected activity that was avoided times the number of such activities. The third term is the marginal increase in cost of sanctions that will have to be imposed on additional individuals who are caught by surveillance. Finally, the last term is merely the marginal increase in administrative costs of the surveillance.

1. Effect on optimal sanction

Note that the surveillance increases deterrence in two ways. First, it deters harmful acts by increasing the probability of detection, represented by $p'(x)$. Second, it deters harmful acts by increasing the privacy disutility that a wrongdoer must suffer in order to commit harmful acts, $l'(x)$. In other words, invasion of privacy is a way to inflict punishment on wrongdoers and deter them. In most cases, however, the privacy disutility will be small compared to the expected sanction, $l(x) << p(x)s$. But this does not have to be always true.

Consider an extreme type of privacy invasion. Suppose, for example, that a clothing store instituted strip searches upon exit of the store.[76] This may substantially deter crime because few individuals, including shoplifters, would want to be subjected to that kind of embarrassment. Of course, as this example clearly illustrates, inflicting privacy disutility is a socially costly way of deterring harmful acts. The reason is that the privacy disutility is inflicted on many innocent individuals as a byproduct, which is reflected in the term $l'(x)n\int_{l(x)}^{\bar{b}} f(b)\,db$. Thus, not only will shoplifters stop going to the store, regular shoppers will also stop shopping at the store. In addition, those who do shop — because they cannot live without their Prada pants — suffer large privacy disutility from shopping.

In conclusion, even though privacy disutility can substitute for sanctions, it will generally not be desirable to do so because sanctions are likely to be less costly to impose.

[76] Although strip searches may seem extreme, police in Chicago used to strip search women who had been arrested for traffic violations from 1952 to 1979. *See* JEFFREY ROSEN, THE UNWANTED GAZE 37 (2001).