Mark Tunick, "Privacy in Public Places: Do GPS and Video Surveillance Provide Plain Views?",
Social Theory and Practice 35(4): 597-622 (2009)
Final version available at www.jstor.org/stable/23558699.

[597]I. The Issue

Technologies such as motion activated video cameras or global positioning systems (GPS) make it increasingly difficult to keep one's location private. Law enforcement officers are attracted to these technologies as they are relatively inexpensive and effective for monitoring suspected criminals compared to conducting round the clock (24 x 7) physical surveillance, which is costly, poses a danger to the investigators, and is more likely to be detected and avoided by the suspect. Police have surreptitiously attached inconspicuous GPS devices to individuals' cars, without a search warrant, to determine that a suspect was at each of the locations of a series of burglaries, that a suspected murderer drove to the location of his victim's buried body, and that a suspected drug trafficker traveled to a remote location where marijuana was illegally cultivated. [1]

When courts address concerns about the invasiveness of GPS surveillance, they consider whether it violates an established legal right. The Fourth Amendment of the U.S. Constitution declares "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches." The Amendment prohibits not all searches, only unreasonable ones, and only those conducted by state actors.[2] A prominent approach courts use to determine whether a search is unreasonable is to ask whether it violates an expectation of privacy that society regards as reasonable. [3] Using this 'reasonable expectation of privacy' paradigm, [598] courts in the U.S. have permitted GPS and video surveillance, on the grounds that people cannot reasonably expect privacy in the fact that they are located in a publicly accessible place where they could be observed by anyone, and since no one can reasonably expect privacy in public places, there is no good reason why government should not employ technologies enabling them more efficiently to gather information about a suspect's location.[4] I shall lay out two objections to this position.

---

[1] State v. Scott, 2006 WL 2640221 (N.J.Super.A.D. 2006) and People v. Lacey, 787 N.Y.S. 2d 680 (2004)(burglaries); State of Washington v. Jackson, 76 P. 3d 217 (2003)(murder); U.S. v. McIver, 186 F. 3d 1119 (1999)(drugs).

[2] The 4th Amendment limits only state action and provides no protection against private persons who violate an expectation of privacy. For example, a private citizen who sits down right next to me on a park bench and peers over my shoulder to read a letter I compose acts rudely and no doubt violates a reasonable expectation of privacy, but the 4th Amendment does not apply to him. In this article I focus primarily on legal protections of privacy we have against state actors.

[3] This approach was introduced by Justice Harlan in his concurring opinion in Katz v. U.S., 389 U.S. 347 (1967).

[4] State v. Sveum, 2009 WL 1229942 (Wis. App. 2009); People v. Weaver, 860 N.Y.S. 2d 223 (2008), reversed in 2009 WL 1286044 (N.Y. 2009) on state constitutional grounds; U.S. v. Garcia, 474 F.3d 994 (7th Cir. 2007); cert. denied at 128 S. Ct 291 (2007); People v. Gant, 802 N.Y.S. 2d 839 (2005); U.S. v. McIver, 186 F. 3d 1119 (1999); U.S. v. Moran, 349 F. Supp. 2d 425 (2005); Osburn v. State, 118 Nev. 323 (2002); U.S. v. Jones, 451 F. Supp.2d 71 (2006). The only courts in the U.S. requiring a warrant for GPS or similar surveillance appealed to state constitutions which offer stronger privacy protection than the federal constitution, see People v. Weaver, 2009 WL 1286044 (N.Y. 2009); State of Oregon v. Campbell, 759 P. 2d 1040 (1988); and State of Washington v. Jackson, 76 P. 3d. 217 (2003).

First, it wrongly assumes we cannot reasonably expect privacy in public places. When we venture out in public we must accept the risk that we may be seen by chance, but not the risk that we will be followed, or our movements tracked. Tracking one's location amounts to following a person; anger, resentment, and fear are among our likely responses if we were followed without our consent; and these reactions can be given a principled defense.[5] According to this objection, there is at least one sense in which people can reasonably expect privacy in public places—they can expect not to be followed without their consent.

The second objection to the position is that it wrongly assumes that as long as information could possibly be uncovered using legitimate means of observation, then police may use any means at their disposal to obtain that information, including new technologies of surveillance.

II. The plain view principle

It is not impermissible to uncover information about someone if they cannot reasonably expect privacy in that information. If you use an illicit drug in the open area of a public restroom, you cannot claim your privacy has been violated by a police officer who observes you there, for no one in that location can reasonably expect not to be seen. If you are in a restroom in a remote and unfrequented area of a public park in the late hours of the night, so that it is unlikely anyone would see you, you still [599] cannot reasonably expect to keep your activity private, because it is not implausible that someone legitimately could walk into the restroom and see you. This powerful intuition is the basis for the "plain view principle."[6]

> Plain view principle: (1) *If information about ourselves (including the fact that we are engaged in an activity or present in a certain location) is in plain view or earshot of anyone engaged in legitimate means of observation, we cannot reasonably expect privacy in that information;* (2) *otherwise we can.*

In some cases other relevant considerations may lead us to qualify the second part of the plain view principle. One such consideration is that we may think the value of privacy must be balanced against the value of preventing harmful acts. While I shall not defend the position here, some searches that the plain view principle might otherwise disallow may be justified on a balancing of costs and benefits. For example, airport x-ray scans reveal what is not in plain view, but may be justified because their benefits in deterring hijackings or bombings outweigh the costs of intruding on privacy. Another consideration may be that we cannot reasonably expect privacy in information about ourselves that we voluntarily convey to others (discussed in section IV). This consideration may also be relevant in explaining why airport x-ray scans are justified, although some will doubt that we truly consent to these searches if we have no choice but to travel on commercial flights. I will speak of a search that violates the plain view principle as violating a reasonable expectation of privacy, with the understanding that there may be other considerations, such as the results of a balancing test, requiring us to modify that conclusion in some cases.

---

[5] Cf. Helen Nissenbaum, "Protecting Privacy in an Information age: The Problem of Privacy in Public," Law and Philosophy 17(5/6):559-96 (1998), p. 581, on the need not just to appeal to indignation but to make sense of it.

[6] Cf. Mark Tunick, "Privacy in the Face of New Technologies of Surveillance," Public Affairs Quarterly 14:259-77 (2000), where an earlier version is developed of the theoretical framework employed here. Something like the plain view principle has been used in numerous U.S. Supreme Court cases, e.g. Katz v. United States, 389 U.S. 347, 351 (1967); California v. Ciraolo, 476 U.S. 207, 213-14 (1986).

According to the plain view principle, we can reasonably expect privacy in information that is not in plain view and is (or can be) discovered only by illegitimate means of observation.[7] For example, police officers violate a reasonable expectation of privacy we have in a closed toilet stall of a public restroom when they climb into a ventilator shaft and peer through a hole they cut through the ceiling of the stall, since we are not in plain view of someone engaged in legitimate means of observation.[8] [600] However, we cannot reasonably expect privacy in our conversation on a cordless phone if it can be heard over an FM radio by someone turning its dial, since listening to FM radios is a legitimate activity in our society.[9] One might take a different position, and hold that in this case we still do have a reasonable expectation of privacy, because a person who is surfing on a radio and happens upon a phone conversation should assume the conversation is meant to be private and refuse to listen. One might even take the position that persons entering the open area of a public restroom should avert their eyes were they to see you using an illicit drug, by appealing to the idea that there can be "conventional situational closure" even in the absence of actual physical closure.[10] But there are other duties citizens have besides respecting the privacy of others. We ought, and may have a duty, to be alert to threats to our own safety and the safety of others, which we cannot do if we avert our eyes or cover our ears in a public place. The plain view principle requires those who wish to keep information about themselves private to avoid locations in which this information can be uncovered using legitimate means of observation. Adhering to this principle constrains our liberty to some degree, but is preferable to living in a society in which people were expected to avoid observing others in public places. Life in such a society, one can imagine, would be extraordinarily inconvenient and even dangerous, which helps account for why we should want to adopt the plain view principle.

The plain view principle recognizes that there are acceptable means of uncovering information; but it also allows that some means of observation are illegitimate, against which we retain a reasonable expectation of privacy. Of course to apply the principle, we must determine which practices of observation are legitimate.

III. Legitimate Means of Observation

Whether an activity—such as following a person, or searching through their garbage-- is legitimate may depend on normative criteria—including the extent to which we value privacy; but it may also depend on empirical or descriptive facts, such as how prevalent the activity is, whether it is prohibited by laws or moral norms, and what public attitudes are toward the activity. We sometimes disagree about whether a particular means of observation is legitimate. I shall present an objection to GPS [601] surveillance of one's movements in public that assumes it is not legitimate to follow a person for an extended period of time. But the courts permitting GPS surveillance assume it is legitimate to follow a vehicle, pointing to *U.S. v. Knotts*. In *Knotts,* a majority of the United States Supreme Court held that police do not violate a

---

[7] Whether information is observed in plain view or merely could have been is a distinction central to the second objection, which I discuss in section IV.

[8] Cf. State v. Bryant, 177 N.W. 2d 800 (1970)(officer looks into toilet stall from ventilator shaft); Britt v. Superior Court of Santa Clara County, 374 P.2d 817 (1962)(officer observes toilet stall from a space between ceiling and upper floor); Bielicki v. Superior Court of L.A. County, 371 P.2d 288 (1962)(officer looks through ceiling pipe from roof to see into toilet stall).

[9] Tunick, "Privacy," p. 265; Cf. U.S. v. Smith, 978 F. 2d 171, 177-9 (1992).

[10] See Erving Goffman, Behavior In Public Places (New York: Free Press, 1966), pp. 151-2.

reasonable expectation of privacy when they track a vehicle's location using an electronic beeper attached to a container placed in the vehicle, on the grounds that a police car "could have observed" the vehicle.[11]

A convincing application of the plain view principle requires a plausible account of what means of observation are legitimate. In this section I discuss what I take to be among the most important considerations in developing such an account.

(a) Snooping

Consider the following examples.

(1) One morning my neighbor, stepping out to get her newspaper, sees some papers on her driveway that were blown there by the wind. The papers had been in loosely tied, opaque plastic garbage bags that I left on the curbside the evening before for pickup by trash collectors, but the bags were ripped and rummaged through by animals late at night. She picks up and reads the papers.

(2) Two friends have a quiet and discrete conversation at a restaurant while sitting at their corner table. Their conversation could not be heard by other patrons or restaurant staff without special equipment. A person sitting at a table out of earshot discerns the content of the conversation by lip reading.

(3) I place my garbage in opaque, tied plastic bags, and place the bags in a heavy aluminum garbage can, topped by a sturdy lid, and I secure the lid with a block of wood. My neighbor removes the wood and lid, rips open a bag to look for items of interest or value, and reads some papers I had left in the bags.

(4) A suspected tax evader shreds documents into 5/32 inch strips and leaves them in an opaque, tied, plastic garbage bag, placed in a lidded can, for pickup by the trash collectors. Federal investigators, without a warrant, take the bag, empty its contents, and painstakingly piece together the strips to reconstitute the documents.[12]

[602] One possible criterion for whether a means of observation is legitimate captures a distinction between Example 1 and Examples 2-4. In example 1, information I want to keep private is uncovered accidentally, by someone who is not snooping. I have bad luck, but my neighbor does not violate a reasonable expectation of privacy. If it was important to me that no one read my papers, I should have taken additional precautions to avoid what transpired. Examples 2-4 all involve snoops intending to uncover information they should know is not meant for their eyes or ears. In each of these cases precautions were taken to preserve privacy that were not enough to stop the snoop. But snoops act badly.[13] Characteristics of a snoop may include acting "on the sly," prying into matters one need not be concerned with, in a "sneaking or meddlesome manner," stealing or misappropriating, or doing what one is not supposed to do.[14] We distinguish snooping from legitimate means of observation. One reason we do is that snoops frustrate an important interest we have in privacy, an interest I discuss later in this section.

---

[11] 460 U.S. 276, 285 (1983). I discuss *Knotts* in section IV.

[12] U.S. v. Scott, 975 F. 2d 927(1st Cir. 1992); discussed in Mark Tunick, Practices and Principles: Approaches to Ethical and Legal Judgment (Princeton, NJ: Princeton University Press, 1998), pp. 177-8.

[13] Justice White, in California v. Greenwood, argues that we cannot reasonably expect privacy in garbage we leave for pickup because the garbage could be gone through not merely by animals or children, but by "snoops" (486 U.S. 35, 40-1 [1988]). He is wrong to use a snoop as a standard of legitimate conduct.

[14] O.E.D., 2nd ed. (1989).

The reason we should treat Example 1 differently from Examples 2-4 is that it is plausible to think we have no reasonable expectation of privacy in information that could be discovered accidentally, but that we can reasonably expect privacy in information that can be discovered only by a snoop, where a snoop refers to someone who obtains information which they should know they are not meant to have and that could not have been obtained accidentally by someone not intending to snoop. While we might admire someone who made an effort not to listen to an intimate but loud conversation between young lovers having a heated argument at the adjacent table of a restaurant, we cannot expect people to avoid what is in plain view or earshot. But we can blame them for taking measures to discover information not in plain view and not meant for them.

A few clarifying points may be helpful in understanding this conception of a snoop. Finding out where a person lives by asking them (without using coercion) is not snooping even though the information could not be obtained accidentally, because the information is voluntarily conveyed and therefore not information one should know they are not meant to have. Cases where I ask a third party to reveal to me a secret about you are more complicated. In some cases this can be snooping, but in some cases it is partaking in the legitimate practice of gossip. Even when it amounts to snooping, if you had voluntarily conveyed the information to others you may no longer reasonably expect privacy in it; your doing [603]o so may let the snoop credibly deny that they should have known the information is not meant for them.[15] A further point: to be a snoop one need not intend to obtain the information one actually discovers. Suppose a peeping Tom climbs a ladder to peer into a 2nd-floor window, enabling him to see what could not be seen accidentally; suppose also that his intention is to see someone in a state of disrobe. If instead he discovers an illicit drug transaction by fully clothed people, he is still a snoop. In contrast, an elderly woman who observes a young couple having a picnic in a park for hours, because it warms her heart to watch young people in love, does not act on the sly and is no snoop, even though concentrating on the couple is willful and cannot happen accidentally. She would be a snoop if she followed them from the park to learn about who they were and where they go; but merely observing a couple in a public place is a legitimate activity. If she stared intrusively and they frowned at her, she would learn that her actions were unwanted, and if she still continued observing them we might say she acts badly, although she would probably violate no legal right.[16] Finally, the idea that a snoop should know they are not meant to have the information they try to obtain is parasitic on other criteria for legitimate behavior. If we think that you are a snoop if you follow someone, or go through your neighbor's garbage, and you deny being a snoop by claiming that you do not know that you should not do these things, we might need to draw on these other criteria to establish that you should have known that the information you obtain is not meant for you.

If we want to retain privacy in information, we need to take measures to ensure it cannot be discovered accidentally, but we should not have to take measures to protect it from snoops. The moral judgment that we should not condone snooping can be given an economic rationale:

---

[15] Shared secrets between people in intimate relationships such as close friends or family pose a difficult problem: it is unlikely that such secrets will be readily revealed to curious strangers, but still we might think that one's expectation of privacy has been reduced by sharing the secret. I discuss this further in the last part of section IV.

[16] Not being a state actor, there is no possibility that she violates the 4th Amendment; and it is doubtful she commits a tort. For her to violate a legal right, there would need to be a law in place prohibiting staring. I thank one of *Social Theory and Practice*'s anonymous reviewers for suggesting the example.

requiring us to protect against clever snoops would cost us much more than what it costs to protect against accidental exposure. An escalation of wasteful expenditures—by snoops on surveillance technologies, by us on protective counter-measures—can be avoided by a moral or legal prohibition of snooping. But the economic rationale might not best explain why snooping is wrong—other arguments may, such as that the snoop fails to respect his victims, and treats them in ways the snoop would not want [604] others to treat him.

The consideration that snooping is wrong is the basis for what I call the "mischance principle":

> Mischance Principle: *If information about ourselves could be discovered accidentally, or without snooping, we cannot reasonably expect privacy in that information; otherwise we can*.[17]

The mischance principle captures the intuition that it is not legitimate to snoop, but leaves open the possibility that we may not reasonably expect privacy in information discovered by a snoop if it could have been discovered legitimately by a non-snoop. The mischance principle does not hold that one can legitimately obtain information only by accident. It allows people to intentionally uncover information so long as what they uncover could be discovered accidentally or is voluntarily conveyed.

There is some leeway for interpreting the phrase "could be discovered": one might endorse a "possibilist" account that denies us a reasonable expectation of privacy so long as it is possible, even if extremely improbable, for information to be discovered accidentally; or a "probabalist" account that requires that there be at least a minimum probability that the information could be discovered accidentally.[18] I shall not say too much about this issue, but note that how we interpret this part of the principle is likely to depend on how extensive are the precautions we think people should need to take to protect their privacy. For example, adopting a possibilist account, to expect privacy in discarded papers one might have to shred them, as in Example 4, since even the heavily secured garbage can in Example 3 could be compromised (for example, by a tornado, or collision with a vehicle), leaving its contents in plain view. A primary reason to adopt the mischance principle is that to preserve privacy people should not have to take extreme measures, or measures so expensive they might only be available to the wealthy.[19] We should not have to retreat to a windowless basement and talk in whispers to have a [605] private conversation; or supplement the tall fence surrounding our backyard with a large canopy so that snoops can't take satellite images of our activities there. This reason would be undercut by the 'possibilist' interpretation of the mischance principle.

Consequentialists such as those adopting a law and economics approach that applies the criterion of economic efficiency to policy questions might try to determine an optimal

---

[17] Cf. Tunick, "Privacy," p. 264. "Or without snooping" in this formulation may seem redundant since when one discovers information accidentally one normally does not snoop. I include it as a useful reminder of why non-accidental uncovering of information can be ethically problematic.

[18] The distinction between 'probabalist' and 'possibilist' accounts is made by Robert Goodin and Frank Jackson, "Freedom from Fear," Philosophy and Public Affairs 35(3):249-65 (2007), in the context of determining which external impediments to action that are due to human agency should engender rational fear.

[19] The wealthy (or any people) who take extreme precautions to preserve their privacy would be protected by the mischance principle against snoops, even if most people were unprotected against accidental discovery of information by non-snoops, because they could establish that in their case a snoop revealed what could not have been revealed accidentally.

probability threshold. They might try to weigh for a given threshold level the costs individuals would need to incur to preserve their privacy against the benefits of increased police efficiency and reduced crime. There could be a great deal of skepticism about whether these estimations could be made reliably, however, and this, along with criticisms of an approach that decides policy by appealing solely to economic measures of social welfare, might motivate us to seek other ways of resolving this issue.[20] One alternative would be to rely on a low probability threshold that rules out only implausible scenarios (such as that a tornado undermines the integrity of a well-secured garbage can). In section IV I consider still another approach, one that rejects the premise of the mischance principle that whether we have a reasonable expectation of privacy hinges on the counterfactual of how information could have been discovered, and focuses instead on the legitimacy of the means of observation actually used.

One might argue that Example 3 should be treated differently than Example 4 on the ground that police investigators should be exceptions to the rule that snoops act badly. A primary function of the police power is to detect crime, and we might think that snooping is essential to this function and is therefore legitimate when conducted by agents of government. On this view, the interest we have in privacy is an interest in denying access to information about ourselves to friends and loved ones, neighbors, employers, business competitors, the news media, colleagues, and the like, but not to law enforcement officers, so long as we can be sure that the officers do not reveal our secrets to those not needing or entitled to know them.

While there are circumstances in which police investigators are properly excepted from the rule that snoops act badly, which I shall discuss shortly, I believe there is a compelling argument for not regarding government snooping in general as legitimate. We could never be sure that illicit or inappropriate use won't be made of the information the govern [606] ment obtains. There are benign uses of location data: it could establish alibis of people wrongly accused of crime.[21] But it can also be abused. This could happen not only in the unlikely but conceivable scenarios where government agents are corrupt and use the information to intimidate or blackmail;[22] but where secondary uses of the data are made. Government is uniquely situated to facilitate abuses because of its ability to discover large amounts of information, store and access it; private snoops generally lack this ability.[23]

---

[20] For criticisms of a law and economics approach, see Mark Tunick, "Efficiency, Practices, and the Moral Point of View: Limits of Economic Interpretations of Law," in Mark White, ed. Theoretical Foundations of Law and Economics (New York: Cambridge University Press, 2009); Mark Sagoff, "Values and Preferences," Ethics 96(2):301-16 (1986); and Jules Coleman, "Review: The Grounds of Welfare," 112 Yale L.J. 1511 (2003).

[21] See Benjamin Weiser, "Murder Suspect Has Witness: A Metrocard," New York Times, November 19, 2008 (subway card allowed suspect's movements to be traced, indicating he could not have committed the murder of which he was accused).

[22] See Daniel Solove, "A Taxonomy of Privacy," 154 U. Pa. L. Rev. 477 (2006), pp. 495-6, 542-4 (on blackmail); Stanley Benn, "Privacy, Freedom, and Respect for Persons," in Ferdinand Schoeman, ed. Philosophical Dimensions Of Privacy: An Anthology (NY: Cambridge University Press, 1984), p. 226; cited in Jeffrey H. Reiman, "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future," 11 Santa Clara Computer & High Tech. L.J. 27 (March, 1995), p. 35 n. 22. Cf. Dorothy Glancy, "Privacy on the Open Road," 30 Ohio N.U.L. Rev. 295, 324-5 (2004), pp. 327-8; and Shaun Spencer, "Reasonable Expectations and the Erosion of Privacy," 39 San Diego L.Rev. 843 (2002), citing examples of government abuse of data.

[23] This does not mean that we have no privacy interest against unwarranted private uses of data. Google, for example, is capable of tracking its users' searches or the content of their google email—see Jeffrey

To illustrate such risks of government control of sensitive information generally, imagine the government collects and stores DNA samples of all persons living in or entering the country. Doing so would create a powerful tool to detect and deter crime; but it would also create unacceptable risks from illicit or inappropriate use of the information. For example, the identity of biological parents of adopted children could be revealed; long term care insurers or prospective employers could learn of a person's probability of suffering a genetic disease and refuse them coverage or employment;[24] a person's associations and activities could be documented by collecting exfoliated hair or cigarette butts or soda cans they discarded. A corrupt police officer could frame innocent individuals by placing items with their DNA at crime scenes. While laws could be enacted limiting access to and use of the database, no system is completely immune to security breaches.[25] Moreover, future legislators may decide to remove access-restrictions for the sake of expediency. While [607] abuse of location information that GPS surveillance presently could facilitate may pose fewer risks than would abuse of DNA evidence, if in the future the government implanted GPS chips in all people living or entering its jurisdiction, or used advanced satellite imaging to detect people's locations, the risks might be comparable. Even presently, the risks are serious enough to have us question whether the government should be permitted to obtain this information without a warrant.

Government should be held to higher and not lower standards than those to which we hold citizens, given the difference in power between it and them.[26] Doing so is consistent with a fundamental principle of U.S. constitutional law, that the rights the Constitution grants to individuals, such as to speak and exercise religion freely, to not be searched unreasonably, or not to be discriminated against, protect individuals against only state action and not private actors. [27] These rights were enumerated in the Constitution to address fears about a too powerful government, a government which is uniquely situated to restrict individual liberty.[28] Law enforcement agents are licensed to investigate crime and in doing so to act like snoops, so that the state may fulfill its function of protecting its citizens against internal and external threats, but only when they are authorized to do so by a warrant. The Constitution's warrant requirement ensures that agents of the state snoop only when doing so is likely to uncover information relevant to an investigation of someone they have probable cause to believe is engaged in

---

Rosen, "Google's Gatekeepers," New York Times Magazine, Nov. 30, 2008, pp. 54-5. For general discussion of this interest, see Daniel Solove, The Digital Person: Technology and Privacy in the Information Age (NY: NYU Press, 2004).

[24] Cf. Amy Harmon, "Insurance Fears Lead Many to Shun DNA Tests," New York Times, Feb. 24, 2008.

[25] Spencer, pp. 886-7.

[26] Cf. Richard Posner, "The Uncertain Protection of Privacy by the Supreme Court," 1979 Supreme Court Review 173 (1979), pp. 175-8; Annabelle Lever, "Mrs. Aremac and the Camera: A Response to Ryberg," Res Publica 14:35-42 (2008), pp. 37-8. Lever notes that government could use its power to violate equality by singling out people for unauthorized surveillance based on prejudices or contempt for certain people. Ryberg, in response, is content to rest on other protections against inappropriate government conduct rather than hamper police in their pursuit of criminals, see Jesper Ryberg, "Moral Rights and the Problem of Privacy in Public: A Reply to Lever and Goold," Res Publica 14:49-56 (2008), p. 53.

[27] Cf. Benjamin Goold, "The Difference Between Lonely Old Ladies and CCTV Cameras: A Response to Ryberg," Res Publica 14:43-47 (2008), p. 45.

[28] More precisely, the Bill of Rights were adopted out of fear of the federal government's powers, although at the time some questioned whether they were needed since the new federal government had only limited enumerated powers; rights established through the 14th Amendment were set up out of fear of states' powers.

criminal activity. Government investigators with a warrant to search are an exception to the general rule that snoops act badly, but when they snoop without a search warrant, they act badly. Of course they do not need a warrant to uncover information in plain view using legitimate means of observation. [608]

(b) Prevalence and acceptance

If information about ourselves could not be obtained accidentally and is not voluntarily conveyed—if only a snoop could uncover it—we have reason to expect privacy in this information, as snooping is generally not a legitimate activity. But we may need to appeal at times to other standards of legitimacy. The mischance principle focuses on whether information could be revealed accidentally, but some observations that could not be made accidentally may still be legitimate. If there were a severe shortage of aluminum, a society might encourage people to scavenge through garbage to gather scraps of the needed metal: in that society, observations of the contents of garbage would not occur accidentally but may well be legitimate. As I noted earlier, the concept of being a snoop may be parasitic on other standards of legitimate conduct.

Other potential criteria for whether a means of observation is legitimate are its prevalence and acceptance. While neither of these need be decisive factors, they are relevant to an all things considered judgment. Where a surveillance device is widely used and accepted, people may not have a reasonable expectation of privacy in information that it can uncover. For example, Erving Goffman observes that on the Shetland Islands, it was common practice for residents to observe their neighbors with pocket telescopes, given the Islands' strong maritime tradition. One would "check constantly what phase of the annual cycle of work one's neighbors were engaged in."[29] Given this practice, Shetlanders could not reasonably expect privacy against observations using these telescopes.

But that a device's use is prevalent does not mean all of its uses are legitimate. Though pocket telescopes are commonly used on the Shetland Islands, using one to peer though a hole you drilled into your neighbor's backyard shed to observe what they do inside is not legitimate.

This is a particularly important point when we think about using GPS devices to track a person's movements. GPS devices are widely available and used to find one's location or destination. Sometimes the device is used to monitor the location of someone else. Dispatchers of trucks, taxis, buses, and delivery vans use them to track employees; parents use them to track their children; antitheft systems incorporate them to locate stolen vehicles; and most new cell phones include Enhanced 911, which allows a caller facing an emergency to be located using GPS technology.[30] Some have argued that because these uses of GPS devices are [609] prevalent, covert GPS surveillance is legitimate.[31] But that conclusion is unwarranted. All of the above uses must be distinguished from use of GPS devices to track a person's whereabouts over time without their consent. With each of the above uses there is implied or express consent, as when a consumer purchases a vehicle with an anti-theft tracking system, or parents consent to track their children; or there is an employer-employee relation in which expectations of privacy are limited; or in the case where Enhanced 911 is used, movements are not tracked over extended

[29] See Goffman, p. 15 n. 3; cited in Tunick, Practices and Principles, p. 158. Cf. Tunick, Practices and Principles, ch.5, for a discussion of the role played by both social practices and public opinion (as measured in surveys) in evaluating whether expectations of privacy are reasonable.

[30] John S. Ganz, "Comment: It's Already Public: Why Federal Officers should not need Warrants to use GPS Vehicle Tracking Devices," 95 Journal of Criminal Law & Criminology 1325, 1330-1 (2005).

[31] Ganz, pp. 1343-7.

periods of time so as to provide a record of one's activities throughout the day. The point here is not that even though GPS surveillance is prevalent, prevalent use of technology, if misused, might be regarded as illegitimate by appealing to the value of privacy, though that is true; it is, rather, that the use of GPS surveillance that is prevalent is fundamentally different than its use by police: we can't point to the prevalence of consensual GPS surveillance to show that nonconsensual, covert use by the police is legitimate.

Even if nonconsensual GPS surveillance by police were prevalent, that a particular sort of surveillance is prevalent does not itself make it legitimate. Some social practices of surveillance may be prevalent but not legitimate because they violate accepted normative standards, or undermine values that we think society ought to recognize (see section (c) below).

Another indication that existing behavior, even if prevalent, may not be legitimate is if the behavior is prohibited by law. This can be an unreliable indication since laws may not accurately reflect societal values: some laws are not enforced because they are thought to be obsolete and are still on the books only because the legislature has not gotten around to revoking them; some legislation that is enforced results from such undue influence of certain interest groups that it would be unpersuasive to say that the behavior the law supports is legitimate because it is legal; [32] and some judge-made law can arise from court decisions we regard as mistaken. But if we recognize limitations such as these, laws can be a helpful indication of what activities are accepted and legitimate.

A number of court opinions and state laws prohibit use of GPS devices in non-emergency situations without the clear consent of the person being tracked. For example, a car rental company that used GPS devices to determine whether their customers were subject to a penalty for driving the rental cars out of the state, in violation of the rental car agreement, was ordered to reimburse the customers and fined for unfair pract-[610]ices.[33] One court recently held that when a husband placed a GPS device on his wife's car without her knowledge he violated the state's stalking statute.[34] Several states and the federal government have enacted or are considering legislation requiring disclosure that a vehicle is equipped with a vehicle data recorder.[35]

There is little reason to think that this recent trend is the result of inordinate influence of particular interest groups and does not reflect societal values. At least presently, one can probably make the case that some uses of GPS devices are prevalent and accepted, but not use of the device to covertly monitor a non-consenting individual's whereabouts over time, by relying on a descriptive account of social practices and laws, without having to resort to the additional consideration of whether the uses, even if prevalent, comport with normative standards that

---

[32] Spencer, pp. 857-61.

[33] Ulysses Torassa, "Car Rental Firm to Repay Customers Tracked by GPS," *San Francisco Chronicle*, Nov. 10, 2004. Cf. American Car Rental, Inc. v. Commissioner of Consumer Protection, 273 Conn. 296, 869 A. 2d 1198 (2005). At least two states have enacted laws prohibiting rental car companies from using a GPS to impose penalties on renters, see California Civil Code Sec. 1936; N.Y. Gen. Bus. Law Sec. 396-Z.

[34] *People v. Sullivan*, 53 P. 3d 1181, 1183-4 (2002), referring to Colorado Statute 18-9-111(4)(b)(III), C.R.S. 2001.

[35] NHTSA 49 CFR Part 563 (requires notice in owner's manual that vehicle is equipped with Event Data Recorder); California Vehicle Code Sec. 9951; Colorado S.B. 224; Maine L.D. 1885; N.H. H.B. 599; Virg. H.B. 816. At least 12 states have enacted and 8 have introduced similar legislation, see National Conference of State Legislatures, "2008 Privacy Legislation Related to Event Data Recorders ("Black Boxes") in Vehicles" (December, 2008), http://www.ncsl.org/programs/lis/privacy/blackbox08.htm (accessed May 9, 2009).

reflect the importance of our interest in keeping our location private. But if recent court decisions permitting police use of GPS surveillance without a warrant come to establish it as a prevalent and accepted means of inquiry, to make this case one would need to appeal to the importance and value of privacy.

(c) The value of privacy

Existing laws and prevailing practices of observation, while important, are not decisive in determining what means of observation are legitimate. Eavesdropping was prevalent in Nazi Germany and the Soviet Union, but this descriptive fact does not justify the practice in those societies.[36] Even if existing laws and practices supported a type of surveillance, it may nevertheless be illegitimate if the value of the privacy we forego from it is too great.[37]

[611]At this point it would be appropriate to provide a detailed discussion of the value of privacy. As there already are numerous accounts evaluating privacy generally, I shall focus on the more specific, less-discussed, and perhaps puzzling claim that we have an important interest in privacy when in public places.[38] This claim may seem puzzling since public places, by definition, are places where others have a right to be and can legitimately observe us. In public places we cannot expect others to avert their eyes. But there are contexts in which we do, and should, expect privacy even in a public place. If we are softly whispering to an associate in an uncrowded marketplace, out of earshot of anyone else, it is not unreasonable to expect privacy in our conversation even though we cannot reasonably expect privacy in the fact that we are talking to each other (unless our appearance is concealed, perhaps by a disguise or veil). Having protection from technologically aided surveillance of a conversation in this circumstance lets us communicate with friends and associates without having to overcome the obstacle of finding a private place to meet.[39]

A case can also be made that we have an important privacy interest in our movements in public places. We cannot reasonably expect privacy in the fact that we are at a particular public location at a particular time. But GPS surveillance reveals more than that. It tracks a vehicle's movements over time, which is equivalent to following it. In considering whether following a person is legitimate, we need to assess the importance of our interest in not being followed without our consent.

There are at least two distinct ways in which following someone without their consent impinges on important interests. Following someone can threaten a person's autonomy by instilling fear and anxiety in them, and amount to the wrong of stalking. This is illustrated by the

---

[36] See Vladimir Shlapentokh, Public And Private Life Of The Soviet People (1989), p. 181; Bernt Engelmann, In Hitler's Germany (1986), pp. 57, 59, 100, 157, 165; and Tunick, Practices and Principles, pp. 159-60.

[37] Cf. Nissenbaum, "Privacy as Contextual Integrity," pp. 145-6; Solove, "Conceptualizing Privacy," 90 Cal. L. Rev. 1087 (2002), pp. 1142-3.

[38] For accounts of privacy in general see, for example, Charles Fried, "Privacy," 77 Yale L.J. 475 (1968); Ruth Gavison, "Privacy and the Limits of Law," in Schoeman, ed; Stanley Benn, "Privacy, Freedom and Respect for Persons," in Schoeman, ed.; Edward Bloustein, "Privacy as an Aspect of Human Dignity," in Schoeman, ed; James Rachels, "Why Privacy is Important," in Schoeman, ed.; Daniel Solove, "Conceptualizing Privacy"; Jeffrey Rosen, The Unwanted Gaze (NY: Random House, 2000); and Mark Tunick, "Does Privacy Undermine Community?", Journal of Value Inquiry 35:517-34 (2001).

[39] Elizabeth Paton-Simpson, "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places," 50 Univ. of Toronto L.J. 305 (2005), p. 343; cf. Nissenbaum, "Protecting Privacy."

.

findings relied upon by one court that ruled that a husband who covertly placed a GPS device on his estranged wife's car violated a stalking statute: upon suspecting she was being followed, the wife experienced fear, physical [612] ailments, anxiety, loss of sleep, took alternate routes, and had to take a leave of absence from work and enter a safe house.[40] Some theorists would characterize such violations of autonomy as violations of privacy by invoking a particular conception of privacy, the right to be let alone.[41] Others are troubled by this association of autonomy with privacy. They argue that the wrong involved when you violate someone's autonomy by, for example, assaulting them, may bear little resemblance to the wrong involved when you conduct an unreasonable search.[42]

When we are aware we are being followed, our autonomy is diminished insofar as we feel fear, anxiety, and restrict our activities. But autonomy is not the only value diminished when we are followed. Our interest in not being followed must involve something more than an interest in not suffering the fear and anxiety that comes from being stalked, for otherwise we would have no interest in privacy against skillful surveillance of which we are unaware. The other interest that is threatened by someone who follows us without our consent is our interest in informational privacy. When I am followed, information about my movements that I may want to keep private is exposed. To appreciate the interest in not having this happen, we need to envision life in a society in which our location can at any time be inferred. Deceivers and rule violators would have reason to object to such a society for their infelicities could be discovered. For example, those driving above the posted speed limit could be easily detected by GPS surveillance, which can record speed as well as location; and employees might no longer be able to abuse their company's leave policy by calling in sick when they actually are out and about. But some deceptions, and some rule-violations, are justified. A GPS might detect employees interviewing for a new job; and may be unable to distinguish the subset of speeders who drive recklessly from those who speed safely with the flow of traffic.[43] It might expose deceptions we employ to avoid hurting the feelings of someone who is [613] vulnerable or confronting someone who is unreasonable, or to preserve beneficent surprises. As GPS surveillance could not distinguish such cases, it might deter too much. A world in which our activities can be inferred and discovered might not be unwelcome for uncompromising moral absolutists. One argument against a regime of exposure is that it would create anxiety in everybody else, putting people in the position of having to explain their choices.

If our location at any time could be exposed by government, or by anyone who could reveal this information to those we don't want to know, we may feel compelled to avoid the risk of discovery. This might mean refraining from activities we want to keep secret, such as going to a psychologist, drug-treatment center, job interview with our firm's competitor, or any number of places where we are inclined to enjoy a lifestyle we don't want just anyone to know about. Even

---

[40] People v. Sullivan, 53 P.3d 1181, 1185 (2002). The wife suspected she was being followed because of comments the husband made to her about her whereabouts. Cf. Nader v. General Motors Corp., 25 N.Y.2d 560; Paton-Simpson, p. 325.

[41] Samuel Warren and Louis Brandeis, "The Right to Privacy," Harvard Law Review 4:193-220 (1890), reprinted in Schoeman, ed.

[42] Solove, "Conceptualizing Privacy," p. 1102. On the other hand, Judith Jarvis Thomson doesn't think there is a distinct right to privacy: a violation of what we call a right to privacy can be understood as a violation of some right other than privacy, such as a right over our person or a right to property; in "The Right to Privacy," Philosophy and Public Affairs 4(4):295-314 (1975), 296.

[43] See "Poll: Most Californians Speed—and Feel No Guilt," San Jose Mercury News (Feb. 19, 1993), 3B.

though our activities may be legal and entirely innocent, we may be deterred from engaging in them in order to avoid mere appearances of impropriety, and the perhaps ill-founded speculations they could generate.[44] But the promotion of individual liberty is not the only benefit of informational privacy. If we do not suspect we are under surveillance, we might take no deterrent measures and our liberty would not be restricted, but the actual loss of informational privacy resulting from the surveillance could result in psychic or material injury. Moreover, privacy is not just important for individuals. Theorists of privacy have noted that privacy promotes an autonomy that can be essential for community; and that it is essential for democracy to function well. [45] Privacy may seem to be valuable only for deceivers and criminals, and one might think that protecting privacy facilitates only fraud and deception.[46] But we must keep in mind all of the ways in which presenting a public persona, or not having to explain ourselves, can be essential for the well being of individuals and communities.

Being aware we are followed without our consent can engender anger, embarrassment, and resentment; it can threaten our autonomy by making us fearful and anxious, and by deterring us from engag-[614]ing in some activities. If we are unaware that we are personally under surveillance, but we live in a society in which we know government is permitted to follow our movements, our informational privacy is at risk, making us less able to control our public persona. The interests we have in autonomy and in informational privacy, while distinct, have similarities: threatening these distinct interests can have similar chilling effects.

To summarize the argument so far: the plain view principle tells us that we may reasonably expect privacy in information unless that information is in plain view of anyone engaged in legitimate means of observation. That information about ourselves could be uncovered by a snoop does not mean we cannot reasonably expect privacy in that information, because snoops generally act not legitimately, but badly. This idea is the basis for the mischance principle. In deciding whether a means of observation is legitimate we may need to supplement the mischance principle with appeals to other standards of legitimacy, such as whether a means of observation is prevalent, accepted, or legal, or whether even prevalent and legal activities nevertheless undermine important values to such an extent that we should regard them as illegitimate.

Using the above considerations, we might be led to conclude that lip reading a conversation not directed at you, going through someone's garbage, or using GPS surveillance surreptitiously would always violate reasonable expectations of privacy because they cannot occur accidentally, are done without the effected person's consent, and are not otherwise regarded as legitimate activities. But another conclusion is possible. The mischance principle holds that we may have a reasonable expectation of privacy in information unless that information *could be* discovered accidentally without snooping. It leaves open the possibility that if what the snoop discovers could have been discovered by a non-snoop, we might not reasonably expect privacy in that

---

[44] Glancy; Reiman, "Panopticon," pp. 35-8; and Daniel Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," 44 San Diego L. Rev. 745 (2007), p. 765 (surveillance "can inhibit people from engaging in" legal activities), and p. 766 ("Having nothing to hide will not always dispel predictions of future activity").

[45] Tunick, "Does Privacy Undermine Community?"; Solove, "'I've Got Nothing to Hide'," 762; Nissenbaum, "Contextual Integrity," 146, 150; Priscilla Regan, Legislating Privacy: Technology, Social Values, and Public Policy (Chapel Hill: University of North Carolina Press, 1995).

[46] Richard Posner, "The Economics of Privacy," American Economic Review 71(2):405-9 (1981), p. 406: protecting private facts is like allowing concealment of defects, inefficiently reducing the amount of information available.

information. In the next section I turn to what in the introductory section I called the second objection: if information could be uncovered using a legitimate means of observation, may police use any means at their disposal to obtain that information?

IV. Using technology as a substitute for legitimate means of observation

Recall Example (1), in which I discard some papers in a garbage bag, a raccoon claws its way through the bag, and the papers fly out and rest on the driveway of my neighbor, who innocently picks up and reads them. One might argue that if my papers can be discovered accidentally in this way, then it doesn't matter if they are in fact discovered by the police breaking open the bag and searching through it. If so, one adopts what I [615] call the "object-relative" principle:

> Object-relative principle: *If information could be discovered by anyone using legitimate means of observation, then one has no reasonable expectation of privacy in this information even if the information is actually uncovered by illegitimate means.*

But we might think it does matter whether the police rifle through garbage like snoops or fortuitously discover information using legitimate means of observation. The object-relative principle can be distinguished from a more restrictive "search-relative" principle:

> Search-relative principle: *Only where a search is made using legitimate means of observation is there no reasonable expectation of privacy against the search.*[47]

Whether we should prefer the object-relative or the search-relative principle is a difficult question. I am not sure I have a satisfactory answer, and in this article I will be content to lay out the choice and point to a few reasons for preferring one or the other principle (section (b), below). I first argue, though, that the choice is irrelevant in deciding whether GPS surveillance violates a reasonable expectation of privacy. If we adopt the search-relative principle we would allow GPS surveillance only if we recognize it as a legitimate means of observation. If we adopt the object-relative principle we would allow GPS surveillance if the information it uncovered could have been discovered using legitimate means of observation. Because I think neither condition is met, I believe both principles rule out GPS surveillance without a warrant.

(a) Applying the search-relative and object-relative principles to GPS and video surveillance

GPS tracking of someone without their consent is snooping: the information it reveals cannot be obtained accidentally and is not voluntarily conveyed; and the tracker should know this information is not meant for them, given that surreptitious GPS surveillance is not prevalent and may be illegal in a number of jurisdictions. If we accept this conclusion, we still cannot rule out GPS surveillance. If a person's movements could have been tracked without the GPS device by following the person using 24 x 7 visual 'dragnet' surveillance, then if that method of inquiry were legitimate, GPS surveillance would be permissible using the object-relative principle. This has been the logic of the courts permitting GPS surveil-[616]lance.[48] Is 24 x 7 dragnet surveillance a legitimate means of observation?

The answer may seem straightforward if we regard as decisive the position that snoops act badly, for one's movements over an extended period of time can be discovered only by a snoop and not accidentally, even on a possibilist interpretation of the mischance principle. However, someone who follows another person might deny they are a snoop uncovering information not meant for them, since the person they follow is in a public place. As I have noted, the idea that a

[47] Cf. Tunick, "Privacy," 267-8.

[48] See the cases cited in note 4 and accompanying text, above.

snoop is someone who obtains information which they should know they are not meant to have can be parasitic on our standards for what practices of observation are legitimate.

One standard of whether a means of observation is legitimate may be whether it is legal. Surprisingly there is no authoritative judgment on whether 24 x 7 dragnet surveillance without a warrant violates a reasonable expectation of privacy and is unconstitutional. In the Supreme Court case that comes closest to deciding this issue, *U.S. v. Knotts*, police monitored an electronic beeper they placed in a container of chemicals that was picked up by the suspect, during a single journey of about 100 miles between the location in Minneapolis where the chemicals were purchased and the cabin in Shell Lake, Wisconsin where they were unloaded.[49] The Court allowed use of the beeper because it revealed the location of a vehicle that was being driven on public roads, and which could have been seen in plain view had officers successfully followed it. The *Knotts* Court thus relied on the object-relative principle and assumed that following a vehicle for 100 miles would be legitimate. But the Court declined to decide the issue of whether the police may engage in 24 x 7 surveillance without a warrant, noting that "if such dragnet type law enforcement practices … should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[50] Courts upholding GPS surveillance have relied on *Knotts*, even though in *Knotts* the police followed a vehicle for a relatively brief time and not for days or weeks, which is the length of most GPS surveillance.[51]

Another indication of a practice's legitimacy is its prevalence and acceptance. 24 x 7 surveillance is not prevalent, certainly not if conducted by private citizens as distinct from law enforcers. One way to think about society's acceptance of the practice is to reflect on what a typical reaction would be to being followed without your consent. In some circumstances being followed by a stranger while driving on a public road may cause stress or anxiety but no loss of informational privacy: perhaps you [617] had cut the stranger off and they are tailing you in anger; perhaps they want to meet you. But the situation is different where a stranger, or a team of strangers, follows you for weeks, days, or perhaps just hours. The point at which being followed instills fear, anxiety, or resentment will depend on the circumstances. On a sparsely driven highway stretching for about 100 miles from Minneapolis to Shell Lake, Wisconsin, with few turnoffs, it may not be alarming to have the same car behind you for over an hour—the car may just be following taillights on a dark road for safety's sake—and there is little risk of losing informational privacy; but if you are in a city making numerous turns, being followed for 20 minutes by a stranger might raise concerns. Both examples differ from dragnet or GPS surveillance, which usually extends for days or weeks and which reveals more than the details of a single trip.[52] Such surveillance reveals information about one's location over time that invites

---

[49] *U.S.v. Knotts*, 460 U.S. 276, 278.

[50] 460 U.S. 276, 283-4.

[51] See note 4, and note 52 and accompanying text.

[52] People v. Weaver, 2009 WL 1286044 (65 days); State v. Sveum, 2009 WL 1229942 (five weeks); People v. Lacey, 787 N.Y.S. 2d 680 (over three weeks); State v. Campbell, 306 Or. 157,160-1 (a week); State v. Scott, 2006 WL 2640221 (nearly two weeks); State v. Jackson, 150 Wash.2d 251, 257-8 (three weeks); U.S. v. Garcia, 2006 U.S. Dist. LEXIS 4642 (over two months); U.S. v. McIver, 186 F.3d 1119, 1123 (over a week); U.S. v. Carr, 2006 W.L. 3054323 (five days). In some cases it was used for a day or less: U.S. v. Moran, 349 F.Supp.2d 425, 167-8 (July 29-30); People v. Zichwic, 94 Cal.App.4th 944, 950 (from night of Nov. 13 to about 2 am the following morning, tracking a vehicle through city streets); State v. Meredith, 337 Or. 299, 302 (evening to next day, with real-time monitoring for 90 minutes).

speculation about what one does and who one meets.[53] If the surveillance is discovered, it can engender the harms associated with stalking. What I take to be a commonly shared understanding--that following a stranger for an extensive period of time is not accepted in our society--is supported by the fact that doing so might subject someone to punishment or civil suits under stalking laws.[54]

There are good reasons to think that following someone over an extended period of time without that person's consent is not a prevalent or accepted means of observation. Even if we disagreed with this assessment, one might appeal to the importance of the interest we have in keeping private our location over time, and to the intrusiveness of being followed, in arguing that such surveillance ought not to be regarded as legitimate.

This argument can also be applied to video surveillance of particular locations, when used to track movements. Video cameras are placed in [618] public places in order to deter or detect crimes or perhaps to identify known criminals using face-recognition software.[55] These uses of video surveillance reveal the fact that someone is in a particular location, a fact that is in plain view. One may be hard-pressed today to argue it is illegitimate to situate a video camera outside in a public place so that it uncovers what anyone could legitimately observe, such as who is entering or leaving a house the entrance of which is in plain view.[56] The reason is not simply that video camera use has become prevalent; it is that to have a reasonable expectation of privacy in one's location outside would require people to avert their eyes, which is not only inconsistent with prevailing practice but impractical and undesirable. So long as police place the camera where anyone might legitimately be at any time-- and not, for example, on a power pole to monitor a suspect's otherwise hidden backyard--they do not, the argument goes, violate a reasonable expectation of privacy.[57] There may be good reasons to object to the police surreptitiously pointing a video camera at your front door to monitor who goes in and out—such monitoring is more objectionable than being observed in a park for hours by an elderly woman who doesn't know who you are, precisely because she does not seek information about you, whereas the police who monitor the camera do. But I shall not pursue those objections here. Whatever we think of such video surveillance, it differs categorically from surveillance of someone's movements in public.

---

[53] State v. Jackson, 150 Wash. 2d 251, 262 (it provides a "detailed picture of one's life").

[54] For example, Cal. Civil Code §§ 1708.7; Kentucky Stat. Sec. 525.070 (1)(d)(1996); Mich. Comp. Laws. Ann. §750.411(h); 720 Ill. Comp. Stat. 5/12-7.3(2001); Haw. Rev. State. §§711.1106.4-1106.5(2000); Conn. Gen. State. §§53a-181d-181e(2001); Wis. Stat. Ann. §940.32(2000); cf. Souder v. Pendleton Detectives, 88 So 2d 716 (1956) (tort action).

[55] Christopher Milligan, "Note: Facial Recognition Technology, Video Surveillance, and Privacy," 9 S. Cal. Interdisc. L. J. 295 (1999); GAO, "Video Surveillance: Information on Law Enforcement's Use of Closed-Circuit Television to Monitor Selected Federal Property in Washington D.C.," www.gao.gov/new.items/d03748.pdf (June, 2003; accessed May 9, 2009).

[56] Courts agree, e.g. State v. Fellows, 84 Wash. App. 1088 (1997); U.S. v. Aguilera, 2008 WL 375210 (E.D.Wis. 2008). Cf. Jesper Ryberg, "Privacy Rights, Crime Prevention, CCTV, and the Life of Mrs Aremac," Res Publica 13:127-43 (2007), arguing that because there should be no moral objection to an elderly and immobile woman looking out her bay window onto the street for the entire day, it is hard to support the view that using video cameras to observe public places violates a right to privacy. But see Lever, and Goold, who object when the camera is placed there by the state.

[57] While a power company lineman could have seen over the fence when making a repair, we should not expect that a person would be situated on a power pole for an extended period of time. Cf. U.S. v. Cuevas-Sanchez, 821 F. 2d 248, 250-51 (1987).

If video cameras were placed at every street corner, and law enforcement officers, without probable cause and a warrant, monitored all of the cameras so as to determine that a suspect was at location A at time t_1, location B at t_2, and so forth, in order to, in effect, follow the suspect over an extended period of time, their use of these cameras would go beyond the legitimate uses of deterring or detecting crimes at particular [619] locations, or locating wanted criminals with outstanding warrants.[58] One can plausibly argue that either a warrant would be needed to track the suspect's movements, or there would need to be a compelling public interest in preventing a potential harm, an interest sufficient to outweigh the cost in lost privacy. If video cameras were placed extensively in all public places and the images stored, and there were inadequate safeguards against aggregating this information to reveal a person's movements, then as a practical matter the very presence of these cameras would be objectionable.

(b) Choosing between the Object-Relative and Search-Relative Principles

Suppose, contrary to this argument, that 24 x 7 visual surveillance without a warrant was legitimate. Would the acceptability of government dragnet surveillance mean that the police may instead use motion-activated video surveillance, satellite imaging, or GPS tracking as a shortcut to avoid the difficulty and expense of assembling the manpower required for dragnet surveillance, or to preserve the safety of its officers? What if the police would not have been able to uncover the information they seek using visual surveillance by officers, because they could not afford it, or the officers would have been spotted by the suspect?

One might think that we need not prohibit police from using ethically suspect means of surveillance as a shortcut to avoid the inconvenience of using legitimate means of surveillance. If the use of technologically sophisticated surveillance provides the same information that could be obtained without those methods, why should it matter to our expectation of privacy how the police actually got their evidence?

But there are reasons to prefer the more restrictive search-relative principle. First, it holds the government to higher standards than citizens are presently held to, which may be desirable given the government's vast powers to restrict individual liberty. It prohibits government, without probable cause, from acting like snoops.

Another reason to resist the use of substitutes for legitimate means of observation is that technologically sophisticated surveillance methods, or even unsophisticated tactics used by snoops such as sifting through garbage, may provide more information than could be revealed legitimately, making the search more intrusive. Tracking a vehicle with a GPS obviously provides more information than attempts at visual surveillance that suspects successfully evade. Some uses of technology are more intrusive [620] because they reveal information that would not otherwise be available.

Not all uses of technology make a search more invasive. When an agent tapes an incriminating conversation with a defendant, the recording technology provides an accurate record that, without the recording, might be imperfect due to flaws in the agent's memory; but it does not reveal information that was not already revealed without use of the device, and so using the device does not necessarily increase the intrusion upon the defendant's privacy. Some have argued that technology can make surveillance less intrusive. For example, the Supreme Court of Vermont argued that police use of a video camera with a motion sensor is less intrusive than in-

[58] Such surveillance is analogous to aggregation of data: while providing bits of data about myself to different entities may not violate my privacy, aggregating that data can frustrate privacy interests, see Solove, Digital Person; and Nissenbaum, "Privacy as Contextual Integrity."

person surveillance.[59] But we must be cautious about that claim. A video camera is less likely to be detected than in-person surveillance, and therefore less likely to threaten the target's autonomy by intimidating or creating anxiety in them. Using technology as an alternative is in this sense less intrusive. But in-person surveillance is more intrusive in this sense only if it is discovered, and if it is discovered, it is less likely to uncover private information (although it is likely to constrain the liberty of the subject of the surveillance). While technologically sophisticated devices may be more immune to detection, that makes them more of a threat to informational privacy and in that sense more intrusive.

Permitting government to discover information using illegitimate means of observation merely because the information could be discovered in other ways is theoretically problematic regardless of whether the information the government uncovers is more comprehensive and detailed. Suppose your spouse shares a secret with you that only the two of you know. Each of you has an important privacy interest in this secret. Some philosophers argue that one of the most important reasons privacy is valuable is that it enables just these sorts of secrets, which are essential to the preservation of intimate relationships.[60] Now suppose the two of you separate with enmity, and you decide to reveal the secret to others, in order to embarrass and hurt your former spouse. They may not be able to reasonably expect privacy in the secret since they voluntarily conveyed it to you and assumed the risk that you would reveal it to others. Even according to the search-relative principle, one assumes the risk when sharing secrets with a friend or loved one that they will tell the police, as there is nothing illegitimate in the police listening to informants who voluntarily come forward. But according to the object-relative prin-[621]ciple, the possibility that a friend or loved one with whom you share a secret could betray you warrants the government taking any means whatever to uncover the secret, short of violating criminal or other laws, such as laws against trespass, wiretapping, or battery. Adopting the object-relative principle would in theory create a tremendous deterrent to sharing intimate secrets.

On the other hand, should the police be hampered in their pursuit of criminals and terrorists by the additional restrictions in their ability to uncover information that the search relative principle would impose? Should we limit police resourcefulness while criminals are able to take advantage of advances in technology to avoid detection?[61] Of course if we agree that privacy is important, and we fear government abuse of its police powers, and don't think it should be permitted to engage in illegitimate means of observation absent the special justification provided by a warrant, then our answer would be yes. But many may think that the government's interest in detecting and deterring crime and terrorist acts is too strong to simply reject the object-relative principle outright, even recognizing all that can be said against the principle. A blanket adoption of the object-relative principle has troubling theoretical implications; if it were to become widely adopted, it might be hard to avoid the conclusion that because someone I trust a secret to could betray my trust and reveal the secret to the police, I cannot reasonably expect privacy in any

[59] *State v. Costin*, 168 Vt 175 (1998).
[60] See Fried, "Privacy." Daniel Solove points to ways in which privacy involves more than preventing disclosure of secrets—see Solove, "Conceptualizing Privacy," 1099; and Solove, "A Taxonomy of Privacy." I agree that there are many important senses in which privacy can be violated. But I do think Fried's account captures one of these important senses when we think about informational privacy.
[61] Cf. U.S. v. Scott, 975 F. 2d 927, 930: "There is no constitutional requirement that police techniques in the detection of crime must remain stagnant while those intent on keeping their nefarious activities secret have the benefit of new knowledge."

information I reveal to anyone, against virtually any sort of search. We might accommodate the concerns of these competing positions. While rejecting a blanket adoption of the object-relative principle, we could permit exceptions to the search-relative principle when there is a good reason to allow the government, without a warrant, to use illegitimate means of observation to uncover information (and no more) that could have been discovered legitimately. Assuming that the surveillance the government wants to undertake is not more intrusive than what legitimate means of observation would reveal, a good reason for allowing police to use substitutes for legitimate means of inquiry might be if doing so were necessary to protect their safety; but that the legitimate means of inquiry was unlikely to succeed, or too expensive, might not be a good reason, in light of what has been said above about the importance of our interest in privacy.

I am sympathetic to the search-relative principle, according to which government is permitted to use otherwise illegitimate means of observation only if they secure a warrant. But I recognize that the issue is com-[622]plex and not one to be quickly resolved. However, I do not think we need to decide whether to adopt the more restrictive search-relative principle for the purpose of deciding whether GPS surveillance without a warrant violates a reasonable expectation of privacy. When GPS surveillance tracks movements over an extended period of time, it does not reveal what could be revealed using legitimate means of observation, insofar as 24 x 7 surveillance that tracks a person's movements violates a reasonable expectation that we will not be followed without our consent.

V. Conclusion

If we recognize the distinct nature of GPS surveillance, that it involves following a person's movements and not the mere spotting of someone in a public place that can happen by accident, we must conclude that GPS surveillance, like use of video cameras to track movements, does not provide a plain view. The prospect of living in a society in which we can be followed—of not being able to limit access to information about our location and movements—and not only the fear we experience when we know we are being followed (for if law enforcement officers are skilled, we would not know)—may convince us that it is reasonable to expect that we are not followed without our consent. If so, we must reject the view that one can never expect privacy in public places.

GPS surveillance also raises the question of whether efficiency and safety are sufficient reasons to allow the use of new technologies of observation. Technologies of surveillance may reveal more efficiently or safely what could be revealed through legitimate means only with some luck, great cost, and considerable risk. Before allowing their use by government we must consider not only these benefits, but also what it means to permit the government to act like snoops when it does not have probable cause for a warrant.

Mark Tunick
Wilkes Honors College
Florida Atlantic University
tunick@fau.edu