http://www.press.uillinois.edu/journals/paq.html

PUBLIC AFFAIRS QUARTERLY
Volume 14, Number 3, July 2000

PRIVACY IN THE FACE OF NEW TECHNOLOGIES OF SURVEILLANCE

Mark Tunick

I. THE PROBLEM

The government routinely conducts aerial surveillance, uses infrared thermal imaging devices, and conducts random drug tests involving sophisticated chemical analysis of urine or hair samples, all without search warrants or probable cause. As technologies continue to develop, the capacity to uncover information will continue to expand. People's movements can be monitored through the use of microchip implants; millimeter-wave cameras can detect concealed weapons; a sensor that detects gravity fluctuations may soon provide the ability to reveal contraband in closed containers.[1] Sometimes the exposing of information by government is not troubling, for the information uncovered is not information a person could reasonably expect to keep private. But sometimes investigators resort to technologically sophisticated devices because they want to find out something that could not be discovered without the device through normal and legitimate means. Should such searches be permitted?

All individuals living in a well-ordered society must expect to have information about themselves revealed to others. If you want a loan to purchase a house you should expect to provide credit information to the lender as a condition of receiving the loan, and having to provide this information to the lender is reasonable. It would be unreasonable when we walk down the street talking to a friend to expect others to avert their eyes or cover their ears. If we don't want them to see or hear us we should not be in plain view and within earshot. But to have privacy in our homes we shouldn't have to whisper while hiding in a windowless and soundproof room. Society has norms of permissible and impermissible methods of gathering information, and we should have to protect what we don't want exposed only against permissible methods of exposure.

Courts decide whether searches by state actors are permissible by asking whether the search violates a reasonable expectation of privacy. The Fourth Amendment to the U.S. Constitution holds that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause." The Supreme Court has interpreted the amendment to hold that the government may conduct searches without a warrant so long as the searches pass a twofold test. First, if the person affected by a search had no expectation of privacy in the object of or information revealed by the search, then the search is reasonable. One problem with this criterion is that in the face of new technologies of surveillance, people may be unaware that their privacy can be frustrated. People unaware that thermal imaging devices can detect heat emitted from their homes may have no expectation of privacy in their heat waste. But it is far from clear that this should mean that use of thermal imaging devices is permissible. Even if the subject of a search has a subjective expectation of privacy, the search is still permissible if it passes the second prong of the Court's test: a search is reasonable even if it frustrates a subjective expectation of privacy if that expectation of privacy is not one society recognizes as objectively reasonable.[2] If someone commits a crime in a public place in plain view then their privacy has not been violated even if they had a subjective expectation of privacy, for in this situation it is objectively unreasonable to expect privacy.

We should expect some disagreement about whether an expectation of privacy is reasonable in a culturally diverse society. In some cultures one knocks at the front door and waits to be let in to a neighbor's home, but in other cultures it is common simply to enter a neighbor's home without advanced warning.[3] Whether a police officer's warrantless search of a home violates expectations of privacy society recognizes as reasonable will depend on the extent to which the norms of that society demand respect of a person's privacy in their home. But the judgment that an expectation of privacy is or isn't reasonable is culturally relative only to a point. Eavesdropping was so prevalent in Nazi Germany and the Soviet Union that few in these societies could expect privacy in their home. But the fact that norms of exposure prevailed does not make these norms right. We can say that the surveillance practices that shaped expectations in these societies violated moral principles by which a free society must live.

The purpose of this article is to develop a principle of privacy ethics to guide us in determining whether expectations of privacy are reasonable in the face of new technologies of surveillance. It must be a principle sensitive to societal norms, but to norms that may themselves be subject to critical scrutiny.[4]

II. Developing a Principle of Privacy Ethics

The approach I take in determining which technologies of surveillance are acceptable and which are unacceptably intrusive is to begin with intuitions about when a search is unduly invasive, intuitions that reflect societal norms. The idea is this: we identify searches we agree are unacceptably intrusive, and those that clearly are acceptable. We then single out the features unique to the former searches and articulate a principle that characterizes what makes them unduly intrusive. This principle becomes a guide for determining whether a search violates reasonable expectations of privacy. The principle can be repeatedly tested against other cases to see if it is consistent with our intuitions. Where the principle contradicts our intuition in a particular case, we can either revise the principle to fit the intuition, or use our principle to correct our intuition.

It may seem troubling to begin with intuitions in developing an ethical principle that is then used to confirm or correct our intuitions. This is akin to deriving what "ought" to be from what "is," a feat found incredulous by some moral and political philosophers. The approach may appear all the more problem-ridden when we reflect on how so many people, trained judges as well as ordinary citizens, have conflicting intuitions about whether particular searches are reasonable. This latter concern becomes less troubling when we recognize that in many cases there *is* considerable agreement about what is and isn't acceptable. The hope is that from these cases of agreement we can develop a principle to deal with cases of disagreement. This ethical approach is called *immanent criticism*. When we adopt immanent criticism, we begin with existing norms and practices of ethical or right conduct, develop an account of the principle(s) immanent in these norms and practices, and then use the principle(s) to criticize actions that violate the principle(s). Objections to and defenses of this methodological approach cannot be considered here but are discussed elsewhere.[5]

I begin with what I take to be a fairly uncontroversial intuition. Where we share a room with others so that there is no visual or auditory barrier between us, we cannot reasonably expect privacy in our activities or conversations in that room. This intuition can be captured by what I call the "unavoidability principle," which holds simply that where exposure is physically or practically unavoidable, there is no reasonable expectation of privacy.

The unavoidability principle has some force. Suppose a couple is staying in the motel room next to yours. They are talking loudly and you can hear every word because the walls are so thin. Is it wrong to overhear their exchange, or must you take active measures not to hear, such as

focusing your attention elsewhere, covering your ears, or turning up the volume on the television to drown out their voices? Straining to hear would seem wrong. But that the couple can be heard without effort and perhaps even unavoidably strongly suggests that they do not have a reasonable expectation of privacy in their conversation, and if we agree with this intuition, then we have some reason to adopt the unavoidability principle.

But there are compelling reasons to reject the principle. One difficulty with it is that there is almost no such thing as physically unavoidable exposure. It is nearly always possible to avoid seeing or hearing something. If the principle proscribed any observation we could avoid making, it would rule out clearly reasonable activity. A police officer has not acted unreasonably when he links me to a crime by picking up an implicating sheet of paper that falls from my hands onto the street. He acts reasonably not because he uncovers a crime, but regardless of the nature of the information discovered.

Where windows are uncurtained, rooms crowded, doors open, walls thin, it is possible for us to avoid finding things out, just as it is possible where exposure is difficult to use our ingenuity to pierce veils; whether the latter is permissible or the former is expected is not adequately explained by appealing to the unavoidability principle. While the principle seems persuasively to explain why there is no reasonable expectation of privacy if the conversation of our couple in the motel could not but be heard next door, it cannot tell us whether it would be wrong to put a stethoscope, glass, or ear to the wall to hear the conversation. Where a conversation can remain private but can also easily be heard either accidentally or by a resourceful snoop, we need some other principle to tell us whether an expectation of privacy in that conversation is reasonable.

It seems more unethical to use a glass or stethoscope to overhear a conversation next door than to overhear it simply by listening with the naked ear. We might conclude from this intuition that a search that uses sense-enhancing devices violates reasonable expectations of privacy.[6] This "no sense-enhancement principle," given a proper formulation that allowed for the use of sense-enhancing devices such as contact lenses or hearing aids, which compensate for individual defects but do not provide capacities exceeding the abilities of the average well-functioning human being, would be especially effective in dealing with new technologies of surveillance, at least from the perspective of privacy advocates. For in effect it would rule out the use of sense-enhancing devices without a search warrant.

Why adopt the no sense-enhancement principle? People form expectations of the sorts of measures they need to take to protect their privacy,

expectations of the sorts of intrusions they reasonably can anticipate. These expectations are largely based on the capacities of the average human being, which is why use of contact lenses does not undermine anyone's expectations, for the lenses don't expand the capacities of observers that we need to take into account to preserve our privacy. But new technologies that expand information-gathering abilities beyond those of the average human being unsettle these expectations, unfairly changing the rules of the game and requiring those who have already taken reasonable precautions either to further limit their liberty or to incur added expenses to maintain their privacy. The no sense-enhancement principle preserves the important values of liberty and fairness above and beyond protecting the value of privacy.

There are two problems with this principle. First, it seems wrong to put an ear to a wall to listen to a conversation, and not just wrong to use a glass or stethoscope, so the use of a sense-enhancing device does not itself make otherwise ethical behavior unethical, and an otherwise legitimate search illegitimate. If I have a reasonable expectation of privacy in the contents of my diary, then you act unethically whether you use your natural abilities to rip it open and read it against my wishes, or whether you use a super-sophisticated wall penetrating x-ray device that lets you read my diary's contents from afar.[7] The converse is true as well, and leads to the second objection to the no sense-enhancement principle. If I am using drugs in my first floor curtainless windowed studio apartment in plain view of people walking along the sidewalk outside, then I have no reasonable expectation of privacy in my activity against either a random passerby staring through the window, or a narcotics agent using binoculars from a third-floor apartment across the street. The fact that the agent uses binoculars seems to make no difference so long as the information he uncovers is of the same quality and detail as that which could be discerned by the passerby from the sidewalk. Similarly, if in using a stethoscope against the wall separating her motel room from the noisy couple next door a detective hears precisely the same information that could be heard in the same room without making any effort at all to hear the conversation, then while we may look askance at the detective's overzealousness, it is hard to make the case that she violated a reasonable expectation of privacy (although later I shall consider a way in which the case might be made). Whether a sense-enhancing device is used is peripheral to the question of whether the search is excessively intrusive.

Intuitively it makes a great difference whether the conversation by the couple in the motel room next door could have been overheard accidentally, or only by a resourceful snoop. Consider another situation

involving observation of someone in a neighboring motel room. In *U.S. v. Mankani,* an officer with the Drug Enforcement Agency (DEA) checked into a hotel room adjacent to a suspect and, without a search warrant, moved a piece of furniture, knelt down to a hole that fortuitously was in the wall separating the two rooms and which had been obstructed by the furniture, and put his ear to the hole.[8] Without taking these measures the agent could not have heard the conversation next door. Intuitively, where overhearing the noisy couple through thin walls is not obviously wrong, the DEA agent's conduct is. We should seek a principle that captures this difference. Such a principle holds that an expectation of privacy in a place or activity is unreasonable, not if exposure is unavoidable, or occurs without the use of a sense-enhancing device, but when exposure can occur by mischance. On this principle—I call it the mischance principle—where exposure is intentionally undertaken to reveal what could not be accidentally discovered by a non-snoop (someone not intending to uncover information) using legitimate and normal means of observation, there is a reasonable expectation of privacy against such exposure.

In *Mankani,* the DEA agent's hearing the conversation was not, and could not have been, the result of mischance.[9] According to the mischance principle the agent's action violates a reasonable expectation of privacy. This seems to me to be the correct result. The federal court of appeals held otherwise, upholding the warrantless search, on the ground that "the Fourth Amendment protects conversations that cannot be heard except by means of artificial enhancement."[10] The judge writing the opinion appeals to the no sense-enhancement principle. That principle was rejected earlier in part because it fails to proscribe searches using only natural means of perception that are nevertheless unreasonable. We were led to the mischance principle because it captures an intuition the no sense-enhancement principle does not, an intuition the judge seems not to share, but that nevertheless seems right.

The mischance principle does not protect us against all possible exposures. It leaves us exposed to many accidental observations, but protects us against many snoops. It also protects us from searches the very possibility of which we are unaware owing to the newness of the technology involved. This is true so long as the technology reveals what could not be revealed by legitimate and normal means of observation, that is, observation the possibility of which we are aware and which we can therefore anticipate and protect against if we choose.

What justifies the mischance principle? Why should we grant people protection against searches that violate this principle? One defense would appeal to the value of privacy, and the associated values of liberty and autonomy, about which discussions are available in other places.[11] With

the mischance principle enforced, individuals need only take measures to protect privacy against observations they are likely to encounter, without having to worry about taking measures against government agents acting like illegal snoops. The mischance principle affords significant liberty, but not so much liberty as to unfairly hamper law enforcement agents. It is important to see that the mischance principle does not proscribe all intentional exposure by snoops. Such searches are allowed if what they uncover could have been uncovered unintentionally by legitimate means. If I use an FM radio or bearcat scanner to listen in on your cordless phone conversation, I have not violated a reasonable expectation of privacy just because I intended to uncover information, so long as your cordless phone conversation could have been accidentally exposed by anyone with an FM radio or bearcat scanner who was randomly turning the dial to pick up whatever might be out there.[12] The user of a cordless phone can't reasonably expect privacy in her conversation if her phone shares frequencies with FM radios or scanners given how in our society such devices are legitimately used for non-intrusive purposes. Conversely, if I do have a reasonable expectation of privacy against invasion by snoops or spies, the expectation of privacy doesn't become unreasonable simply because the exposer didn't intend to uncover private information about me. When you go through my diary you violate my privacy just as much when your purpose is to expose intimate details of my life as when it is to look for a lost ticket stub or find out the date of a concert.

A utilitarian might try to show that the mischance principle provides an optimal level of social utility, or is economically efficient in not requiring the wasteful expenditure of resources to protect against highly unlikely or illegitimate searches. The justification I rely on in this article is different, though not averse to these other arguments. I arrive at the mischance principle by showing that it coheres with our intuitions about which searches are and are not ethical.

III. Development and Clarification of the Mischance Principle

So far the mischance principle has been presented only in outline, without specifying some of its crucial terms. In this section the principle is further developed and clarified.

One ambiguity in the present formulation of the mischance principle is whether, if we are to retain a reasonable expectation of privacy in information we want to keep private, it must be impossible, or merely unlikely, for the information to be revealed by mischance. Where discovery is likely through legitimate means of observation, an expectation

of privacy is unreasonable. But even where observation of my activity through legitimate and normal means is unlikely, though possible, I still may lack a reasonable expectation of privacy. Observation of a drug deal in a remote part of Central Park late at night is unlikely; but if a police officer by chance happens to be passing by and sees it, he has not violated a reasonable expectation of privacy.[13] The formulation I give the mischance principle literally implies not likelihood but possibility: "where exposure is intentionally undertaken to reveal *what could not be* accidentally discovered by a non-snoop using legitimate and normal means of observation, there is a reasonable expectation of privacy against such exposure." But a less rigid formulation will be required to capture our intuitions in some cases. People should have to expend resources or otherwise take protective measures to ensure their privacy only for what is foreseeable, even if unlikely. But some events are so unforeseeable that it is unreasonable to expect people to anticipate them. Who would anticipate that our private papers that we keep in a locked drawer of a desk in our home, which we also keep locked, might be exposed if our house burns while we're away, the desk is destroyed, and our papers, salvaged but exposed, blow into the hands of the very person who mustn't see them? It's possible for our papers to be exposed in this way, but it would be unreasonable to take measures to prevent this contingency. Requiring people to expend resources for extremely unlikely contingencies such as this would be more wasteful and inefficient than having legal protection against the unwanted consequences of such unlikely occurrences.

While the mischance principle contains the ambiguity about just how unlikely discovery by mischance must be for us to retain a reasonable expectation of privacy, this is not a reason to reject the principle. If a moral principle is to be convincing in the face of disagreement, it may need to provide the very discretion that makes the principle indefinite in the rare hard case. But such discretion need not be open-ended. The mischance principle can be combined with other principles and considerations when its interpretation is ambiguous. One such principle, just hinted at, is a principle of economic efficiency. Another such principle would give weight to the extent to which a practice of surveillance restrains our ability to lead a private life. In our society certain places are assigned special significance for providing this ability, most notably the home. One might wish to apply the mischance principle more stringently when the government intrusion at issue uncovers information about us in our home or one of its surrogates.

The above ambiguity in the mischance principle is related to another. Suppose information about me *could* be uncovered accidentally through legitimate means, but that *in fact* police officers resort to searches that

go beyond normal means of observation to acquire this information: has a reasonable expectation of privacy been violated? Should police be permitted to use new technologies of surveillance as a shortcut that lets them avoid having to rely on the usual, legitimate means of observation and on luck?

Consider a police search of garbage. A police officer, without a search warrant, asks the trash collector in a suspect's neighborhood to pick up the plastic garbage bags the suspect leaves on the curb in front of his house, and to turn them over before their contents are mixed with garbage from other homes. Searching through the rubbish, the officer finds evidence of a crime and with this evidence secures a warrant that leads to further evidence and ultimately a conviction. It's conceivable that the evidence in the garbage bag could've been exposed by an animal digging through it, so does this mean the search by the officer is reasonable?

According to the U.S. Supreme Court in *Greenwood vs. California,* searches of garbage are reasonable. Justice White supports this conclusion by noting that "[i]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public." The police, he adds, "cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public."[14] That our garbage could be exposed accidentally or by snoops means we can't reasonably expect privacy in our garbage, the argument goes.

While few scavengers and children and no animal would read the scribble on our discarded papers, all may undermine the integrity of garbage containers, leaving its contents exposed to the wind. For the dissent in Greenwood, it mattered that this was not in fact how the officer came to the evidence concealed in the garbage. Had "'animals, children, scavengers, snoops, [or] other members of the public' . . . actually rummage[d] through a bag of trash and expose[d] its contents to plain view," police may have been justified in searching for ~~we then~~ in this case we could not expect them to avert their eyes.[15]

[AUTHOR: PLEASE RE-READ THE PRECEDING SENTENCE AND CORRECT]

Is the dissent correct in saying it matters that this is not how the police in this case came to observe the contents of the garbage? Consider the following, more restrictive version of the mischance principle: only where an act of exposure is a sort of activity that society regards as legitimate and that could be employed in a way that accidentally exposes information is there no reasonable expectation of privacy against this exposure. I call this the "search-relative mischance principle" be-

cause it focuses on the means of intrusion, rather than the object being exposed.[16] On this principle the garbage search would be invalid absent a warrant because the police officer did *not* simply view papers scattered in the wind. He did *not* employ legitimate means of observation and happen to get lucky. He acted like a snoop.

Do we need to appeal to this more restrictive principle? If we understand the standard mischance principle to rule out searches that reveal information that would not likely (as opposed to could not) be revealed by mischance, then we would not need the more restrictive principle to prohibit the garbage search, or searches using new technologies of surveillance that uncover information that conceivably but probably would not have been obtained legitimately without the technology. On the other hand, if a police officer uncovers information through use of a technologically sophisticated device not in normal use, but the information she receives is exactly the same as could plausibly have been obtained through legitimate and normal means of observation, then it seems irrelevant that she chose unnecessarily elaborate and technologically advanced means of observation. This was my point earlier when discussing an agent's use of binoculars from across the street to see what any passerby from the street could see. The use of binoculars makes no difference so long as the information the agent uncovers is no more detailed than what could be discerned by the passerby from the sidewalk. One reason the no sense-enhancement principle should be rejected is that it singles out what in itself may be an arbitrary fact—the nature of the device used in the surveillance—as determinative in evaluating the intrusiveness of the search. The more restrictive search-relative mischance principle, like the no sense-enhancement principle, rejects use of technologies not ordinarily used, and so the objections to the no sense-enhancement principle come into play against it as well.

The reason I believe we may feel differently about technologically enhanced searches is that in most situations they are used because they reveal details that are inaccessible without the technology. Even when voices can be heard from an adjacent room with the unaided ear, it is wrong to use a stethoscope because the device lets one pick up additional information—the details of the conversation—and not just the sounds of voices or occasional words, and this information is forbidden knowledge when it could not be obtained without the device. In *U.S. v. Cuevas-Sanchez,* the U.S. Court of Appeals for the 5th Circuit properly refused to extend a precedent permitting aerial photographs of a defendant's back yard to the video surveillance of the defendant's back yard from a power pole bordering his property, because the nature of the surveillance was fundamentally different. It was not a minimal intru-

sion but allowed a continuous record of all activity in the defendant's back yard, and therefore provided information unavailable without use of the technology.[17] But uses of technology that do not provide information beyond what could have been acquired using normal and legitimate means of observation do not violate the mischance principle, and do not violate reasonable expectations of privacy. In practice it may be difficult to establish that, for example, the details of a conversation could have been overheard without use of a listening device, and so in practice there will be a strong presumption against use of sense-enhancing devices. But there is no need to adopt the more restrictive search-relative mischance principle to provide the protection we require.

The mischance principle appeals to a standard of normal and legitimate observation against which the actions of those wielding new technologies of surveillance are judged. The point of the mischance principle is to rule out not the use of technologies that do not currently exist or that are not part of normal use, but the use of new technologies that uncover information that could not otherwise be expected to be revealed through what society regards as acceptable, legitimate means of observation. This raises the question of what counts. Legitimate and normal means of observation is not identical with prevailing practices of observation. The expectations of privacy one can reasonably possess *do* depend on the social practices in one's community: where doors can be entered without knocking, to secure privacy one must be discreet even in one's home. Where windows must be left open to cope with summer heat, criminal plots must be made in whispers. What counts as normal observation or discovery by mischance itself is a judgment that will vary among societies depending on their customs and practices, architecture, and other culturally variant factors. But in some cases prevalent practices of surveillance might be "normal observation," but not legitimate, and therefore they should not be regarded as a standard for ethical conduct. This is the case with some of the surveillance practices prevalent in Nazi Germany, the Soviet Union, and Orwell's 1984. Practices of surveillance may prevail and make it necessary to go to great lengths to secure privacy, but those within a society can appeal to principles or values to criticize these practices and argue that even where there is no expectation of privacy there ought to be one. The values to which we can appeal include those of liberty and autonomy.

One final qualification must be made if the mischance principle is to be persuasive. Consider searches using magnetometers at airports and other searches that while mildly intrusive serve a great and compelling public purpose. Magnetometers reveal the existence of concealed weapons, information that could not be discovered by mischance (that is, by

someone not intending to uncover the information and using normal means of observation), and are therefore ruled out by the mischance principle as it is presently stated. But these searches are eminently reasonable. Any principle that bars them can't be correct. This example points to how some searches, while invasive, are nevertheless justified on balance because of the great advantage they provide society. Magnetometer searches help prevent hijacks and bombings, so most people gladly consent to them. But even without the search subject's consent, use of magnetometers is still justified. In this case, a technology of surveillance, because its benefit far outweighs its cost in terms of intrusiveness, is legitimate. The mischance principle is persuasive when applied to new technologies of surveillance only when we revise it by adding the proviso that *if use of new technologies of surveillance reveal what could not be exposed to a non-snoop by mischance but in a way that has little or no costs to privacy, and for a worthwhile end that clearly outweighs whatever minimal costs to privacy there may be through general use of this technology of surveillance, then the use of the technology should be permitted.*

Having now invoked a balancing test as part of a privacy ethics principle, someone might now ask why I don't just rely on a balancing test exclusively to decide all privacy issues, and leave aside the mischance principle. The reason is that a purely utilitarian or balancing test approach would likely fail to give due respect to the value of privacy. The value of privacy can't always be measured or evaluated in a way that would let us compare it to the societal cost of lost convictions, a cost that itself is difficult to measure. We *can* conduct a balancing test when the intrusion on privacy is minimal or nonexistent. We can reasonably conclude, for example, that an important deterrent such as an airport magnetometer search outweighs the loss in privacy of having the fact that one is carrying metallic objects revealed to airport officials. But once a search becomes more invasive, or a moderately intrusive search is used to secure convictions of crimes of which the harm to society is questionable, it seems futile to attempt to weigh a search's invasiveness against the dent in the crime rate that would result from allowing the search. No reasonable person would object to minimally intrusive searches such as airport magnetometer searches that benefit society greatly. A reasonable person could, however, conclude that searches that invade privacy should not be permitted even where the benefit of the search in a particular case may be greater than the loss of privacy suffered, or where the benefit to society of allowing such searches as a rule may be greater than the resulting loss of privacy. Given the difficulty of weighing the loss of privacy against the effect on society of a poten-

tially higher crime rate, the mischance principle is useful as a default, even for committed utilitarians, to ensure that privacy is respected in the many cases where results of a utilitarian calculation are not clear. That there is a *right* to privacy—a "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures"—means that privacy cannot readily be sacrificed for a greater good, and surely not in situations where we are uncertain that its sacrifice would yield a greater good.

In determining whether an expectation of privacy is reasonable, I have argued, we can appeal to the mischance principle, which itself appeals to practices of normal observation that shape what is subject to chance discovery. We ask whether what is exposed by an intentional search could plausibly have been discovered accidentally by normal means of observation. If the answer is yes, before we can conclude that no reasonable expectation of privacy was violated we still need to ask whether society should require that we take measures to avoid the possibility of such accidental exposure, that is, whether that means of exposure should be regarded as legitimate. Finally, where new technologies of surveillance reveal what could not be exposed to a non-snoop by mischance but are nonintrusive and provide information the benefit of which clearly outweighs whatever minimal costs to privacy there may be from general use of the means of surveillance, the use of the technology should be permitted.

The mischance principle's reference to a standard of "legitimate" means of observation, appeal to the pliable concept of plausibility or likelihood of exposure by mischance, and invocation of a balancing test afford discretion to its interpreters that means it is not a rule that can always be applied uncontroversially and without deliberation. Given the complex nature of privacy issues, and the difficulties presented by some hard cases, I take this to be a necessary feature of any acceptable principle of privacy ethics.

IV. The Mischance Principle Applied

The mischance principle is a general theory about the scope of privacy that should be afforded. In this section I show how the principle can be applied to instances of government searches and be used as a critical tool in adjudicating Fourth Amendment cases. The applications let us consider some of the difficult issues that are presented by new technologies of surveillance.

Aerial photography

Dow Chemical Company has a 2,000-acre complex with elaborate security, but it is not feasible for the company to cover the entire area to prevent aerial surveillance. The Environmental Protection Agency (EPA) conducted aerial surveillance without a warrant, using a sophisticated camera costing $22,000 to take photographs. Dow Chemical, claiming that this is a violation of its reasonable expectations of privacy, sought a court order prohibiting the EPA from taking further aerial photographs. In a 5–4 decision the Supreme Court held that the EPA was not violating the Fourth Amendment rights of Dow Chemical.

Assuming that commercial enterprises possess Fourth Amendment rights similar to those possessed by individuals, the mischance principle would proscribe the EPA searches insofar as the information they uncover could not otherwise be revealed by legitimate means of normal observation. The majority of the Court, in upholding the searches, argued that the use of sophisticated surveillance equipment in this case was not decisive, because the photographs "here are not so revealing of intimate details as to raise constitutional concerns. . . . The mere fact that human vision is enhanced somewhat . . . does not give rise to constitutional problems."[18] Chief Justice Burger noted that the camera could not detect details such as a "class ring" or identify faces or secret documents. The very same day as it announced the *Dow* opinion, the Court also announced a decision in a related case, *California v. Ciraolo.* In *Ciraolo,* police had received an anonymous telephone tip that marijuana was being cultivated in the respondent's back yard. Unable to observe the yard from ground level due to a 6-foot outer and a 10-foot inner fence, officers trained in marijuana identification secured a private plane and flew over the house at 1,000 feet, observing marijuana and photographing it with a 35mm camera. With this evidence they secured a warrant of the home and seized evidence used to convict the respondent. The respondent sought to suppress the evidence as the fruit of an unconstitutional search. A 5–4 majority upheld the warrantless search in *Ciraolo.* Chief Justice Burger argued that the marijuana was seen "in plain view." While the respondent may have had a subjective expectation of privacy in his back yard, this expectation is unreasonable because, despite the fences, the contents of the yard still could be discovered accidentally through normal observation: "[A] 10-foot fence might not shield these plants from the eyes of a citizen or a policeman perched on the top of a truck or a two-level bus." Exposure, Burger suggests, could reasonably be the result "of a casual, accidental observation."[19]

The *Ciraolo* decision also holds that aerial surveillance is so prevalent that people should not reasonably expect that activities which can possibly be seen from the skies remain private. Even assuming the Court

is right to think that aerial surveillance is so widespread as to amount to "normal observation," the possibly widespread use of new technologies of exposure does not in itself condone their use. We can appeal to the value of privacy and the related values of liberty and autonomy to criticize some new technologies of surveillance. But it is unnecessary to go this route, because the searches in both *Ciraolo* and *Dow* revealed what could not otherwise be revealed accidentally by a non-snoop through legitimate means of normal observation. Exposure through aerial surveillance can and does occur, just as snoops can and do rummage through our garbage or burglars wrongfully enter other peoples' homes. But if it happens it's not the result of legitimate observation. Snoops and burglars act badly. Nor did the government in *Ciraolo* and *Dow* uncover information by mischance. Identifying any activity in a back yard while flying overhead at 1,000 or even 400 feet (let alone above 10,000 feet, where most commercial passengers fly) requires a concentrated effort, and not a mere accidental, fleeting glance. Such exposure from the skies, while perhaps possible (at least from 400 feet), is not prevalent or commonplace.[20]

No general norm of observation from airplanes or helicopters exists to support the claim that detailed observation of private activities from the skies can occur by accident. And in the case of *Dow* in particular, as Justice Powell notes in dissent, it is not the case that anyone could have obtained the information gained by the EPA, since few could afford a $22,000 camera, and "the camera saw a great deal more than the human eye could ever see."[21]

There are some instances of aerial surveillance, however, that can be regarded as normal and legitimate observation. In remote wooded areas official flights often occur in order to seek out forest fires, and where this is the case, people living in such areas cannot reasonably expect open fields to be free from aerial observation. Airplanes that are regularly used for legitimate public purposes and not intended to invade privacy rights may reveal information accidentally in the course of legitimate activities, and such searches would not violate the mischance principle.[22] However, if the government used a plane equipped with special detection devices not ordinarily used, for the purpose of uncovering information someone in that area could reasonably expect to be private and not subject to exposure through legitimate and normal observation, the mischance principle would be violated.

Aerial surveillance is invasive. Unlike magnetometers, which generally reveal only the presence of weapons one has no right to possess, observation from planes and use of sophisticated cameras can expose information people legitimately have an interest in keeping private, such as proprietary information, or the fact that one sunbathes nude. Permitting

such searches as a rule would significantly limit liberty, increase anxiety, and perhaps cause people to incur significant costs to preserve their privacy, and these costs do not clearly outweigh the benefit to the government of conducting its warrantless searches.

Thermal Imaging Devices

A forward-looking infrared radar (FLIR) reveals heat sources through a monitor. Existing devices can detect the heat from a person leaning against a relatively thin barrier such as a plywood door. The device also can disclose which rooms a homeowner is heating, perhaps his financial inability to heat the entire home, and possibly the number of people in the home.[23] Some models can apparently determine the level of coffee in a cup, or detect tear ducts on a human face.[24] Normal uses include locating missing persons in a forest, identifying inefficient building insulation, and detection of forest fire lines through smoke. The device is increasingly used by law enforcement agents to detect marijuana growing labs.

Use of FLIR devices has more often been upheld then disallowed by courts.[25] Courts have declared that there is no legitimate expectation of privacy in "heat waste," and that the device is not very intrusive.[26] Most people, unaware of this new technology, have no subjective expectation of privacy in the amount of heat emitted from their homes. But this does not mean they have no subjective expectation of privacy in the activity in their home that the FLIR device may help reveal.[27] Even if people do not have a subjective expectation of privacy against a type of search the existence or possibility of which they are unaware, they can retain an expectation of privacy in the information about themselves that the search uncovers. But what I take to be an even more compelling reason to ignore the first prong of the Supreme Court's two-part test is that it has increasingly become irrelevant in the face of new technologies of surveillance. Requiring a subjective expectation of privacy only encourages a regime to promote secret technologies that excessively restrict privacy and the associated values of liberty and autonomy.

One of the few decisions invalidating FLIR searches without a warrant takes as determinative the fact that FLIR devices are technologically sophisticated and reveal what is not in plain view.[28] I have argued, in contrast, that the use of new technologies of surveillance is not in itself constitutionally suspect. The use of technology is suspect only where the technology reveals what could not otherwise be revealed by mischance through normal and legitimate means of observation.

The mischance principle would seem to rule out FLIR searches. The device reveals information that could not be obtained by accident through

normal, legitimate observation. According to the *search-relative* mischance principle, the search was improper. However, if excessive heat of the sort that could prompt a judge to issue a warrant for a search of the premises could be revealed simply by "feeling" heat being released from the building, then according to the *standard* mischance principle, the use of a high tech sensory device would be permissible, since the information it uncovers could plausibly have been revealed by legitimate means. But since it is not possible to obtain probable cause for suspecting the existence of a marijuana lab merely by walking past the outside of a building and feeling heat, use of the FLIR device is necessary, and where technology is used to gather what could not otherwise be gathered by normal and legitimate means of observation, even the standard mischance principle proscribes its use.

This conclusion may seem troubling. As noted earlier in the discussion of airport magnetometers, Fourth-amendment adjudication requires some balancing of interests, where we weigh the benefits to society of allowing searches that can detect crime against the intrusiveness of these searches. Whether a new technology of surveillance is permissible depends on its level of intrusiveness, and this crucially depends on the capabilities of the technology. If FLIR devices expose details that people have a legitimate interest in shielding, then the mischance principle would explain why warrantless searches using the device would be unacceptable. If the devices could reveal legitimate, non-criminal activities in one's home, then especially in light of the special protection the home receives in Fourth Amendment case law, we should probably find the potential intrusiveness of such searches to outweigh the benefit of allowing the police to uncover marijuana labs through a shortcut of using the FLIR device without probable cause. A majority of courts, concluding that FLIR devices cannot reveal such activities, have held that privacy is not really at stake and the searches are justified on balance. If their assessment of the devices' capabilities is accurate, this conclusion is reasonable. But this assessment may not be accurate. Some FLIR devices are advertised as having the ability to "monitor activity in critical rooms or large facilities."[29] In one case, an officer using the device admitted that the response he received from the device could have been triggered by a common dehumidifier.[30] The device cannot distinguish between the growing of marijuana and the growing of tomatoes. It therefore potentially reveals noncriminal activities inside one's home. Since our society regards activities in one's home as especially deserving of privacy protection, a device that uncovers activities in the home, activities that would not otherwise be revealed, frustrates legitimate privacy interests.

Judges who uphold FLIR searches on the ground that it is not invasive put themselves in a bind: either the device does provide enough information to establish probable cause that a crime is being committed, in which case it does have the capacity to reveal activities in one's home and is therefore invasive; or it does not have this capacity, in which case a judge should not issue a search warrant merely on the basis of the findings of an FLIR search.[31] Given this uncertainty concerning the invasiveness of the device, it may be difficult to conclude that the benefits of convicting marijuana growers clearly outweighs the cost to individuals' privacy imposed by use of the device.

Florida Atlantic University

NOTES

1. *New York Times*, June 12, 1999, p. A9; *Aviation Week and Space Technology*, September 16, 1991, p. 66.

2. Katz v. U.S., 389 U.S. 347 (1967), at 361.

3. Native Americans had to be taught the unfamiliar practice of knocking at the door first and asking leave to enter before coming in. See David Flaherty, *Privacy in Colonial New England* (Charlottesville: University Press of Virginia, 1967), pp. 88–89.

4. For a detailed account of the ways in which culturally variant practices affect expectations of privacy, that includes an earlier statement of the principle I develop in this article, see Mark Tunick, *Practices and Principles: Approaches to Ethical and Legal Judgment* (Princeton, N.J.: Princeton University Press, 1998), chapter 5.

5. See Mark Tunick, *Punishment: Theory and Practice* (Berkeley: University of California Press, 1992), chapters 1, 5.

6. Robert Power in his "Technology and the Fourth Amendment," 80 J. Crim. L. 1 (Spring, 1989), discusses variations of such a principle at 44–47 and 93–103.

7. Judith Jarvis Thomson imagines such a device in her "The Right to Privacy," *Philosophy and Public Affairs*, vol. 4 (1975), pp. 295–314.

8. 738 F 2d 538 (1984).

9. If the DEA agent had instead been a repairman fixing the hole, this might be otherwise. But the repairman, insofar as he is not a snoop, would not put his ear to the hole and listen in. If he does, he becomes a snoop and violates the mischance principle.

10. 738 F 2d 538, 543 (1984); the judge added that the outcome might have been different had the agent created the hole or enlarged it (p. 544).

11. For discussions of the value of privacy, see the essays in *Philosophical Dimensions of Privacy: An Anthology*, ed. Ferdinand Schoeman (Cambridge: Cambridge University Press, 1984).

12. See *U.S. v. Smith*, 978 F. 2d 171 (1992).

13. The example is taken from Note, "Private Places," 43 NYU L.R. 968 (1968), p. 983 and is discussed in Robert Power, "Technology and the Fourth Amendment," 80 J. Crim. L. 1 (Spring, 1989), n. 101.

14. *Greenwood v. California*, 486 U.S. 35, at 40-1 (1988).

15. 486 U.S. at 53.

16. See Tunick, *Practices and Principles*, chapter 5.

17. 821 F 2d 248 (1987).

18. 476 U.S. 227 (1986), at 238.

19. 476 U.S. at 211–12. For criticism of this argument, see Tunick, *Practices and Principles*, pp. 178–182.

20. A point Justice Powell makes forcefully in his dissent, 476 U.S. at 223–4.

21. 476 U.S. at 243.

22. See *People v. Mayoff*, 197 Cal Rptr 450 (1983).

23. *State v. Young*, 123 Wash. 2d. 173 (1994), at 177, 183.

24. *U.S. v. Field*, 855 F. Supp. 1518 (1994), at p. 1531: referring to training material for one model of an FLIR.

25. See, for example, *U.S. v. Penny-Feeney*, 773 F Supp 220 (1991); *U.S. v. Porco*, 842 F Supp 1393 (1994); *U.S. v. Kyllo*, 809 F Supp 787 (1993) and 1999 U.S. App Lexis 21562 (Sept. 9, 1999); but see *People v. Deutsch*, 44 Cal. App. 4th 1224 (1996); and *State v. Young*, 123 Wash 2d 173 (1994).

26. *U.S. v. Penny-Feeney*, 773 F. Supp. at 227: "use of the FLIR . . . entailed no embarrassment to or search of the person." See also *U.S. v. Porco*, 842 F Supp 1393, 1398: the device is "non-intrusive"; and *U.S. v. Kyllo*, 809 F Supp 787, 792: the device does not "reveal intimate details as to the inside of the home," and "intimacy," "personal autonomy," and "privacy" are not threatened.

27. See Judge Noonan's dissent in *U.S. v. Kyllo*, 1999 US App Lexis 21562 (1999), pp. 19–20.

28. *U.S. v. Ishmael*, 843 F Supp at 213. Judge Noonan's dissent in a recent FLIR case also rests in part on the fact that the device amplifies the senses. See *U.S. v. Kyllo* (1999), p. 22.

29. *U.S. v. Kyllo*, 1999 U.S. App Lexis 21562 (1999), p. 17 (Noonan's dissent).

30. *U.S. v. Field*, 855 F. Supp 1518 (1994), at 1525.

31. This argument is pointed to in *U.S. v. Field*, 855 F. Supp 1518, 1531: "It is disingenuous for the government to argue that thermal imagers do not reveal what is happening inside of a home. The whole point of the exercise is to attempt to learn what is happening inside of the home."

blank