Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns

Thomas B. Kearns

Repository Citation
Thomas B. Kearns, Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns, 7 Wm. & Mary Bill Rts. J. 975 (1999), http://scholarship.law.wm.edu/wmborj/vol7/iss3/10
TECHNOLOGY AND THE RIGHT TO PRIVACY:
THE CONVERGENCE OF SURVEILLANCE AND INFORMATION PRIVACY CONCERNS

While the privacy concerns raised by advances in surveillance and information technologies are widely recognized, recent developments have led to a convergence of these technologies in many situations, presenting new challenges to the right to privacy. This Note examines this convergence of surveillance and information technologies and its potential impact on individual privacy interests.

The Note first discusses the right to privacy, personal information, and surveillance technology separately, noting ways that new technologies create privacy concerns. The Note then describes the merging of surveillance and information technologies and the resulting convergence of two formerly distinct privacy issues. Finally, the Note examines existing protections for privacy, considers why they are insufficient, and proposes measures to enhance the constitutional protection of privacy interests to address these new technologies.

* * *

"Privacy makes possible individuality, and thus, freedom."¹

INTRODUCTION

Technological advances are changing the face of American society dramatically. New technology affects individuals in countless ways, including the manner in which they interact with each other, with businesses, and with the government. While technology makes it possible to accomplish many tasks more efficiently, and even to accomplish tasks previously not possible, these accomplishments do not come without costs. Even though they provide solutions to current problems, many technological developments often create new, sometimes unforeseen, problems. As society incorporates these developments into its structure, the problems that the developments create must be confronted so that the benefits of technology outweigh its burdens.² One area in which new technology currently is creating such problems

² Ideally, society would confront the problems relating to a new technology before the technology is introduced into everyday use. Unfortunately, because these problems often are unforeseen, they sometimes are not addressed until at least parts of society have suffered negative consequences. For example, the invention of the automobile brought relief from the problem of horses littering in the streets. Not until after the automobile was in widespread use, however, did society recognize the problem of exhaust pollution.

A more recent example of such an unforeseen problem is the increase in the number of accidents at toll plazas where E-Z Pass technology, see infra note 90, has been installed.
is the right to privacy. Surveillance technology invokes privacy concerns perhaps more directly than any other type of technology because surveillance equipment, by its very nature, is designed to enable a surveillant to observe that which the subject does not intend to be observed. Although surveillance is a useful and necessary aspect of criminal investigation, new developments in surveillance technology equipment, such as magnetic gradient measuring, passive millimeter wave imaging, back-scattered x-ray imaging, and radar-skin scanning, give rise to privacy issues that previously did not exist. Furthermore, although privacy concerns stemming from surveillance activity traditionally involve government intrusion, private actors increasingly have access to surveillance equipment and the ability to invade individuals’ privacy.

A more recent concern regarding privacy rights is information privacy. Information privacy involves an individual’s personal information and his ability to control that information. Personal information includes data assigned to an individual, such as a social security number, address, or telephone number. Other personal information is generated on a day-to-day basis, such as records of bank transactions, credit card purchases, phone calls, and medical treatments. The

See Editorial, DAILY GAZETTE OF SCHENECTADY, Dec. 24, 1996, in Associated Press, Some Recent Editorial Opinion [sic] from Across New York, Jan. 1, 1997, available in 1997 WL 2491560. Although outside the scope of this Note, this example also demonstrates that the new technologies discussed herein often raise issues other than privacy concerns.

Concerns regarding technological advances encroaching upon the right to privacy are nothing new. See, e.g., Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that wiretapping the residences of conspiracy defendants did not constitute an unlawful search). Recent developments, however, have brought new concerns to the issue of privacy and technology. See infra notes 53-125 and accompanying text.

Although surveillance techniques certainly can be used to observe a subject’s public activities, a concern arises with the observation of private activities. Another concern, as this Note will discuss, is that new technology can create difficulties in demarcating those activities that are public and those that are private. See infra notes 21-36, 53-83 and accompanying text.

See infra notes 76-80 and accompanying text.

See infra notes 37-52, 84-104 and accompanying text; see also Sheri A. Alpert, Privacy and Intelligent Highways: Finding the Right of Way, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 97, 106-07 (1995) ("The less opportunity individuals have to limit access to their own personal information, or to limit the amount of personal information they must give up to others (either voluntarily, or by coercion), the less privacy they have."); Sandra Byrd Petersen, Note, Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?, 48 FED. COMM. L.J. 163 (1995) (addressing the threat to individual privacy presented by the collection, processing, and dissemination of personal information through computers).
“assigned” personal information may be used primarily to identify a subject; the
“generated” information may be used to track the subject’s activities and habits. This
information then can be used, unbeknownst to the subject, by government,
businesses, and individuals for any number of purposes. As society becomes more
dependent on computer databases and electronic record-keeping, an individual’s
ability to control who has access to his personal information becomes more tenuous.
This inability to control the use of personal information gives rise to the issue of
information privacy.

Both surveillance activity and the use of personal information present opportunities to endanger the privacy of an individual. Because both categories
invoke privacy concerns when considered separately, it is easy to view them as two
distinct issues, each touching upon a different aspect of privacy. New technology
and new uses of current technology, however, blur the distinction between
surveillance activity and the use of personal information. New surveillance
technology can obtain and store personal information about an individual, while
personal information can be used in new ways akin to surveillance. This merging of
two categories of technology presents new challenges for the right to privacy and
amplifies existing challenges.

This Note examines the merging of surveillance and information privacy
concerns and the resulting potential to diminish individuals’ privacy. Comprehension of the right to privacy is necessary to understand how new
technology can endanger this right. Accordingly, Part I of this Note discusses the
development of the privacy right and its application to surveillance measures and
personal information. Part II discusses privacy concerns with regard to new

---

7 These purposes may range from relatively innocuous ones, such as targeting consumers
based on buying habits, to more disturbing possibilities, such as determining at what times
individuals typically are away from their homes. *See infra* notes 84-104 and accompanying
text.

8 One commentator has classified the current proliferation of advances in information
technology as the “metamorphosis of America into an information-based society.” Peck,
*supra* note 1, at 27.

9 *See infra* notes 85-88, 94-96 and accompanying text; *see also* Randolph S. Sergent,
Note, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L.
REV. 1181, 1182 & n.2 (1995) (“Although no law inherently requires us to sacrifice privacy
to developing technology, we certainly have less control over personal information than we
once had.” (citing Larry Tye, *Privacy Lost in High-Tech Era*, BOSTON SUNDAY GLOBE, Sept.
5, 1993, at 1, 18-19)). Parties accessing personal information “might include law enforcement
agents, private investigators, advertisers, or stalkers.” Dorothy J. Glancy, *Privacy and
Intelligent Transportation Technology*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 151,
technology, examining surveillance and personal information issues separately. Part III describes the merging of these two aspects of privacy as a result of technological developments. Lastly, Part IV examines existing protections for privacy and considers why they are insufficient. This final Part also proposes measures to prevent the erosion of individual privacy in the face of technological developments.

I. THE RIGHT TO PRIVACY

A. Interests in Privacy

Privacy is an essential element of a free society. Many commentators agree that without privacy, freedom is not possible. Without the ability to interact with one another in private, individuals cannot exchange ideas freely. This "marketplace of ideas" is essential for a democracy to function properly and give rise to a free society. Although no "universally accepted definition of the right to privacy" exists, court opinions that address privacy issues often encompass three areas of privacy interests: autonomy, intrusion, and information privacy.

10 Justice Douglas posed the question: "If a man's privacy can be invaded at will, who can say he is free?" Osborn v. United States, 385 U.S. 323, 354 (1966) (Douglas, J., dissenting). Justice Brandeis described the right to be left alone as "the most comprehensive of rights and the right most valued by civilized men." Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). See also Frank Askin, Surveillance: The Social Science Perspective, 4 Colum. Hum. Rts. L. Rev. 59, 62-88 (1972) (presenting an appendix from Plaintiff's Brief, Tatum v. Laird, 444 F.2d 947 (D.C. Cir. 1971), rev'd, Laird v. Tatum, 408 U.S. 1 (1972), and giving a scientific definition of "chill" and describing the psychological and sociological evidence indicating that a U.S. Army surveillance program chilled the exercise of First Amendment rights).

A distinction must be made between privacy as a universal concept (an interest in privacy) and privacy as a legal right. Although everyone has their own individual concept of privacy, the fundamental idea of privacy has existed for centuries. The legal right to privacy, however, is a relatively new concept that the courts still are developing. See, e.g., Griswold v. Connecticut, 381 U.S. 479, 483 (1965) (holding that the right to privacy exists in the penumbras formed by the Bill of Rights); see also infra notes 37-41 and accompanying text (discussing the constitutional right to privacy as established by the Court in Griswold). Interests in privacy and the right to privacy do not necessarily coincide.

11 See Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) (disagreeing with the majority's intent test and applying the "clear and present danger" standard to defendant's speech).

12 Alpert, supra note 6, at 102.

13 See id. at 104 (citing GEORGE B. TRUBOW, PRIVACY LAW AND PRACTICE (1991)). As Sheri Alpert points out, these three interests in privacy are "by no means mutually exclusive."
Autonomy generally is the ability of an individual to engage in private activities free from intervention or regulation. Put succinctly, autonomy allows people to make decisions freely and act as individuals.

Privacy also includes an interest against intrusion. This interest means being free from surveillance in situations in which an individual has a reasonable expectation of privacy. The interest against intrusion is tied to the anonymity of individuals. Anonymity in this context does not signify a complete lack of ability to identify someone; instead, it refers to an individual’s ability to go about his daily life without having his every move observed. Surveillance technology is designed to intrude upon this anonymity and, in certain situations, society accepts this intrusion. It can be unclear, however, what types of intrusion are acceptable, and to what extent, when new advances in surveillance are involved.

The third major aspect of privacy is that of information privacy. Information privacy also is tied to the concept of anonymity but, instead of addressing an individual’s actions and movements, it is concerned with his personal information. Individual bits of personal information can identify a person and his activities. When various items of personal information are pieced together, an even more telling picture can develop. The argument for information privacy stems from the concern that individuals have a right to some control over who has access to their personal information, and for what purpose.

Id. at 107. The merging of surveillance and personal information technologies tends to intertwine these interests even further. For the benefit of discussion of the right to privacy, however, it is helpful to separate them into distinct categories.

Although an autonomy interest is important to the concept of privacy, neither surveillance technology nor personal information problems disturb the autonomy aspect of privacy. This Note, therefore, is concerned primarily with the other two major privacy interests. It is worth noting, however, that technological advances that endanger the autonomy element of privacy do exist. See, e.g., id. at 104-05, 108-10 (discussing Intelligent Vehicle Highway System (“IVHS”) user services that implicate the autonomy element of privacy); Valerie Reitman, Look Who’s Getting a License to Drive: Automated Cars Operate Without Human Drivers, WALL ST. J., July 25, 1997, at A7 (describing auto industry efforts to develop automated cars that can drive on the highway with minimal human intervention).

This concern arises out of anonymity concerns in the same way as the interest against intrusion does. Information privacy concerns differ from intrusion concerns, however, in that they address an individual’s personal information, rather than the individual himself.
New technology can encroach upon all three of these privacy interests. Intrusion and information privacy interests, however, especially are relevant to the technologies discussed here and to the merger of these technologies.  

B. Surveillance Intrusion

Surveillance activity directly relates to an individual’s interest against intrusion because it is an intentional attempt to observe that which the individual believes to be private. It is impossible to consider the relationship of surveillance activity to privacy concerns without discussing searches and the Fourth Amendment of the United States Constitution. An unreasonable search is an intrusion on an individual’s right to privacy. New developments in surveillance technology, however, can make unclear what constitutes such a search.

In earlier Fourth Amendment jurisprudence, the Supreme Court used the trespass doctrine when considering searches. This “area-based” approach narrowly construed the Fourth Amendment, holding that a search did not occur unless physical

---

20 This is not to say that the technologies discussed here do not have the potential to affect an individual’s interest in autonomy. See, e.g., Alpert, supra note 6, at 108-09 (discussing IVHS user services with the potential to affect the autonomy interest—particularly Advanced Vehicle Control Systems); Glancy, supra note 9, at 155-56 (discussing Intelligent Transportation System (“ITS”) automated applications with the potential to compromise individual autonomy).

21 U.S. CONST. amend. IV. It is the search aspect of the Fourth Amendment to which surveillance activity relates. The Amendment provides:

The 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, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Id.

22 See, e.g., Katz v. United States, 389 U.S. 347, 350 (1967) (holding that the Fourth Amendment “protects individual privacy against certain kinds of governmental intrusion”).

23 For example, one commentator on back-scattered x-ray imaging devices likened their use to “a high-tech strip search without a warrant.” Elizabeth Fernandez, State Prisons Scanning Visitors with X-Rays, S.F. EXAMINER, Nov. 3, 1997, at A1.

24 The Court established the trespass doctrine in Olmstead v. United States, 277 U.S. 438 (1928). In Olmstead, the Court held that a wiretap did not constitute an illegal search because no physical intrusion of the defendant’s “houses, persons, papers, and effects” occurred. Id. at 465.

25 Sergent, supra note 9, at 1187.
intrusion into one of the subject’s “constitutionally protected area[s]” occurred.²⁶ Surveillance such as wiretapping, that did not require physical intrusion, did not constitute a search, and, thus, did not require a warrant.²⁷

In 1967, the Supreme Court replaced the trespass doctrine with what has come to be known as the *Katz* doctrine. In *Katz v. United States*,²⁸ the Court found that a telephone wiretap did in fact constitute a search.²⁹ This decision, which extended the protection that the Fourth Amendment gives to individuals, was based in the concept that “the Fourth Amendment protects people, not places.”³⁰ The Court in *Katz* responded to the fact that surveillance technology enables the violation of an individual’s interest against intrusion without any physical trespass.³¹

The *Katz* doctrine has been used since to determine whether a search has occurred. The test developed in *Katz*, which appears in Justice Harlan’s concurring opinion,³² is a two-pronged test that measures both subjective and objective factors.³³ In the first prong of the test, the subject must “have exhibited an actual (subjective) expectation of privacy.”³⁴ The second prong then assesses whether that “expectation [is] one that society is prepared to recognize as ‘reasonable.’”³⁵ For activity, including surveillance activity, to constitute a search under the *Katz* test, both prongs of the test must be met.

The *Katz* doctrine was a significant step in expanding the protection of individuals’ privacy against technological advances. The Court recognized that physical trespass is not required for invasion of one’s privacy, and determined that

²⁶ Silverman v. United States, 365 U.S. 505, 510 (1967) (holding that eavesdropping surveillance constituted an illegal search because the microphone physically intruded into the premises).

²⁷ See Olmstead, 277 U.S. at 466. Interestingly, prior to the *Olmstead* decision, the Court at times construed the Fourth Amendment less narrowly, finding the occurrence of a search without physical trespass. See, e.g., Boyd v. United States, 116 U.S. 616, 622 (1886) (holding that a law compelling the defendant to produce books and papers constituted an illegal search, even without physical entry onto defendant’s premises).


²⁹ See id. at 354.

³⁰ Id. at 351.

³¹ See id. at 362 (Harlan, J., concurring) (holding that Fourth Amendment protections extend beyond physical invasion, because “in the present day . . . reasonable expectations of privacy may be defeated by electronic as well as physical invasion”).

³² See id. at 360-62 (Harlan, J., concurring).

³³ For a critical argument that the “objective” prong of the *Katz* test is not objective at all, see Sergent, *supra* note 9, at 1193-94.

³⁴ *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

³⁵ Id.
such nonphysical intrusion by the government could constitute a search. The *Katz* test as currently applied by many courts, however, does not provide sufficient protection against numerous emerging technologies.

### C. Information Privacy

Although the Fourth Amendment addresses the tension between the interest against intrusion and surveillance technology, as it relates to searches, no specific constitutional clause addresses the right to privacy generally. Because the right to privacy is not enumerated in the Constitution, there is disagreement over what that right entails.

The right to privacy first was stated explicitly by the Supreme Court in *Griswold v. Connecticut.* Although the Court previously had quashed laws that limited the autonomy of individuals, it had done so on the grounds that these laws infringed upon the liberty guaranteed by the Due Process Clause of the Constitution. In *Griswold,* the Court drew upon these prior cases in demonstrating that a right to privacy is implicit in the Constitution and that several “specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance.” For the rights protected by the Bill of Rights to have

---

36 The holding in *Katz* does not prevent the use of surveillance equipment by police and government entities altogether. However, the holding in *Katz* helped safeguard privacy interests by establishing that the use of such equipment can constitute a search, thereby requiring a warrant.

37 381 U.S. 479 (1965). Although the Court mentioned the “freedom to associate and privacy in one’s associations” in *NAACP v. Alabama,* 357 U.S. 449, 462 (1958) (holding that compelled disclosure of membership in a political organization violated an individual’s freedom of association), it did not specify, in that case, that a right to privacy exists. Rather, the Court recognized privacy as necessary to the “peripheral First Amendment right” of freedom of association. See *Griswold,* 381 U.S. at 483 (citing *NAACP,* 357 U.S. at 462).

38 See, e.g., *Pierce v. Society of Sisters,* 268 U.S. 510 (1925) (holding that an Oregon law requiring children to attend public schools violated due process); *Meyer v. Nebraska,* 262 U.S. 390, 403 (1923) (holding that a Nebraska law prohibiting the teaching of grade school classes in any language other than English deprived parents and teachers of liberty without due process).

39 The Fourteenth Amendment states, in pertinent part, that “[n]o State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law . . . .” U.S. CONST. amend XIV.

40 *Griswold,* 381 U.S. at 484. It is interesting to note that Justice Harlan, who established the *Katz* test providing for greater protection from surveillance intrusion, did not see a need to recognize a separate right to privacy. Instead, he believed that the “Due Process Clause
any substance, the Court reasoned, the rights must “create [related] zones of privacy.”

Because the right to privacy exists only in these zones of privacy as they relate to enumerated Constitutional rights, privacy is not a clearly defined right. How far this right extends to information privacy is the subject of significant uncertainty.

Information privacy is based on an autonomist view of individuals in which personal data are included as part of the “self.” In this view, the right to privacy protects the information that comprises a person’s “data image” the same way it protects a person’s physical being. As society becomes ever more information-based, the need for individuals to distribute their personal information increases. An unwillingness to give personal information to others effectively would prevent an individual from functioning in society. Of the Fourteenth Amendment stands . . . on its own bottom.”

41 Id. at 484.
42 Until the Supreme Court specifically recognizes the right to privacy in a certain area, privacy in that area is speculative. Even after the Court recognizes privacy in an area, the degree to which the right extends often is uncertain. For example, following the Griswold decision, no one knew whether the protection of sexual privacy extended only to married couples, or whether unmarried heterosexuals and homosexuals also were entitled to this privacy. The Eisenstadt v. Bard decision, 405 U.S. 438, 443 (1972), later demonstrated that this right protects unmarried heterosexuals; conversely, the Bowers v. Hardwick decision, 478 U.S. 186, 191 (1986), showed that homosexuals do not necessarily enjoy the protection of this right.

43 See Steven A. Bercu, Toward Universal Surveillance in an Information Age Economy: Can We Handle Treasury’s New Police Technology?, 34 JURIMETRICS J. 383, 401 (1994). See also ELLEN ALDERMAN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY 326 (1995) (“A portrait of you . . . will exist in cyberspace. The profile could be so complete that it will be like having another self living in a parallel dimension; it is a self you cannot see, but one that affects your life just the same.”).

44 Bercu, supra note 43, at 401.

45 See id. at 400 (citing Joel Feinberg, Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution?, 58 NOTRE DAME L. REV. 445-47, 453 (1983)).


47 See OFFICE OF TECHNOLOGY ASSESSMENT, COMPUTER-BASED NATIONAL INFORMATION SYSTEMS: TECHNOLOGY AND PUBLIC POLICY ISSUES 77, 108 (1981), quoted in Bercu, supra note 43, at 408 n.129 (“[I]t is questionable whether future participation in a computerized society can be construed to be voluntary if the alternative is to forgo all services necessary to live comfortably as a member of that society.”). For an example of such compelled participation, or at least the perception thereof, see Carol Power, Little White Box Cuts Toll Bridge Queues, IRISH TIMES, Nov. 7, 1997, at 59, available in 1997 WL 12033993
important and is accessible to a greater number of people and institutions, the need to protect such private information intensifies.

The Supreme Court has examined the issue of information privacy only once. In Whalen v. Roe, the Court held that the State of New York could maintain a database on individuals who legally obtained narcotics by prescription. The Court found that the legitimate state interest of regulating drugs that could be sold illegally outweighed the information privacy rights of the individuals whose personal information appeared in the database. In performing this balancing test, however, the Court explicitly recognized that an information privacy interest exists.

In the same way that the right to reproductive privacy established in Griswold remained uncertain until subsequent decisions by the Court, the scope of the right to information privacy similarly is unclear. Scholars generally agree that, at present, the right to privacy in personal information is weak. As personal information plays a greater role in the daily lives of individuals, and the interest in personal information privacy increases, the need to develop this right will increase as well.

(discussing automatic toll collection technology used in New York); Wire Services, N.J. Prepares for High-Tech Road Toll System; Pa.-to-Mass. Effort Expected to Cut Smog, Congestion and Stress, BALTIMORE SUN, Apr. 20, 1997, at 15B (discussing a multistate network that would use automatic toll collection technology).

49 See id. at 591.
50 See id. at 598-602.
51 See id. at 605 ("The right to collect and use such data for public purposes is typically accompanied by a concomitant duty to avoid unwarranted disclosures. . . . [I]n some circumstances that duty arguably has its roots in the Constitution . . . .").
52 See ALDERMAN & KENNEDY, supra note 43, at 141-42; Bercu, supra note 43, at 422 n.193 (citing PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 381-82, 384-85 (1977); Priscilla M. Regan, Privacy, Government Information, and Technology, 44 PUB. ADMIN. REV. 629, 629 (1986); C. Dennis Southard, Individual Privacy and Governmental Efficiency: Technology's Effect on the Government's Ability to Gather, Store, and Distribute Information, 9 COMPUTER L.J. 359, 370 (1989)). For an argument that no right to information privacy currently exists, see Petersen, supra note 6, at 170-71.
II. TECHNOLOGY AND PRIVACY CONCERNS

A. Surveillance Technology

*Katz v. United States* replaced the trespass doctrine with the "reasonable expectation of privacy" standard for determining whether certain activity constitutes a search under the Fourth Amendment. This new standard no longer requires physical intrusion for a warrantless search to violate an individual's right to privacy. While the *Katz* doctrine was a response to the Court's recognition that technology could make an invasion of privacy possible without physical intrusion, recent technological advances in surveillance equipment make the effectiveness of the *Katz* test questionable.

While *Katz* established that the Fourth Amendment requires both a subjective and objective expectation of privacy, advances in surveillance technology bring both of these expectations into question. The subjective prong of the *Katz* test assesses whether an individual under surveillance had an actual expectation of privacy. The test measures this expectation by the individual's conduct and the steps the individual took to ensure privacy. Steps that prevent visual observation, such as fences or coverings, establish a subjective expectation of privacy in some circumstances. Under current law, however, as technological advances make new methods of observation possible, individuals will be required to guard against more and more methods of surveillance to demonstrate their subjective expectation of privacy.

---


54 One commentator asserts that "[n]ever before has there been the unusual combination of hi-tech citizen searches and a bald lack of individualized suspicion." Jennifer Mulhern Granholm, *Video Surveillance on Public Streets: The Constitutionality of Invisible Citizen Searches*, 64 U. DET. L. REV. 687, 711 (1987). For examples of different technological developments making such "citizen searches" possible, see infra notes 60-62, 76-80 and accompanying text.

55 See *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

56 See United States v. Broadhurst, 805 F.2d 849, 854 (9th Cir. 1986) (holding that the "use of metal roofing" demonstrated that defendants had a subjective expectation of privacy in their greenhouse by attempting to hide its interior).


59 The danger to an individual's interest in privacy is "particularly ominous when the new technology is designed for surveillance purposes . . . . Control over the technology of surveillance conveys effective control over our privacy, our freedom and our dignity—in short, control over the most meaningful aspects of our lives as free human beings."
One technology that already has eroded the significance of the subjective expectation of privacy is thermal imaging scanning.\(^6\) Thermal imaging scanning can be used to detect excessive "heat waste"\(^6\) that could signify illegal activity such as indoor marijuana cultivation.\(^6\) In United States v. Myers,\(^6\) the Court of Appeals for the Seventh Circuit determined that the defendant did not display a subjective expectation of privacy while using indoor growing techniques because he made no effort to "conceal or contain the heat emissions from his home."\(^6\) Although Myers had taken other steps that might have created a subjective expectation of privacy, the court held that he had no such subjective expectation because he failed to conceal these heat emissions.\(^6\) Under the Myers holding, an individual must protect against the discovery of activity through thermal imaging technology, even in his own home, to establish the subjective expectation of privacy required by the Katz test.\(^6\)

If a subject establishes a subjective expectation of privacy, the second, objective prong of the Katz test assesses whether that "expectation is one that society is

---


\(^{61}\) Thermal imaging scanning, also referred to as thermal imaging, uses infrared technology to detect the escape of heat from the object being scanned by a thermal imaging device. The surveillant then is able to view an image of this escaped heat on a monitor. See United States v. Myers, 46 F.3d 668, 669 (7th Cir.), cert. denied, 516 U.S. 879 (1995).

\(^{62}\) See id. Indoor marijuana cultivation requires heat lamps, which produce significant amounts of heat that thermal imaging can detect. See id. at 669.

\(^{63}\) 46 F.3d 668 (7th Cir.), cert. denied, 516 U.S. 879 (1995).

\(^{64}\) Id. at 669.

\(^{65}\) See id. For example, Myers did not leave any trash at the curbside of his home, presumably because he was disposing of marijuana clippings. See id. at 668-70. Such clippings left in the trash outside the home would not be protected by any claim of privacy. See id. (noting that waste products "intentionally or inevitably exposed to the public" are not protected by privacy interests (quoting United States v. Ford, 34 F.3d 992, 997 (11th Cir. 1994)) (citing California v. Greenwood, 486 U.S. 35, 37 (1988))).

\(^{66}\) One could argue that an effort to conceal heat emissions to protect against thermal imaging scanning would be a reasonable requirement in establishing a subjective expectation of privacy only when an individual is engaged in an activity which produces an unusually large amount of heat waste. Conversely, because the human body itself produces heat emissions, one could argue that protection against thermal imaging scanning is always required to create such an expectation.
prepared to recognize as 'reasonable.' In the Myers case, the Seventh Circuit found that, even had Myers established a subjective expectation of privacy against thermal imaging scanning, this expectation would not have been reasonable under the objective prong of the Katz test. The court likened the heat emissions from the subject's home to curbside trash, which is not protected by privacy interests. The court also stated that thermal imaging scanning “does not intrude in any way into the privacy and sanctity of a home,” in part because thermal imaging “does not penetrate the viewed object, nor does it emit rays or beams of any type.” Because the court in Myers found no objective expectation of privacy, the use of thermal imaging scanning, regardless of what measures the defendant had taken to protect against such surveillance, did not constitute a search within the meaning of the Fourth Amendment.

Although thermal imaging scanning may be used without a warrant because it is not considered a search under the Fourth Amendment, thermal imaging can

---

68 See Myers, 46 F.3d at 670.
69 See id. (citing Greenwood, 486 U.S. at 37).
70 Id. at 670.
71 Id. at 669. It is interesting to note that, under this reasoning, whether a surveillance method will qualify objectively as an intrusion into privacy is, at least in part, dependent on whether any physical intrusion has occurred. It is exactly this trespass doctrine approach that the Katz test was designed to replace. See Katz, 389 U.S. at 353.
72 See Myers, 46 F.3d at 670. The court recognized the possibility that other technologies may develop that would be so intrusive that their use without a warrant would be unacceptable to society and, thus, an objective expectation of privacy would exist. See id. at 670 n.1. The court, however, did not provide any guidelines to indicate at what point surveillance technology would become “unacceptably intrusive.” Id.
73 This is true in at least the Fifth, Seventh, Eighth, and Eleventh Circuits. See United States v. Ishmael, 48 F.3d 850 (5th Cir.), cert. denied, 516 U.S. 818 (1995); United States v. Robinson, 62 F.3d 1325 (11th Cir. 1995); Myers, 46 F.3d. at 668; United States v. Robertson, 39 F.3d 891 (8th Cir. 1994), cert. denied, 514 U.S. 1090 (1995); United States v. Ford, 34 F.3d 992 (11th Cir. 1994). No circuit court has ruled that thermal imaging scanning constitutes a search, although other circuits have not considered the issue, or have sidestepped it by deciding a case on other grounds. See, e.g., United States v. Cusumano, 83 F.3d 1247 (10th Cir. 1996) (holding that a warrant to search defendant's residence was supported by probable cause); United States v. Feeney, 984 F.2d 1053 (9th Cir. 1993) (holding that the police demonstrated probable cause for the warrant under which they conducted their search). But see, e.g., United States v. Field, 855 F. Supp. 1518 (W.D. Wis. 1994) (holding that the use of thermal imaging can constitute a search because the imager "intrudes" into the home by detecting heat sources from within the home); State v. Young, 867 P.2d 593 (Wash. 1994) (holding that warrantless infrared surveillance violated the
infringe upon an individual's interest in, if not right to, privacy. Contrary to the government's position in cases challenging the use of thermal imaging devices, one can make a strong argument that thermal imaging scanning enables the user to observe characteristics and activities inside the home. As United States Magistrate Judge Crocker inquired, if "thermal imagers do not reveal activities that occur inside the home . . . then why does the government use thermal imagers to try to detect indoor [illegal activities]?"

Thermal imaging scanning is just one example of surveillance technology that can erode the right to privacy. Other technologies that allow the user to observe even more details are being developed, including magnetic gradient measuring, passive millimeter wave imaging, back-scattered x-ray imaging, radar-skin scanning, andFourth Amendment and the state constitution's protection against warrantless invasion of the home).

Thermal imaging sometimes can be used to determine the location of walls, dividers, and even people within a structure. See United States v. Olson, 21 F.3d 847, 848 n.5 (8th Cir. 1994) (discussing the visibility of rafters and divider walls in a mobile home with the use of a thermal imaging scanner); Young, 867 P.2d at 595 (discussing the visibility of a person through a curtain or a thin plywood door with the use of a thermal imaging scanner).

Field, 855 F. Supp. at 1531.

Magnetic gradient measuring detects, in the magnetic field surrounding an individual, fluctuations caused by metal materials and compares these fluctuations to those caused by other items, such as weapons. See Mark Hansen, No Place to Hide: If Crime is Everywhere, So, Too, May Be Police Surveillance Cameras and Contraband Detection Devices to Combat It. But Who's Looking out for Privacy Rights?, 83 A.B.A. J. 44, 47 (Aug. 1997); Highly Sensitive Gun Detectors May Soon Be in Hands of Police, MINNEAPOLIS-ST. PAUL STAR TRIB., Apr. 13, 1997, at 21A.

Passive millimeter wave imaging detects variations in electromagnetic rays emitted by objects. These waves can produce an image of the objects on a person's body by contrasting the objects' variations with the variations produced by the body itself. The variations can be measured regardless of the objects' composition. See Hansen, supra note 76, at 46, 48; Fox Butterfield, Arms Detector Technology Aims High, COMMERCIAL APPEAL (Memphis, TN), Apr. 7, 1997, at A8; Stephen Grey & Steven Haynes, Police See Knife Carriers at 60ft with X-Ray Spy Cameras, SUNDAY TIMES (London), May 11, 1997, at NEWS7; Bruce D. Nordwall, Hybrid Camera to Seek Runway Through Fog, AVIATION WEEK & SPACE TECH., July 7, 1997, at 66.

Back-scattered x-ray imaging bounces a low dosage of x-ray radiation off of the subject's skin, rather than penetrating the body like traditional x-rays. The reflected x-rays then can be used to produce a computer-enhanced outline of the subject's body and everything he is carrying. See Highly Sensitive Gun Detectors May Soon Be in Hands of Police, supra note 76; Estes Thompson, Security Detector Sees All: San Diego Firm's System Helps Pierce Cloak of Secrecy, SAN DIEGO UNION-TRIB., Apr. 10, 1997, at C1; War on Drugs is Boon to X-Ray Manufacturer, ORLANDO SENTINEL, Nov. 5, 1997, at B4. One
TECHNOLOGY AND THE RIGHT TO PRIVACY

While these technologies all operate differently and may reveal different information, the result is the same in that each enables the user to observe that which previously was private.

If the Katz test, as currently applied by the majority of courts, is applicable to these new surveillance technologies, then use of these technologies will not constitute a search and the Fourth Amendment will not prevent their use without a warrant. Even if courts were to find that an expectation of privacy against such equipment was reasonable, thereby passing the objective prong of the Katz test, the current standard commentator has said that back-scattered x-ray machines "produce a crude image of [subjects'] bodies without clothing." Elizabeth Fernandez, *State Prisons Scanning Visitors with X-Rays*, S. F. EXAMINER, Nov. 3, 1997, at A1.

Radar-skin scanning can produce a very precise image of the subject's body, including intimate anatomical details, thereby revealing objects on the body. See Mark Fischetti, *Defusing Airline Terrorism*, TECH. REV., Apr. 1997, at 38, 44; Hansen, *supra* note 76, at 46. The ability to create such images raises the interesting question of whether the established right to privacy in one's naked body, see, e.g., Bowling v. Enomoto, 514 F. Supp. 201, 203 (N.D. Cal. 1981) (holding that prisoners in an all-male institution had a limited constitutional right to privacy that included the right to be free from unrestricted observation of their genitals and bodily functions by female prison officials) (citing York v. Story, 324 F.2d 450 (9th Cir. 1963), *cert. denied*, 376 U.S. 939 (1964)), extends to such electronically produced images.


One can draw an analogy between satellite imaging and aerial surveillance. Current standards regarding aerial surveillance would make warrantless satellite imaging legal. See, e.g., California v. Ciraolo, 476 U.S. 207 (1986) (holding that, although defendants demonstrated a subjective expectation of privacy, there exists no objective expectation of privacy from aerial surveillance in one's back yard); Dow Chem. Co. v. United States, 476 U.S. 227 (1986) (holding that taking aerial photos of exposed areas of an industrial plant does not constitute a search); United States v. Broadhurst, 805 F.2d 849 (9th Cir. 1986) (holding that taking aerial photos of a greenhouse does not constitute a search).

Additionally, it is conceivable that satellites could make use of the new technologies listed above, or perhaps others. Although the Court in *Dow Chemical* did warn that the use of sophisticated equipment by the government may, at some point, require a warrant, it did so in dicta and did not provide clear standards as to when this threshold would be crossed. *See Dow Chem.*, 476 U.S. at 238.
still would require the subject to take protective measures against the equipment’s use to establish a subjective expectation of privacy. With technological advances occurring at an increasingly rapid pace, it is unlikely that a person would be aware of what surveillance technology observers are using and what steps he must take to protect himself. While such surveillance equipment reveals private information, under the current standard it does so without infringing on any legally defined right to privacy.

B. Information Privacy

The interest in information privacy differs from the privacy interest against surveillance in that, in the former, the use of private information does not involve observation of the actual person. Instead, the subject’s personal information is scrutinized and used, usually without the subject’s knowledge. In some ways, this information can be even more telling than direct observation through surveillance. As in the field of surveillance technology, new developments in the use of personal information increase the potential for an infringement of information privacy.

The threat to information privacy stems from the gathering and distribution of personal information. Individuals generate personal information on a daily basis through, for example, bank transactions, credit card purchases, and medical records. Often, small pieces of personal information can be very informative, with the potential to reveal further sensitive data about the subject.

---

81 Interestingly, the court in United States v. Ishmael held the reverse to be true: The defendants displayed a subjective expectation of privacy in their “heat waste,” but such an expectation was not objectively reasonable. See United States v. Ishmael, 48 F.3d 850, 854-55 (5th Cir.), cert. denied, 516 U.S. 818 (1995).

82 It is unclear whether an individual even can take any steps to effectively prevent observation via the use of some of these new technologies. Additionally, it is conceivable that observers could subject a person to observation by numerous surveillance tools, thereby making protection against observation prohibitively expensive, if possible at all. Judge McKay, in finding a subjective expectation of privacy against use of a thermal imaging scanner, stated that, without such an expectation, “the privacy of the home would be left at the mercy of the government’s ability to exploit technological advances.” United States v. Cusumano, 83 F.3d 1247, 1259 (1996) (McKay, J., concurring in part and dissenting in part).

83 Judge McKay, in arguing against the current standard, noted: “Technological wizardry neither obviates nor supplants a warrant.” Id. at 1261 (McKay, J., concurring in part and dissenting in part).

84 Bank records can reveal a person’s income, for example, through records of direct deposit. Credit card records can display which clothing stores or restaurants a person prefers. Perhaps even more sensitive information is contained in medical records, which can reveal
Even more information may be gleaned when personal information from a variety of sources is collected and placed in one comprehensive database. This result is known as the "Mosaic Theory." The mosaic theory is based on the principle that "the sum of bits of data can be greater than the individual bits [and that] putting pieces of information together can create new information." As society generates and stores more personal information than ever, and as databases from various businesses and government agencies become more interconnected, the compilation of a dossier on an individual from his personal information becomes easier.

Privacy concerns regarding personal information already exist as the amount of daily activity that is recorded increases. Consider the following hypothetical average day: A man stops at an automated teller machine on his way to work to withdraw cash from his checking account. Once at work, he swipes a security badge to gain access to the building. At lunch, the man goes to a nearby restaurant and

---

85 See Bercu, supra note 43, at 400 & n.89.

86 Id. at 400. The Supreme Court seems to accept the mosaic theory. In United States Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989), the Court saw a distinction between "scattered disclosure of the bits of information" in a Federal Bureau of Investigation rap sheet and "revelation of the rap sheet as a whole." Id. at 764. The Court went on to say that there is a "vast difference" between widely dispersed records and "a computerized summary located in a single clearinghouse of information." Id. Although the Court was examining the privacy interest under Exemption 7C of the Freedom of Information Act and was careful to point out that it was not examining a constitutional question, this "summary of information" argument pertains to the nature of information rather than the standard of privacy. Such an argument, therefore, would apply equally to a constitutional privacy right, even under a different standard.

87 "'Dossier Compilation' refers to a government agency's collection, combination, organization, and analysis of data about an individual." Bercu, supra note 43, at 399. Dossier compilation is not limited necessarily to government agencies; corporations or even private individuals also may engage in this activity. See ALDERMAN & KENNEDY, supra note 43, at 324-25; Glenn Rifkin, Licensee Is Now Selling a Lotus Database, N.Y. TIMES, July 11, 1991, at D5. Government and private firms alike can use a dossier to "profile" individuals for a number of purposes, ranging from targeting criminal suspects to marketing to potential customers. See Michael Higgins, Looking the Part, 83 A.B.A. J. 48-50 (Nov. 1997).

88 See Weingarten, supra note 46, at 741-42.

89 Security access to a building, computer system, or other protected area with an electronic identification card is known as "computer-assisted front end verification." See Bercu, supra note 43, at 399. Other examples of computer-assisted front end verification include passwords, personal identification numbers ("PINs"), voiceprint registers, and retinal scanners. See id. at 399 n.85.
pays with his credit card. On the way home, he takes the expressway, and pays his toll automatically as he drives through the E-Z Pass toll booth lane. Before going home, he stops at the supermarket to buy dinner, which the cashier scans at the checkout counter. Finally, once home, he orders a pay-per-view movie on TV with his touch-tone phone. All of these activities and transactions generate personal information about this man, which potentially may be stored and analyzed for an unlimited time.

While each of these transactions can reveal a particular activity in this man’s day, generally the information is stored in separate databases and does not reveal his overall daily activity. When put together, however, one can learn of his activities for

---

90 E-Z Pass lanes allow drivers to pay a toll without stopping at a toll booth. “Instead, scanning devices mounted in traffic lanes designated for E-Z Pass users read vehicle and account information transmitted by a tag mounted on the inside of the vehicle’s windshield, and the appropriate toll amount is subtracted from a prepaid account.” Richard Richtmyer, Automatic E-Z Pass Continues to Make Inroads in Northeast Toll Collection Plazas, BOND BUYER, Aug. 6, 1997, at 30; see Sue Epstein, Whitman Clears Way for Electronic Tolls; E-Z Pass Would Ease Congestion at Booths, STAR-LEDGER (Newark, N.J.), Apr. 3, 1997, at O22; Power, supra note 47, at 59; Marilyn Wimp, Toll Collection Going High-Tech, PHILA. BUS. J., Nov. 21, 1997, at 9. Although automated toll collection has been in use for several years in a number of states such as California, Oklahoma, and Texas, the E-Z Pass system will create a network that will allow drivers to use one pass in several states, including Delaware, Maryland, New Jersey, New York, and Pennsylvania, regardless of where the pass was purchased. See Epstein, supra at O22; Richtmeyer, supra at 30.

91 With the use of a check-cashing card or other “value” cards, supermarkets can (and do) keep track of their customers’ purchases. Some supermarkets even mail customers coupons that have been tailored to fit the customers’ buying habits. After purchasing a large bag of dog food for a friend, the author of this Note (who does not have a dog) received numerous coupons for dog food and dog products from a supermarket chain in Richmond, Virginia. Although most would find this amusing or, at worst, slightly annoying, it does raise the issue of the accuracy of personal information that is kept in various databases and the problems that inaccurate information can cause. Although the accuracy issue is outside the scope of this Note, discussions of this problem can be found in Alderman & Kennedy, supra note 43, at 325-26; Nicholas de B. Katzenbach & Richard W. Tome, Crime Data Centers: The Use of Computers in Crime Detection and Prevention, 4 COLUM. HUM. RTS. L. REV. 49, 52-54 (1972).

92 Such personal data could be “collect[ed], aggregat[ed] and manipulat[ed] throughout the individual’s lifetime.” Glancy, supra note 9, at 152. A similar problem exists with records collected by surveillance equipment, such as videotapes from security cameras. See Granholm, supra note 54, at 706-07. Another problem regarding electronic databases is that deleting data does not always remove it from the system. Often, it is possible to retrieve “deleted” data until the system writes over that memory location with new data. See Sergent, supra note 9, at 1205-06.
the entire day. Currently, people enjoy "anonymity through obscurity," meaning that, because these bits of information are scattered throughout numerous databases, it is difficult to create a mosaic from them.

A technique called "computer matching" can diminish an individual's anonymity through obscurity. By combining information contained in various databases, one can create a mosaic of a person's activity throughout any given day. Furthermore, by combining the information stored in these databases which has been acquired over an extended period of time, computer matching can reveal an individual's regular behavioral pattern.

One new technology with the potential to diminish individuals' anonymity greatly is the smart card. Like "conventional consumer cards," smart cards both contain personal information and cause it to be generated. Instead of using a magnetic strip to hold this information, however, smart cards contain a computer chip. This computer chip enables the smart card to hold significantly more information than a conventional card, and enables consumers to use the smart card in a greater number of ways.

---

93 Steven A. Bercu, Smart Card Technologies: Novel Privacy Concerns and the Legal Response, 7 J. PROPRIETY RTS. 2, 3 (No. 10, 1995).

94 Computer matching is a "comparison of two or more data bases ... to develop more information about data in the first data base. For example, a welfare agency could compare its list of benefits recipients with the records of a registry of motor vehicles to identify welfare recipients who own expensive cars." Bercu, supra note 43, at 399. As Robert Peck points out, "information collected for one purpose may be shared with other agencies and used for entirely different purposes ... [and] assembled into a complete personality profile at the touch of a computer button." Peck, supra note 1, at 28. Computer matching can be used by government agencies and private actors alike.

95 One commentator asserts that, even when an individual has no privacy interest in individual bits of information, a privacy interest may exist in the mosaic that results when these scattered pieces are combined. See Bercu, supra note 43, at 410-11.

96 For example, someone viewing a credit card record from one day could tell where the cardholder ate lunch on that day (assuming the bill was paid with the card). Viewing that record for a six-month period, however, could reveal how often the cardholder goes out to lunch, which restaurants he frequents, and how much he generally spends.

97 See Bercu, supra note 93, at 2. The term "conventional consumer card" includes credit, debit, automated teller machine ("ATM"), and identification cards. See id.

98 "A smart card can be characterized as a small computer that, for sake of convenience, borrows the form of a conventional consumer card." Id.

99 At this time, smart card microchips can hold more than 20 times the amount of information than a magnetic strip, and advances are expected to increase this amount. See id.

100 A smart card could be used as a credit card, debit card, telephone or calling card, and medical record card. Smart cards also could hold electronic cash, transforming a number of
The most significant difference between smart cards and conventional cards is that smart card technology permits all of this information to be stored on one card, which the consumer then uses to conduct a variety of different transactions. Although this promises greater convenience, data generated by smart cards potentially could be used to create an information mosaic on an individual with great ease.\(^\text{101}\) As Steven Bercu has pointed out, "such cards would appear to facilitate the linkage of types of data that were until now effectively quarantined from one another."\(^\text{102}\) By placing onto one card information that currently is dispersed widely among many databases, computer matching could become unnecessary for piecing together personal information to create a mosaic.\(^\text{103}\) The informational pieces of the mosaic would be located centrally already and, furthermore, it is likely that the increased utility of the card would induce increased usage, thereby generating a greater number of mosaic pieces.\(^\text{104}\)

\(^{101}\) Id.
\(^{102}\) Id.
\(^{103}\) Id.
\(^{104}\) Id.

Several states have considered implementing smart card technology into their drivers' licenses. See Tom Hester, Smart License Plan Died Elsewhere, STAR-LEDGER (Newark, N.J.), Feb. 15, 1998, at 025. It follows logically that, with the increased use of such cards for a greater number of purposes, smart cards would generate even greater amounts of personal information than conventional cards currently do.

"With smart cards, we run the risk that, for example, health, credit, location, spending, and communications data about an individual will converge...." Bercu, supra note 93, at 3.

For several scenarios describing the capacity for such information linkage to encroach upon privacy interests, see id. One executive in the smart card industry predicts that "[e]ventually, smart cards will replace every other card in your wallet." Kelly Spang, Smart, Compact and in Demand, COMPUTER RESSELLER NEWS, Feb. 24, 1997, at 151.

Smart card technology is not a distant reality. The cards already are in widespread use in several European countries, including Austria, France, Germany, and Switzerland. See Cynthia Weaver, Smart Card: Skepticism Lingers over the Business Case for Smart Cards Stateside, AM. BANKER, Mar. 3, 1997, at 4A. In the United States, smart cards already are in use in limited settings such as some universities and government agencies. See Jennifer Kingston Bloom, GSA Leads Charge on Commercial Cards, AM. BANKER, Dec. 3, 1998, available in 1998 WL 13326367; The Wired Campus: Technology is Radically Changing College Life, PC MAG., Oct. 1, 1998, available in 1998 WL 18431386.

Citibank is experimenting with a handheld device called the "VeriFone Personal ATM," which will allow customers to download electronic cash onto a smart card via phone lines. See Citibank to Test Putting an ATM in Your Hand, REPORT ON SMART CARDS, Apr. 28, 1997, available in 1997 WL 8987515. Additionally, Fischer International Systems Corporation has developed the "Smarty," a device that allows a personal computer's regular disk drive to read or write to a smart card. See Wendy S. Mead, Device Lets Ordinary PC Disk Drives Read Smart Cards and Write to Them, AM. BANKER, Mar. 4, 1997, at 4A.
Developments in both surveillance and information technology increase, in different ways, the potential for an erosion of privacy interests. The merging of these two types of technology, however, creates even further concerns.

III. THE MERGING OF SURVEILLANCE AND INFORMATION TECHNOLOGIES

While surveillance and information technologies each create privacy concerns in their own right, recent technological advances have blurred the distinction between these two formerly separate categories. Surveillance technology now can generate personal information, while personal information can be used for surveillance-like purposes.105 Merging these two fields of technology heightens privacy concerns beyond the point that either category invokes separately.

Perhaps the most poignant example of surveillance technology’s potential to generate personal information is found in Intelligent Vehicle Highway Systems (“IVHS”).106 IVHS technology is designed to make private transportation more efficient and safer through a variety of services.107 IVHS is an interactive system in which travelers and their vehicles communicate with the roadway in an effort to “reduce traffic congestion, improve highway safety, and reduce environmental harm from vehicular traffic.” To achieve these goals, an IVHS roadway must receive

---

105 Further, surveillance activity potentially could generate personal information that subsequently is used in a surveillance manner.

106 IVHS technology, also known as Intelligent Transportation Systems (“ITS”), encompasses more than just surveillance techniques. According to Sheri Alpert, IVHS technologies can be placed into seven distinct categories: surveillance, data/voice communications, traveler interface, traffic control strategies, navigation/guidance, data processing, and in-vehicle sensors. See Alpert, supra note 6, at 101.


107 A major IVHS testing ground is the “smart road,” a two-mile stretch of intelligent highway running from Blacksburg, Virginia to Interstate 81. See Mark Clothier, Here’s What Readers Want to Know About ‘Smart’ Road, ROANOKE TIMES & WORLD NEWS (Roanoke, Va.), May 25, 1997, at 4; Mark Clothier, Most-Asked Questions and the Answers, ROANOKE TIMES & WORLD NEWS (Roanoke, Va.), May 25, 1997, at 1; Kathy Loan, Montgomery County Delays Action on Tech Land Offer Price Mountain Site, ROANOKE TIMES & WORLD NEWS (Roanoke, Va.), Mar. 26, 1997, at NRV2.

108 Alpert, supra note 6, at 97.
information from the vehicles on the roadway. Surveillance equipment plays a role in acquiring the information needed to make an IVHS system work.

The use of surveillance equipment to monitor the traffic on roadways raises the privacy concerns that have been discussed previously. Unlike typical surveillance activity, however, IVHS surveillance equipment communicates with computerized monitoring systems. Because IVHS systems involve databases that process the information acquired through surveillance, IVHS also invokes interests in information privacy.

Operators could implement IVHS technology in such a way that each individual's travel activity would be monitored. The roadway could "watch" individuals each time they travel on it, observing such factors as: when and how often a traveler uses the roadway; how he drives, including travel habits such as vehicle speed or lane changes; at what points he makes stops along the way; and whether his vehicle is performing efficiently. As the system acquires this personal information

109 Because IVHS encompasses many technologies, operators could implement it in varying degrees on different roadways: The IVHS target concept is an interactive link of a vehicle electronic system with roadside sensors, satellites, and a centralized traffic management system to monitor constantly each vehicle's location and the traffic conditions. With more advanced systems, drivers would receive alternate route information in real time via two-way communications, onboard video screens, and mapping systems. See id. at 99 (citing Andrew H. Card, Jr., When 'Smart Cars' Meet 'Smart Highways', WASH. POST, Mar. 22, 1994, at D8 (advertising supplement)).

110 See id. at 101. Surveillance techniques that an IVHS system might use include "vehicle probes, infrared sensors, microwave and radar sensors, aerial surveillance, machine vision, Automated Vehicle Identification ("AVI"), closed circuit television, automated vehicle classification, and automated vehicle location." Id.

111 See supra notes 21-36, 53-83 and accompanying text. One commentator has asserted that "[IVHS] technologies provide an unprecedented mechanism for pervasive real-time surveillance of each person's physical location and movement from place to place." Glancy, supra note 9, at 152.

112 For a "top ten" list of privacy concerns invoked by IVHS technology, see Glancy, supra note 9, at 163-69.

113 Though IVHS technology could allow a driver to remain anonymous, some of the proposed IVHS benefits are available only when the technology identifies each driver.

114 Commentators have argued that "such surveillance also trammels one's constitutional right to travel, one's liberty of movement, and one's freedom to associate." Granholm, supra note 54, at 695 n.40 (citing James J. Tomkovicz, Beyond Secrecy's Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province, 36 HASTINGS L.J. 645, 709-11 (1985)). Although Ms. Granholm was discussing video surveillance specifically, other types of surveillance that track an individual's movement may infringe on these rights in the same way.
through surveillance, it can store the information in a database for future analysis. In this way, IVHS roadways combine surveillance and information technologies so that the system can be used for real-time monitoring and for later use in compiling an information mosaic. In doing so, IVHS invokes both intrusion and information privacy concerns.

While technological developments such as IVHS allow the use of surveillance to yield personal information, advances in database linkage and communication enable the use of personal information for surveillance purposes. The Financial Crimes Enforcement Network ("FinCEN") provides an example of such a merger. FinCEN has been described as "[a] hybrid between a data base and a focused surveillance tool," linking government and private databases to amass personal information from many different sources.

The U.S. Treasury Department initially developed FinCEN to detect and prevent money laundering crimes. The government recognized that this combination of databases was a powerful resource and developed other uses for FinCEN. Like any database that retrieves and stores personal information, FinCEN invokes information privacy concerns. Additionally, FinCEN raises concerns regarding the privacy interest against intrusion because of its surveillance abilities. The system has the capability to conduct surveillance in two ways: real-time tracking and data searches.

With real-time tracking, FinCEN can locate an individual by his transactions as they occur. For example, by using FinCEN to observe activity on a credit card, the surveillant can pinpoint the location of the subject each time he uses the card. Or,

---

115 See Alpert, supra note 6, at 117. This stored data would have IVHS uses, but potentially could be disseminated or sold for non-IVHS purposes, including law enforcement. See id. For other examples of potential non-IVHS uses of IVHS data, see id. at 112. 
116 Bercu, supra note 43, at 397. 
117 See id. at 390.
118 See id. One such use is checking job applicants' criminal histories. Still other new uses for FinCEN are being developed. See id. at 393-94. 
119 See supra notes 84-104 and accompanying text. 
120 See Bercu, supra note 43, at 397 ("Like a hidden camera, wiretap, or high-powered telescope or parabolic microphone, FinCEN can be used to observe individuals without alerting them to the presence of surveillance."). 
121 This is, of course, assuming that the owner of the card is the person using it. Similar credit card tracking systems exist in the private sector that can be used to help detect credit card fraud and locate stolen cards as they are used. For example, HCN Software, Inc., has developed a tracking program known as "Falcon," which a number of credit card companies use to help prevent fraudulent uses of their credit cards. See Oracle Corp., Alliance Online: Partner Description: HCN Software, Inc. (visited Apr. 2, 1999) <http://alliance.oracle.com/cat-doc/html/p6107.htm>; HCN Software, Inc., Product/Service Description: Falcon Credit
instead of tracking a particular person’s activity, a surveillant could use FinCEN to monitor activity at a specific location, such as an automated teller machine, and to observe each transaction as it occurs to gather information on all individuals who use that machine.

In addition to real-time tracking, FinCEN is capable of surveillance through sophisticated data searches. These searches comb the data stored in FinCEN’s memory looking for flags that signal suspicious financial activity. Such searches do not target a particular subject, but pour over “a sea of innocuous activity” to identify questionable activity. Therefore, probable cause with regard to any of the individuals subjected to the search does not exist. If courts establish more clearly the interest in information privacy, such inquiries could be subject to Fourth Amendment restrictions on illegal searches.

In time, systems such as FinCEN could become more commonplace, with a multitude of surveillance-capable databases observing each transaction. Such an information system even could be incorporated into an IVHS system, furthering the merger of surveillance and information technologies and the privacy concerns that they invoke.

IVHS and FinCEN are just two examples of the merging of surveillance and information technologies. As technological advances develop in both of these fields, more technologies that fall into both categories are likely to emerge. As this occurs, intrusion and personal information privacy interests will be in further jeopardy of being diminished. Courts, therefore, must address privacy concerns as they relate to

---

122 See Bercu, supra note 43, at 397 (“[U]nlke previous law enforcement technologies, FinCEN’s system has a measure of intelligence. It is not simply a data base of stored information awaiting retrieval.”).

123 Id. at 412.

124 See id. at 411-12. Similar problems exist with the use of “conventional” surveillance equipment on nonsuspect individuals, involving activity-based surveillance as opposed to information-based surveillance. See United States v. Cusumano, 83 F.3d 1247, 1254 (10th Cir. 1996) (McKay, J., concurring in part and dissenting in part) (describing the use of thermal imaging scanners by police on nonsuspects); supra notes 53-80 and accompanying text.

125 Of course, if a private actor operated a FinCEN-like system, such Fourth Amendment restrictions would not apply.
these technologies before such technologies are developed and introduced into society.

IV. CURRENT AND PROPOSED PRIVACY PROTECTIONS

Current protections of individuals' right to privacy fall into three categories: common law, legislative, and constitutional. These protections do not address adequately the ability of many emerging technologies to invade a person's interest in privacy. In other words, new technologies can create a disparity between one's right to privacy and one's interest in privacy. Advances in both the surveillance and information technology fields, considered separately, allow legal intrusions upon one's interest in privacy. When these two types of technology converge, the problem is compounded further.

A. Common Law Protections of the Right to Privacy

Common law privacy protection takes the form of a tort action. Dean Prosser categorized common law invasion of privacy as four distinct tort claims: false publicity, intrusion, public disclosure of private facts, and appropriation of name or likeness. The first of these torts, false publicity, does not apply to information privacy because the information involved generally is not false. Similarly, the second tort of intrusion does not apply to information privacy because this tort relates to physical intrusions and trespass. The third privacy tort, public disclosure of

---

126 One commentator suggests that a fourth category of privacy protections exists: contractual protections. See Petersen, supra note 6, at 179-80. Contractual protections are relevant particularly to information privacy issues. Although Ms. Petersen recognizes that current contractual protections of privacy are not adequate, she states that "[t]he contractual solution to the problem of information privacy could work in conjunction with federal legislation setting a minimum standard of privacy for all individuals and all information." Id. at 180. Because this approach requires legislative protection before it is effective, this Note treats contractual protection of privacy as a subset of legislative protection.

127 For an interesting discussion of arguments against the right to privacy, see Glancy, supra note 9, at 169 ("Political viewpoints which place more importance on the community or society than on its individual members generally disapprove of privacy.").


129 See Petersen, supra note 6, at 176 ("The information is generally true or at least believed to be true.").

130 See Prosser, supra note 128, at 392. Although courts could expand this tort beyond
private facts, requires that the information disclosed be offensive, and that it be disseminated to the public at large. Lastly, the tort of appropriation of name or likeness applies only to public figures, and so is not useful for most information privacy cases.

Many privacy issues that stem from new technologies do not fit neatly into these traditional applications of common law tort claims of invasion of privacy. Even if these torts expanded to include such issues, however, common law tort protection is insufficient against rapidly developing technologies. A more fundamental problem with the common law tort approach is that legislative action or judicial decisions can preempt these torts. If the mood of the day favors information dissemination over information privacy, common law legal protections in privacy interests can be decimated with one new law or court decision. Later, if public opinion again favors privacy, it may be difficult to recapture legal protection for those interests. Indeed, it may be impossible, if the technology which creates the invasion of privacy has become widespread and is obtained easily.

physically intrusions in a way similar to the Supreme Court’s expansion of Fourth Amendment from the trespass doctrine to the Katz doctrine, Petersen points out that “there has been virtually no change to the common-law privacy torts,” and that “the law has not kept pace with the changing technology and values of modern times.” Petersen, supra note 6, at 178.

See Prosser, supra note 128, at 393-96. A reasonable person standard determines whether the information in question is “offensive and objectionable.” Id. at 396. It seems unlikely that personal information, such as grocery purchases or bank transactions, would be offensive. Even if the information—or, perhaps more likely, its disclosure—met this standard, organizations generally trade personal information among themselves rather than disclose it to the general public as the tort requires.

See id. at 398; Petersen, supra note 6, at 177. Ms. Petersen argues that, of the common law protections, the tort of appropriation provides the best solution to the problem of information privacy and, thus, courts could expand appropriation claims to include persons who are not public figures. See id. at 177-78. The concept of name or likeness also would have to be expanded, however, to include personal information. Given Petersen’s observation that common law privacy torts do not appear to be evolving, see supra note 130, it seems unlikely that such a double expansion of this tort will occur.

See supra notes 53-104 and accompanying text.

Even if lawmakers subsequently outlaw the technology at issue to address the problem, significant damage already may have occurred if vast amounts of personal information have been made available publicly.
B. Legislative Protections of the Right to Privacy

Legislative protections of privacy appear in a variety of statutes aimed at both government and private actors. The Fair Credit Reporting Act of 1970\textsuperscript{135} was one of the first attempts to protect individuals' interest in information privacy from private actors, while the Privacy Act of 1974\textsuperscript{136} was among the earliest statutory protections against governmental misuse of personal information. Congress has enacted a wide variety of other statutes in an effort to protect information privacy, including the Bank Secrecy Act,\textsuperscript{137} the Cable Communications Policy Act,\textsuperscript{138} the Computer Matching and Privacy Protection Act,\textsuperscript{139} the Driver's Privacy Protection Act,\textsuperscript{140} the Electronic Communications Privacy Act,\textsuperscript{141} the Driver's Privacy Protection Act,\textsuperscript{140} the Electronic Fund Transfer Act,\textsuperscript{142} Title III of the Omnibus Crime Control and Safe Streets Act (also known as the Wiretap Act),\textsuperscript{143} the Right to Financial Privacy Act,\textsuperscript{144} and the Video Privacy Protection Act.\textsuperscript{145}

The large number of acts protecting privacy and the diversity of their subject matter suggest two important points.\textsuperscript{146} First, privacy issues are surfacing in more areas. As more transactions and activities lose their anonymous nature, due either to surveillance or affiliation with an electronic database, those transactions generate more personal information. Conversely, as more information becomes available, more informational surveillance becomes possible. As privacy becomes an issue in a previously anonymous area, Congress reactively enacts legislation to combat the perceived invasion of privacy interests.\textsuperscript{147}

\begin{itemize}
\item \textsuperscript{135} 15 U.S.C. §§ 1681-1681s (1994).
\item \textsuperscript{136} 5 U.S.C. § 552a (1994).
\item \textsuperscript{138} 47 U.S.C. §§ 521-611 (1994).
\item \textsuperscript{139} 5 U.S.C. § 552a(o) (1994).
\item \textsuperscript{140} 18 U.S.C. §§ 2721-25 (1994).
\item \textsuperscript{142} 15 U.S.C. §§ 1693-1693r (1994).
\item \textsuperscript{143} 18 U.S.C. §§ 2510-21 (1994).
\item \textsuperscript{144} 12 U.S.C. §§ 3401-22 (1994).
\item \textsuperscript{145} 18 U.S.C. § 2710 (1994).
\item \textsuperscript{146} The examples listed above are all federal laws. The number and variety of privacy-related laws that state legislatures have enacted is even greater. See Glancy, \textit{supra} note 9, at 177-80.
\item \textsuperscript{147} The Video Privacy Protection Act, 18 U.S.C. § 2710 (1994), also known as the Bork Bill, provides an excellent example of the reactive nature of privacy legislation. "The impetus for enacting the measure arose as a result of Judge Robert Bork's 1987 Supreme Court
Second, existing legislation aimed at protecting privacy generally is ineffective when new technologies emerge. This ineffectiveness is why legislatures must pass new legislation to target specific activities.\(^{14}\) For example, the Wiretap Act of 1968 did not protect communications transmitted over cellular phones, pagers, or electronic mail. Congress subsequently passed the Electronic Communications Privacy Act of 1986 to account for technologies that had "outpaced ... [the] statutory protections."\(^{149}\) This patchwork approach to privacy protection does not address a technology's privacy implications until after they have become an issue.\(^{150}\) Additionally, as information and surveillance technologies continue to develop more rapidly and are used for a greater variety of purposes, these technologies increasingly will outpace the laws that legislatures have designed to regulate their use.\(^{151}\)

Furthermore, legislative protections are subject to the same criticism of instability as are common law privacy tort claims. Legislation can be amended or repealed, and a reliance on measures that are changed easily to protect the fundamental right of privacy is insufficient. If public sentiment swings against privacy, even briefly, facets of that right could be lost forever.\(^{152}\)

\(^{14}\) An in-depth examination of all of these laws and a discussion of why they provide insufficient protection for privacy interests are beyond the scope of this Note. For a discussion of legal privacy protections, see Kastenmeier et al., supra note 59. See also Bercu, supra note 43, at 423-33 (discussing several federal privacy statutes).

\(^{149}\) One commentator has asserted that "the statutory approach ... leaves loopholes that rapidly changing technologies can enlarge." Peck, supra note 1, at 29. For an example of such a loophole, see Askin v. McNulty, 47 F.3d 100 (4th Cir.) (holding that a cordless phone that transmitted via radio waves was not protected by the Electronic Communications Privacy Act of 1986 because such a transmission did not fit the definition of wire, oral, or electronic communication), cert. denied, Askin v. United States, 516 U.S. 944 (1995).

\(^{152}\) Admittedly, this argument assumes that information privacy is a component of the
C. Constitutional Protection of the Right to Privacy

Because of the above concerns regarding common law and legislative privacy protections, constitutional safeguards are a more effective means of ensuring that new technology does not erode privacy. Constitutional protections are not subject to whimsical change the way the common law or legislation can be. Unlike the statutory attempts to prevent technology from encroaching on privacy, constitutional protections address fundamental rights, not specific technologies, and would not be outpaced readily by advances in technology.

Currently, however, the Constitution does not provide adequate protection for privacy interests relating to new technologies. This is so for three reasons: First, the Katz test is insufficient in the face of new technologies; second, although the interest in personal information is strong, the legal right to information privacy is weak; and third, the Constitution ensures a right of privacy against the government only, not against private actors. The document itself need not undergo changes to address these insufficiencies. Instead, a change in constitutional interpretation, as has occurred many times before, would align privacy interests and privacy rights.

1. Improving the Katz Test to Account for New Technologies

The Katz doctrine is itself an example of how the Supreme Court has changed its interpretation of a constitutionally guaranteed protection to keep pace with developing technology. The Court expanded individuals’ Fourth Amendment fundamental right to privacy. If information privacy is not part of the fundamental right to privacy, and such privacy is lost through legislation, one could argue that the privacy right has not been diminished. There clearly is an interest, however, in privacy of personal information. See supra notes 37-52 and accompanying text. Aligning such interests in privacy with the legal right to privacy is the goal of legislative privacy protections.

153 This is not to say that the breadth of constitutional rights does not change over time. Protections provided by the Constitution do, and should, change as society evolves and needs develop. That a constitutional right to privacy exists at all, even though not explicitly stated in the document, is a testament to this fact. Such changes, however, occur more gradually and with greater deliberation, rather than in heated response to a perceived crisis.

154 See Whalen v. Roe, 429 U.S. 589 (1977) (holding that a state interest in controlling pharmaceuticals outweighs the individual’s privacy right); supra notes 48-51 and accompanying text.

155 See Katz v. United States, 389 U.S. 347 (1967) (holding that a telephone wiretap constituted a search under the Fourth Amendment); supra notes 32-36 and accompanying text (discussing the Katz test for determining whether a search has occurred, and the ways the test expanded Fourth Amendment protections).
rights in *Katz* by abandoning the trespass doctrine.\(^{156}\) The expansion of this constitutionally protected right stemmed from the realization that surveillance technology allowed the government to infringe on an individual's interest against intrusion without physical trespass.\(^{157}\)

Today, the *Katz* test as applied is insufficient against emerging new technologies.\(^{158}\) The problem lies in courts' understanding of the subjective expectation of privacy held by a surveillance subject. Even if the objective prong of the *Katz* test is satisfied,\(^{159}\) a subject still must take affirmative protective steps to display a subjective expectation of privacy against surveillance.\(^{160}\) The development of new technologies, however, makes it difficult or impossible to protect against surveillance intrusions.\(^{161}\)

To strengthen the *Katz* doctrine so that it provides a real right against intrusion in the face of advances in surveillance equipment, courts must interpret the subjective prong of the *Katz* test to protect against such technology. Individuals who are the subject of high-tech searches\(^{162}\) should be deemed to hold a subjective expectation of privacy even without taking affirmative steps to protect themselves. Furthermore, the absence of available measures to protect oneself against an advanced method of surveillance should constitute a subjective expectation that no one is conducting such surveillance.\(^{163}\)

---

\(^{156}\) See supra notes 28-31 and accompanying text.

\(^{157}\) See *Katz*, 389 U.S. at 362 (Harlan, J., concurring) (stating that Fourth Amendment protections extend beyond physical invasion, because "in the present day . . . reasonable expectations of privacy may be defeated by electronic as well as physical invasion").

\(^{158}\) The failure of the *Katz* test today is analogous to the failure of the trespass doctrine against technological advancements earlier in the century.

\(^{159}\) Because the objective prong of the *Katz* test uses a "reasonable person" standard, as surveillance technology becomes more advanced—and thereby more intrusive—it is likely that an expectation of privacy against such technology will be "one that society is prepared to recognize as 'reasonable.'" *Id.* at 361 (Harlan, J., concurring). Although such a societal opinion will satisfy the first prong of the *Katz* test, it will not address the second, subjective prong.

\(^{160}\) See supra notes 55-59 and accompanying text.

\(^{161}\) See supra notes 81-83 and accompanying text.

\(^{162}\) Such high-tech searches should include activity-based surveillance methods and data surveillance alike. An increased right in information privacy is needed, however, before data surveillance constitutes a search. See infra notes 168-72 and accompanying text.

\(^{163}\) This interpretation of the subjective expectation of privacy provides a defense against surveillance equipment that subjects are aware exists but cannot escape, and against new technology that subjects are not yet aware exists.
For example, under the current *Katz* test, the subject of passive millimeter wave imaging\textsuperscript{164} surveillance would not have a subjective expectation of privacy unless he took steps to protect himself from such surveillance. This test is not an accurate measure of whether a person expects another party to be measuring the electromagnetic rays emitted from his body. Most people are not aware of this surveillance capability and, therefore, would not think to attempt protective measures against its intrusion. Even if most people did know that such technology exists, because it is not used commonly they would not expect to be the subject of its use or know how to protect against its intrusion. It is natural to assume, therefore, that these subjects do not expect others to be measuring their emitted electromagnetic rays; that is to say, they have a subjective expectation of privacy against such surveillance.\textsuperscript{6}

By removing the requirement that the subject take affirmative measures to protect against new surveillance equipment, this new interpretation of *Katz* essentially provides a presumption that the subject has a subjective expectation against technologies of which he does not know or against which he cannot protect himself.\textsuperscript{165} Although lower courts could begin to construe the *Katz* doctrine in this way on their own,\textsuperscript{6} the Supreme Court should grant certiorari to a Fourth Amendment case involving a new technology and establish this application of the *Katz* test as the law of the land.

\textsuperscript{164} See supra note 77.

\textsuperscript{165} Of course, evidence could show that the subject in this example did not have a subjective expectation of privacy. If the subject was aware of the use of passive millimeter wave imaging and knew how to protect himself against such surveillance—if this is possible—but took no measures to protect himself, he would have no subjective expectation of privacy.

\textsuperscript{166} This interpretation of *Katz* does not modify the *Katz* test as dramatically as it may seem. First, the defendant’s presumption of a subjective expectation of privacy is rebuttable. See supra note 165. Second, the presumption modifies only the subjective aspect of the *Katz* test. If a particular surveillance technology becomes well-known publicly, and if publicly accessible defenses to that method of surveillance are available, an objective expectation of privacy against that surveillance method no longer would exist. In this scenario, such surveillance would not constitute a search, regardless of whether the defendant had a subjective expectation of privacy, because no societal objective expectation would exist.

\textsuperscript{167} Some courts already have granted a subjective expectation of privacy against thermal imaging scanners, but only after the defendant took affirmative steps to prevent such surveillance. See, e.g., United States v. Ishmael, 48 F.3d 850, 854-55 (5th Cir.) (holding that defendants, indoor marijuana growers, exhibited a subjective expectation of privacy by constructing their laboratory in great secrecy and building it as a basement to a steel building that was not visible from a public road), cert. denied, 516 U.S. 818 (1995).
2. Strengthening the Legal Right to Information Privacy

The second reason that current constitutional interpretation provides insufficient privacy protection is that the legal right to information privacy is not strong. The Constitution does not state explicitly that a right to privacy exists; instead, that right has been "found" by the Supreme Court. The Court has held that an interest in information privacy does exist, but that an individual's right to privacy in personal information is weak. Just as the Court gradually expanded privacy in the realm of searches and reproductive rights, it similarly should expand an individual's right to privacy with regard to personal information. As the amount and uses of personal information increase, such information becomes more revealing about a person's activities and lifestyle. When information networks generate personal information to such an extent that the information can be used for surveillance purposes, either in retrospective analysis or in real-time tracking, analyzing such information effectively becomes a search. A stronger privacy right in personal information, and the subsequent requirement that agencies obtain a warrant before conducting such searches, would ensure that individuals' interest against intrusion and their interest in information privacy would receive greater protection from government misuse of data.

3. Applying the Constitutional Protection of Privacy Against Private Actors

Although a constitutional strengthening of the right to information privacy would improve individuals' protection against government action, it would not address the third reason that the Constitution currently does not provide sufficient privacy protection: The constitutional right to privacy grants certain privacy interests a legal right against the government, but not against private actors. Developments in both

---

168 See supra notes 37-41 and accompanying text.
169 See Whalen v. Roe, 429 U.S. 589, 598-602 (1977) (holding that the state interest in regulating medicine outweighed the information privacy rights of individuals whose personal information appeared in the database); supra notes 48-51 and accompanying text.
170 See supra note 52.
171 See supra notes 24-31 and accompanying text (describing the replacement, by the Supreme Court, of the trespass doctrine with the Katz test for determining when a search has occurred under the Fourth Amendment).
172 See supra notes 37-42 and accompanying text.
173 At least one commentator argues that the private sector poses a greater threat to privacy than does the government. See Petersen, supra note 6, at 165.
surveillance and personal information technology, often intertwined, make it easier for nongovernment entities to acquire and use personal information.\(^\text{174}\)

Even a very strong privacy right against the government is of limited use if it does not protect individuals from private actors with access to the same information and technology. Although many of the various legislative measures apply to the private sector, the existing patchwork of statutes provides insufficient protection.\(^\text{175}\) Therefore, constitutional protection of information privacy must extend to private actors as well as the government.

While at first blush such an expansion of the privacy right may seem like a radical extension of the Constitution’s reach, further examination reveals that it is not a great departure from past constitutional interpretation. For example, an analysis of Commerce Clause jurisprudence demonstrates that the Supreme Court has allowed rather tenuous connections to interstate commerce to justify Congressional regulation of business activity.\(^\text{176}\) Although the Commerce Clause requires an activity to be interstate to fall within Congress’s reach,\(^\text{177}\) by expanding the definition of interstate commerce the Court allowed Congress to assert authority over almost any commercial activity. Similarly, the Court could allow such tenuous links to private actors in the realm of surveillance and personal information to establish that they are within the reach of the constitutional right to privacy.\(^\text{178}\) From this position, the Court

\(^\text{174}\) One such technological development is the portability of surveillance equipment. For example, officials expect passive millimeter wave imaging equipment to become handheld for portable use. See Butterfield, supra note 77, at A8; Hansen, supra note 76, at 46-48. In addition to technological advances, political developments also may bring private entities into contact with more personal information. For example, private corporations likely will implement a large portion of IVHS technology. One commentator predicts that the federal government will fund only 20% of IVHS costs. See Norman Y. Mineta, Transportation, Technology and Privacy, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 3, 5-6 (1995). Privatization makes “ownership and control of communications networks . . . very complex. . . . [A] communications system is now . . . put together and operated by a wide variety of firms.” Weingarten, supra note 46, at 742.

\(^\text{175}\) See supra notes 135-52 and accompanying text.

\(^\text{176}\) See, e.g., Katzenbach v. McClung, 379 U.S. 294 (1964) (holding that a local restaurant that purchased supplies from out of state and served interstate travelers affected interstate commerce); Wickard v. Filburn, 317 U.S. 111 (1942) (holding that wheat grown for personal use affected interstate commerce and was subject to regulation).

\(^\text{177}\) The Commerce Clause grants Congress the authority to “regulate Commerce with foreign Nations, and among the several States.” U.S. CONST. art. I, § 8, cl. 3.

\(^\text{178}\) The Court already has expanded the state action doctrine to include private actors in contexts where the private actor is performing a traditionally exclusive public function. See, e.g., Marsh v. Alabama, 326 U.S. 501, 507-09 (1946) (holding that, under the public-function doctrine, owners of the “company town” of Chickasaw, Alabama, could not restrict free
need take only a small step to expand privacy jurisprudence to encompass private actors, regardless of their affiliation with the state.\textsuperscript{179} Simply including private actors within the reach of the right to privacy with regard to surveillance and personal information, however, would be preferable to justifying their inclusion through attenuated connections as this more straightforward approach would leave no doubt as to whether a particular actor could escape the Constitution's reach.\textsuperscript{180}

The idea of a constitutional right to privacy reaching private actors is not without precedent: Several states already have developed a right to privacy that provides

---

\textsuperscript{179} This example does not support misconstruing constitutional authority or creating a subterfuge to achieve a desired result. Instead, it demonstrates that the Court has expanded constitutional doctrines significantly in the past, and that doing so again would not be unprecedented.

\textsuperscript{180} Numerous articles discuss whether the Court should abolish the state action doctrine. See generally Erwin Chemerinsky, Rethinking State Action, 80 NW. U. L. REV. 503, 506 (1985) (concluding that "limiting the Constitution's protections of individual rights to state action is anachronistic, harmful to the most important personal liberties, completely unnecessary, and even detrimental to the very goals that it originally intended to accomplish") (citing Henry J. Friendly, THE DARTMOUTH COLLEGE CASE AND THE PUBLIC-PRIVATE PENUMBRA 17 (1968) (arguing that the broadening of the state action doctrine to include state inaction requires a pragmatic rather than a mechanical application); Charles Black, Jr., Foreword, "State Action," Equal Protection, and California's Proposition 14, 81 HARV. L. REV. 69 (1967) (discussing the use of the state action doctrine to deny state involvement in acts of racism); Paul Brest, State Action and Liberal Theory: A Casenote on Flagg Brothers v. Brooks, 130 U. PA. L. REV. 1296 (1982) (criticizing the Court's manipulation of the public/private distinction while purporting to rely on the state action doctrine); Harold W. Horowitz & Kenneth L. Karst, The Proposition Fourteen Cases: Justices in Search of a Justification, 14 UCLA L. REV. 37 (1966) (discussing the utility of the significant state involvement requirement of the state action doctrine); Michael J. Phillips, The Inevitable Incoherence of Modern State Action Doctrine, 28 ST. LOUIS U. L.J. 683 (1984) (surveying the evolution of the state action doctrine and discussing its inherent contradictions); John Silard, A Constitutional Forecast: Demise of the "State Action" Limit on the Equal Protection Guarantee, 66 COLUM. L. REV. 855 (1966) (predicting the end of the state action doctrine as a means of analyzing equal protection violations); Jerre S. Williams, The Twilight of State Action, 41 TEX. L. REV. 347 (1963) (forecasting the end of the state action doctrine as a test for analyzing violations of constitutional rights)).

Detailed analysis of the many issues that this topic invokes is outside the scope of this Note. Additionally, this Note does not approach the subject of whether the Court should abolish the state action doctrine altogether, or only in certain contexts. Instead, it suggests a possible solution to the inadequacy of constitutional privacy protection regarding the growing problem of the convergence of surveillance and information technologies.
TECHNOLOGY AND THE RIGHT TO PRIVACY

Although state constitutions vary from the United States Constitution, these states' privacy protections show that a constitutional right to privacy reaching the private sector is not unreasonable. In fact, a federal privacy doctrine reaching the private sector may be more reasonable than a multitude of different state protections, in that a federal right would provide nationwide actors uniform treatment in all of the states.

181 In Alaska, California, Hawaii, Illinois, and Louisiana, the state constitutional right to privacy applies to both the private and the public sector. See Glancy, supra note 9, at 190-91. In California, for example, the explicit right to privacy in the Constitution states: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." CAL. CONST. art. I, § 1. California courts have interpreted this constitutional guarantee to protect against government and private parties alike. See, e.g., Porten v. University of S.F., 134 Cal. Rptr. 839, 842 (1976) ("Privacy is protected not merely against state action; it is considered an inalienable right which may not be violated by anyone."). See also McCloskey v. Honolulu Police Dep't, 799 P.2d 953, 956 (Haw. 1990) ("[I]t is the intent of [this] Committee to insure that privacy is treated as a fundamental right for the purposes of constitutional analysis. Privacy as used in this sense concerns the possible abuses [of] highly personal and intimate information in the hands of government or private parties . . . ." (quoting Comm. of the Whole Rep. No. 15, reprinted in 1 PROCEEDINGS OF THE CONSTITUTIONAL CONVENTION OF HAWAI'I OF 1978, at 1024 (1980) (discussing HAW. CONST. art. I, § 6))); Leudtke v. Nabors Alaska Drilling, Inc., 768 P.2d 1123, 1132-33 (Alaska 1989) (finding that, although the Alaska Constitution generally requires state action, its privacy clause, see ALASKA CONST. art. I, § 22, contributed to the public policy basis for a right to employee privacy against private employers); Moresi v. Department of Wildlife & Fisheries, 567 So. 2d 1081, 1092 (La. 1990) (finding that, although no violation of plaintiffs' right to privacy occurred in this case, the right to privacy guaranteed by the state Constitution, see LA. CONST. art. I, § 5, "goes beyond limiting state action"); Walinski v. Morrison & Morrison, 377 N.E.2d 242, 244-45 (Ill. App. Ct. 1978) (finding that the Illinois Constitution, see ILL. CONST. art. I, § 17, granted a private cause of action for discrimination against a private employer).

182 This variation particularly is true in the realm of privacy. Several states other than Alaska, California, Hawaii, Illinois, and Louisiana acknowledge explicit privacy rights in their constitutions; unlike these five states, however, other constitutional privacy provisions do not reach the private sector. See Glancy, supra note 9, at 177; see also generally Mark Silverstein, Privacy Rights in State Constitutions: Models for Illinois?, 1989 U. ILL. L. REV. 215, 226-58 (1989) (surveying the privacy rights provided by various state constitutions).

183 The variation of privacy protections among the states can create difficulties for organizations that operate in several states. See, e.g., Laura B. Pincus & Clayton Trotter, The Disparity Between Public and Private Sector Employee Privacy Protections: A Call for Legitimate Privacy Rights for Private Sector Workers, 33 AM. BUS. L.J. 51, 54-55 (1995) ("There are inherent problems with a state-by-state program for privacy protection. Not only are an employee's rights dependent upon the state in which he or she lives, but the
CONCLUSION

Due to developing surveillance and information technologies and the merger of these technologies, the constitutional right to privacy currently does not coincide with individuals’ interests in privacy. New surveillance equipment allows surveillants to observe, without a search warrant, that which most individuals consider private. This surveillance technology, therefore, invades an individual’s privacy interest against intrusion without infringing upon his legal right to privacy. As such, advances in surveillance technology diminish the legal right to privacy.

The growing use of personal information in society by both the government and private actors threatens to diminish further the right to privacy. As technological advances increase the amount of daily activities that generate personal information, an individual’s ability to control his personal information decreases. This information reveals much about one’s habits and routine, and a lack of control over one’s “data image” diminishes one’s privacy.

An even greater threat to privacy stems from the merger of surveillance and information technologies. When activity-based surveillance generates personal information, and when information technology allows surveillance uses of existing personal information, privacy concerns that formerly applied to only one of these fields now apply to both. IVHS and FinCEN are two examples of this convergence of technologies. As developments in both fields continue, more systems that invoke surveillance and information privacy concerns surely will emerge.

To prevent these technological developments from eroding the right to privacy, courts need to reexamine that right. The Supreme Court should expand the Fourth Amendment protection against warrantless searches to include an expectation against the use of advanced surveillance equipment and against data searches of personal information. For the latter to occur, the Court must strengthen the constitutional right to information privacy, which currently is weak. Finally, because technological and political developments are increasing the role that private actors play in these merging technologies, information privacy must protect individuals from private actors as well as the government. One way to ensure this protection is for the Supreme Court to construe the constitutional right to information privacy to reach private actors as well as the government.
Over one hundred years ago, in discussing the right to privacy, Justices Warren and Brandeis had the foresight to realize that "it [is] necessary from time to time to define anew the exact nature and extent of such protection [due to] [p]olitical, social, and economic changes." Developments in both surveillance and information technologies make now such a time. The Supreme Court must "define anew" the right to privacy, lest these "[r]ecent inventions and business methods" erode that right until it no longer has meaning.

THOMAS B. KEARNS

---

185 Id. at 195.