what-when-how

In Depth Tutorials and Information

Reasonable expectation of privacy

The "reasonable expectation of privacy" test is applied to determine whether the Fourth Amendment to the U.S. Constitution will protect against certain searches and seizures by government officials. The test was first formulated by the U.S. Supreme Court in Katz v. United States, 389 U.S. 347 (1967). The test actually appeared in a concurring opinion by Justice Harlan, who stated the Fourth Amendment covers a search or seizure if (1) a person exhibits an "actual or subjective expectation of privacy" and (2) "the expectation [is] one that society is prepared to recognize as 'reasonable.'"

What constitutes a reasonable expectation of privacy? The answer is rather difficult because it involves understanding a litany of Supreme Court decisions in particular cases. There is no particular formula for determining when a reasonable expectation of privacy exists. Therefore, one must look at the specific circumstances of each case in which the Supreme Court rendered a decision and make generalizations and analogies. In Katz, the Supreme Court famously stated,

For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.

In practice, however, the Court has not always adhered to this approach. In several cases, the Supreme Court has concluded that people lack a reasonable expectation of privacy when they are observed in public. In what is known as the plain view doctrine, the Supreme Court has held that "it has long been settled that objects falling in the plain view of an officer who has a right to be in the position to have that view are subject to seizure and may be introduced in evidence" (Harris v. United States, 390 U.S. 234, 236 (1968)). In Florida v. Riley, 488 U.S. 445 (1989), for example, the Supreme Court held that a person lacked a reasonable expectation of privacy in his greenhouse where the roof was partially open to a view from above and where the police flew over it in a helicopter to peer inside.

People also lack a reasonable expectation of privacy in being overheard when speaking in a public place. In private places, however, if people cannot be seen or heard by others, then generally they will be deemed to have a reasonable expectation of privacy.

Consistent with the view that people lack a reasonable expectation of privacy in public, the Supreme Court has held that a person lacked a reasonable expectation of privacy when law enforcement officials installed a physical-tracking device that monitored where he drove in his car. According to the Court, a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another" (United States v. Knotts, 460 U.S. 276 (1983)). In contrast, a tracking device that monitored a person's movements in his home did infringe upon his reasonable expectation of privacy (United States v. Karo, 468 U.S. 705 (1984)). Whereas the movements in Knotts were in public, the movements within the residence were not, and this amounted to an impermissible search of the residence.

The police can apply sensory enhancement technology to what they see or hear with the naked senses. In Texas v. Brown, 460 U.S. 730 (1983), the Supreme Court held that using a flashlight to "illuminate a darkened area" did not implicate a reasonable expectation of privacy. In Dow Chemical Co. v. United States, 476 U.S. 227 (1986), government officials flew over the defendant's property and used a high-tech aerial-mapping camera to take photographs, which could then be magnified to reveal very small objects. The Supreme Court

concluded that there was no reasonable expectation of privacy because the "mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems."

There are instances, however, when using sensory enhancement technology can implicate a person's reasonable expectation of privacy. In United States v. Kyllo, 533 U.S. 27 (2001), the police used a thermal sensor imaging device to detect heat patterns coming from a person's home. Although the police did not enter the residence, the device measured the heat emanating from the residence. The Supreme Court nevertheless concluded that the defendant had a reasonable expectation of privacy because the device could be used to detect activities within his home.

The Supreme Court also has concluded that people lack a reasonable expectation of privacy in information exposed to third parties. This has become known as the "third-party doctrine." For example, in United States v. Miller, 425 U.S. 435 (1976), the Court held that people lack a reasonable expectation of privacy in their bank records because "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." Employing analogous reasoning in Smith v. Maryland, 442 U.S. 735 (1979), the Court held that people lack a reasonable expectation of privacy in pen register information (the phone numbers they dial) because they "know that they must convey numerical information to the phone company," and therefore they cannot "harbor any general expectation that the numbers they dial will remain secret." Similarly, in California v. Greenwood, 486 U.S. 35 (1988), the Supreme Court concluded that people cannot have a reasonable expectation of privacy in trash left for collection on the curb because they "exposed their garbage to the public" and "placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector."

The third-party doctrine is difficult to square with other Fourth Amendment doctrines. If a person is talking on the phone to another person, this does not negate either person's reasonable expectation of privacy, even though the two are sharing information with each other. One of the parties to the conversation can betray the other, and people do not have a reasonable expectation that their confidants will not communicate their secrets to the police. However, so long as both parties to the conversation have resolved to keep the conversation private, they have a reasonable expectation of privacy if they did not speak in public or where audible to others. Nevertheless, if a person provides information to a bank or a company, then the person has been deemed to have relinquished his reasonable expectation of privacy— even if the bank or company desires that the information be kept private. The Court has not explained why exposing information to a bank or company is different from exposing it to another conversant over the telephone.

The third-party doctrine also gives rise to some difficult issues because of life in the information age. Countless companies maintain detailed records of people's personal information: Internet service providers, merchants, bookstores, phone companies, cable companies, and many more. According to the third-party doctrine, a person lacks a reasonable expectation of privacy in this information because third parties possess it.

Taken together, the cases suggest that the Supreme Court believes that people lack a reasonable expectation of privacy whenever something is exposed to the public or to third parties. In other words, if a person keeps something a total secret, then he can reasonably expect it to be private. However, once something is revealed in public or to others, then he can no longer reasonably expect privacy.

Methodologically, how does the Supreme Court determine whether there is a reasonable expectation of privacy? At first glance, the reasonable expectation test appears to be empirical: a reasonable expectation of privacy is an expectation that a majority of members in society deem reasonable. However, in applying the test, the Supreme Court has rarely looked to empirical evidence or to polls. Instead, the Court has typically applied its own notions of privacy. In at least one instance, the Court acknowledged that the "reasonable expectation of privacy" test has a normative dimension:

For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. In such circumstances, where an individual's subjective expectations had been "conditioned" by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a "legitimate expectation of privacy" existed in such cases, a normative inquiry would be proper (Smith v. Maryland, 442 U.S. 735, 741 n.5 (1979)).

A broader conclusion might be drawn from the preceding statement. Perhaps the "reasonable expectation of privacy" test should measure whether privacy in a particular matter is normatively desirable, as expectations can erode over time as technology advances. On the other hand, under such an approach, who determines what is normatively desirable? Some critics are skeptical as to whether it is appropriate for judges to be making such normative judgments for society.

Other critics have charged that the "reasonable expectation of privacy" test has, in practice, led to a curtailment of Fourth Amendment privacy protection. Many cases applying the test have concluded that there is no reasonable expectation of privacy, and hence no Fourth Amendment protection. Despite much criticism and controversy, the "reasonable expectation of privacy" test remains the central criterion courts use to determine the scope of Fourth Amendment protection.

Next post: Red & Black Publishing Co. v. Board of Regents, 262 GA. 848 (1993)

Previous post: Radio Frequency Identification (RFID)

- **Related Links**
  - Privacy
    - Tuya (fl. 13th century b.c.e.) To Westcar Papyrus
    - Zone of privacy
    - Wiretapping
    - Women and privacy
    - Workplace privacy
- **:: Search WWH ::**

Search

Google™ Custom Search

Expectation of privacy

Definition
: a belief in the existence of freedom from unwanted esp. governmental intrusion in some thing or place
·compare **zone of privacy**
In order to successfully challenge a search or seizure as a violation of the Fourth Amendment to the U.S. Constitution, a plaintiff must show that he or she had manifested a subjective expectation of privacy in the area of the search or the object seized and that the expectation is one that society is willing to recognize as reasonable or legitimate.

Zone of privacy

Definition
: an area or aspect of life that is held to be protected from intrusion by a specific constitutional guarantee (as of the right to be secure in one's person, house, papers, or effects against unreasonable searches or seizures) or is the object of an expectation of privacy <allowed disclosure of medical records, records which were deemed to fall within a *zone of privacy*, upon a showing of proper government interest *Stenger v. Lehigh Valley Hosp. Ctr.*, 609 A.2d 796 (1992)>
compare **expectation of privacy penumbra**

the Fourth Amendment

and the Reasonable Expectation of Privacy

"The protections of the Fourth Amendment are clear. The right to protection from unlawful searches is an indivisible American value. Two hundred years of court decisions have stood in defense of this fundamental right. The state's interest in crime-fighting should never vitiate the citizens' Bill of Rights." -- John Ashcroft, Chairman of the Senate Commerce Committee on Consumer Affairs, Foreign Commerce and Tourism, 1997.

POLICE LINE - DO NOT CROSS POLICE LINE - DO NOT CROSS POLICE LINE - DO NOT CROSS POLICE LINE - DO NOT CROSS POLICE LINE - DO

Despite their clarity, the Fourth Amendment's protections against "unreasonable searches and seizures" have in fact been drastically weakened since they became the law of the land in 1791. As it stands today, unless there exists a "reasonable" expectation of privacy -- that is, a "reasonable" expectation that what one does or says will not be seen or heard by someone else -- neither local police nor federal law enforcement authorities are required to get a warrant or other court order before they start a surveillance operation.

How does one establish whether, in a given instance, one's expectation of privacy is "reasonable"? The criteria are as follows: 1) general legal principles; 2) the vantage point from which the surveillance is carried out; 3) the degree of privacy afforded by certain buildings and/or places; and 4) the sophistication and invasiveness of the surveillance technology employed.

1. General legal principles. The expectation of privacy is *not* reasonable if the behaviors or communications in question were knowingly exposed to public view. Neither the simple desire for privacy, nor the fact that one took steps to obtain it, entitles one to reasonably expect it. For example, even if one set up roadblocks, hung "no trespassing" signs and moved one's house back into the woods, one might still be surveilled from the air without one's Fourth Amendment rights being violated. And yet, as the court stated in *People v. Camacho* (2000) 23 Cal.4 th 824, 835, "we cannot accept the proposition that [the] defendant forfeited the expectation his property would remain private simply because he did not erect an impregnable barrier to access."

2. Vantage point. The expectation of privacy is *not* reasonable if there exists a vantage point from which *anyone,* not just a police officer, can see or hear what was going on and if this vantage point is or should be known or "reasonably foreseen" by the person being surveilled. If such a vantage point exists *in theory,* the police can actually use another vantage point from which to conduct their

surveillance, because what matters is the expectation of privacy, which becomes "unreasonable" if *any* vantage point exists (!). But the police cannot use a vantage point if they have no legal right to take or occupy it. The police cannot commit trespassing; they haven't if they have taken up a vantage point along a normal access route, an "open field," or a common area.

3. Certain buildings and/or pieces of land. The expectation of privacy is *not* reasonable at such public places as automobile thoroughfares (*United States v. Knotts* [1983] 460 US 276, 281), and national forests (*United States v. McIver* [9 th Cir. 1999] 186 F.3d 1119, 1125, but *is* reasonable at public phone booths (*Katz v. the United States,* 389 U.S. 347 [1967]), rock concerts (*Jacobsen v. Seattle,* 658 P. 2d 653 [Wash. 1983]), and sports arenas (*Collier v. Miller,* 414 F. Supp. 1357 [S.D. Tex. 1976]).

4. Technological sophistication. It's easy to forget that, at the time the Fourth Amendment was written and adopted, the photographic camera had not yet been invented; it wasn't until 1826 that Daguerre patented the first photographic process. Because of the rapid development and increasing technological sophistication of televisual surveillance -- first, photography, then, close-circuit televison, and, finally, digital imagery -- "Judicial implementations of the Fourth Amendment need constant accommodation to the ever-intensifying technology of surveillance" (*Dean v. Superior Court* [1973] 35 Cal.App.3d 112, 116); "the Fourth Amendment must likewise grow in response" (*United States v. Kim* [1976] 415 F. Supp. 1252, 1257). This is especially true when it comes to "acquisition technology," that is, devices that, in effect, create vantage points that weren't previously there: audio bugs, wiretaps, and "video bugs" (covert wireless cameras), the use of which requires that the police must get warrants or other court orders.

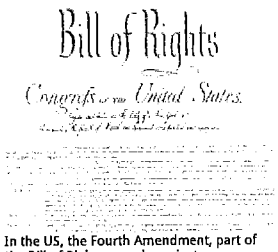
Contact the New York Surveillance Camera Players

By e-mail SCP@notbored.org

By snail mail: SCP c/o NOT BORED! POB 1115, Stuyvesant Station, New York City 10009-9998

NOT BORED!

What Is the Expectation of Privacy?



In the US, the Fourth Amendment, part of the Bill of Rights, guards against unreasonable searches and seizures.

The expectation of privacy is a right codified in United States constitutional law and often applies to search and seizure cases. Citizens have a right to protection against unreasonable searches and seizures of their homes and personal belongings. The government and law enforcement agents acting on a person's behalf do not have the right to intrude on that privacy. To do so would be a violation of the Fourth Amendment as long as there is a reasonable expectation of privacy. The defendant would also only have a constitutional case if the act was carried out by a government agent or other individual acting on behalf of the government.

Some defendants are not successful in asserting a violation of their expectation of privacy if there is a subjective expectation of privacy and not an objective expectation of privacy. For example, in a case where the defendants bagged an illegal drug at an apartment that they had never visited prior, were there for a short time, and had no personal relationship with the tenant, the court found that there was no reasonable expectation of privacy. The defendants' defense that the search by law enforcement of the apartment was illegal was subjective because objective persons in society would not reasonably agree, and the court held that there was no infringement of the defendants' Fourth Amendment rights. Common examples of zones of privacy include one's primary residence; office; or residence of a friend, family member, or anyone who invites you as a guest.

Citizens also have an expectation of privacy as it relates to items they own or pertain to them. The government cannot illegally seize items without violating those individuals' Fourth Amendment rights under the constitution. For example, law enforcement cannot obtain medical records of suspects if the seizure is unreasonable. Seizure of property is subject to the expectation of privacy protection, and that includes seizure of the person. Seizure of the person occurs when the police or other law enforcement uses force to restrain the defendant.

Private parties cannot be sued for search and seizure violations under the Fourth Amendment. For example, there have been cases in which landlords have set up hidden cameras to monitor tenants in an apartment. Those tenants are not often able to raise claims of violation under the Fourth Amendment, because those landlords are not law enforcement or government agents. Defendants will often have to raise other legal defenses under civil laws and criminal laws.

Article Details

- Written By: Daphne Mallory
- Edited By: Melissa Wiley
- Image By: Tex Hex
- Last Modified Date: 06 July 2014
-
- Print this Article

Reasonable expectation of privacy

Contents

Overview

Under current law, to establish a **reasonable expectation of privacy** a person must establish two things: that the individual had a subjective expectation of privacy; and that that subjective expectation of privacy is one that society is prepared to recognize as reasonable.[1] If either element is missing, no protected interest is established.

To support this privacy analysis, the Supreme Court has created a hierarchy of privacy interests:

First, expectations of privacy that "society is 'prepared to recognize as legitimate' have, at least in theory, the greatest protection.[2]
Second, diminished expectations of privacy are more easily invaded.[3]
Third, subjective expectations of privacy that society is not prepared to recognize as legitimate have no protection.[4]

No bright line rule indicates whether an expectation of privacy is constitutionally reasonable.[5] For example, the Supreme Court has held that a person has a reasonable expectation of privacy in property located inside a person's home,[6] in conversations taking place in an enclosed phone booth,[7] and in the contents of opaque containers.[8] In contrast, a person does not have a reasonable expectation of privacy in activities conducted in open fields,[9] in garbage deposited at the outskirts of real property,[10] or in a stranger's house that the person has entered without the owner's consent in order to commit a theft.[11]

"Reasonable expectations of privacy arise from 'a source outside of the 4th Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.'"[12]

Impact of technology on the expectation of privacy

Electronic surveillance is dramatically shrinking the locations and activities in which one has a recognized expectation of privacy. Techniques that derive information from an individual's body fluids, body structure, mental habits, voice timbre, eye motions, temperature change, and scores of other non-controllable attributes generate knowledge about past behavior, allow monitoring and measurement of present activities, and may make possible predictions about future performance. We can electronically monitor criminals, or persons awaiting trial, in their homes. We can call up information about one person from a multitude of government or commercial databases, compare and integrate it and, in effect, reveal new information about that person without their knowledge.

While information has immense benefits and capabilities to improve our lives both individually and as a Nation, it also has dangers. Information about a person is potentially a means of influencing and controlling that person. Information challenges traditional sources of authority and institutions built on that authority. Experience, training, and education may be rendered useless by new information. Information can also erode responsibility: what was once considered a sin to be condemned or a crime to be punished may, with fuller knowledge, appear to some as an illness to be treated or a genetic defect to be repaired. This perception can lead to imposingly difficult questions about the limits on social engineering in the context of constitutional values of personal freedom and privacy.

It is for these reasons that information, and the electronic, chemical, biological, and social technologies that generate and give access to it, often affect constitutional relationships that we are accustomed to think of as political, economic, or legal in nature. constitutional relationships deal with power, with limitations on power, and with the balance between them. Directly or indirectly, information often generates that power, informs its limitations, or affects their proper balance.

Online communications

Computer users lack a legitimate expectation of privacy in information regarding the to/from addresses for e-mails, the IP addresses of websites visited, the total traffic volume of the user, and other addressing and routing information conveyed for the purpose of transmitting Internet communications to or from a user.[13] E-mail addresses and IP addresses provide addressing and routing information to an Internet service provider (ISP) in the same manner as a telephone number provides switching information to a telephone company.[14] Just as a telephone user has no objectively reasonable expectation of privacy in telephone numbers voluntarily turned over to the phone company to enable switching of a phone call, an Internet user has no such expectation of privacy in routing information submitted to an ISP in order to deliver an Internet communication.[15] That routing information also is akin to the addressing information written on the outside of a first-class letter, which also is not constitutionally protected.[16]

With respect to information regarding the total volume of data received and transmitted by an Internet user, that information is no different from the information produced by a pen register regarding the number of incoming and outgoing calls at a particular phone number; and the Supreme Court has long held that an individual has no legitimate expectation of privacy in such information, which already has been exposed to a telecommunications carrier for the purpose of routing a communication.[17]

With respect to the content of an Internet communication (such as an e-mail), a computer user generally has a legitimate expectation of privacy in that content while it is in transmission over the Internet. To date, the federal courts appear to agree that the sender of an e-mail, like the sender of a letter via first-class mail, has an objectively reasonable expectation of privacy in the content of a message while it is in transmission.[18] In *United States v. Maxwell,*[19] the court addressed e-mail privacy:

> "E-mail transmissions are not unlike other forms of modern communication. We can draw parallels from these other mediums. For example, if a sender of first-class mail seals an envelope and addresses it to another person, the sender can reasonably expect the contents to remain private and free from the eyes of the police absent a search warrant founded upon probable cause. However, once the letter is received and opened, the destiny of the letter then lies in the control of the recipient of the letter, not the sender, absent some legal privilege.[20]"

> "Drawing from these parallels, we can say that the transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant. However, once the transmissions are received by another person, the transmitter no longer controls its destiny. In a sense, e-mail is like a letter. It is sent and lies sealed in the computer until the recipient opens his or her computer and retrieves the transmission. The

sender enjoys a reasonable expectation that the initial transmission will not be intercepted by the police. The fact that an unauthorized "hacker" might intercept an e-mail message does not diminish the legitimate expectation of privacy in any way.[21]

> Expectations of privacy in e-mail transmissions depend in large part on the type of e-mail involved and the intended recipient. Messages sent to the public at large in the "chat room" or e-mail that is "forwarded" from correspondent to correspondent lose any semblance of privacy. Once these transmissions are sent out to more and more subscribers, the subsequent expectation of privacy incrementally diminishes. This loss of an expectation of privacy, however, only goes to these specific pieces of mail for which privacy interests were lessened and ultimately abandoned.[22]

Federal courts agree that, again like the sender of a first-class letter, an individual has a "diminished" expectation of privacy in the content of an e-mail that "ha[s] already arrived at the recipient."[23]

Government employees

The U.S. Supreme Court has rejected the contention that public employees "can never have a reasonable expectation of privacy in their place of work."[24] "Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer."[25] Nevertheless, there are reasons to doubt that a government employee has a legitimate expectation of privacy in the content of his Internet communications made using government-owned information systems.

Although an individual generally possesses a legitimate expectation of privacy in his own personal computer,[26] it is less clear that a government employee has a legitimate expectation of privacy in Internet communications he makes using a computer that is the property of the U.S. Government, provided by the taxpayers for his use at work.[27] A government employee lacks an ownership or other property interest in the computer he uses at work; and he especially lacks any such interests in the network infrastructure that the Government provides to enable its employees to access the Internet, which, unlike his personal computer, ordinarily is not within his day-to-day control.

As a general matter, however, the Supreme Court has held that there may be circumstances in which a government employee has a legitimate expectation of privacy in the contents of governmental property that the employee uses or controls at work, such as an office or a locked desk drawer.[28] And the Court also has made it clear that property interests are not conclusive regarding the legitimacy of an individual's expectation of privacy.[29]

Instead, whether, in a particular circumstance, a government employee has a legitimate expectation of privacy in his use of governmental property at work is determined by "[t]he operational realities of the workplace" and "by virtue of actual office practices and procedures, or by legitimate regulation."[30]

Use of log-on banners and computer-user agreements

Although the U.S. Supreme Court has not addressed the issue, the federal courts of appeals have held that the use of log-on banners or computer-user agreements, can eliminate any legitimate expectation of privacy in the content of Internet communications on an employer's computer system. For example, in *United States v. Simons,*[31] the computer-use policy at the Foreign Bureau of Information Services ("FBIS"), a division of the Central Intelligence Agency, expressly noted that FBIS would "audit, inspect, and/or monitor" employees' use of the Internet, "including all file transfers, all websites visited, and all e-mail messages, 'as deemed appropriate.'"[32] The Fourth Circuit held that this policy "placed employees on notice that they could not reasonably expect that their Internet activity would be private" and that, "in light of the Internet policy, Simons lacked a legitimate expectation of privacy" in his use of the Internet at work.[33]

Likewise, in *United States v. Angevine,*[34] the Tenth Circuit held that a professor at a state university had no reasonable expectation of privacy in his Internet use in light of a broadly worded computer-use policy and log-on banner. The computer-use policy stated that the university "reserves the right to view or scan any file or software stored on the computer or passing through the network, and will do so periodically" and has "a right of access to the contents of stored computing information at any time for any purpose which it has a legitimate need to know."[35] The log-on banner provided that "all electronic mail messages . . . contain no right of privacy or confidentiality except where Oklahoma or Federal statutes expressly provide for such status," and that the university may "inspect electronic mail usage by any person at any time without prior notice as deemed necessary to protect business-related concerns . . . to the full extent not expressly prohibited by applicable statutes."[36] The court held that these notices prevent university employees "from reasonably expecting privacy in data downloaded from the Internet onto [u]niversity computers," because users are warned that data "is not confidential either in transit or in storage" and that "network administrators and others were free to view data downloaded from the Internet."[37]

The Eighth Circuit came to the same conclusion in *United States v. Thorn.*[38] Thorn, a state employee had acknowledged in writing a computer-use policy, which warned that employees "do not have any personal privacy rights regarding their use of [the agency's] information systems and technology. An employee's use of [the agency's] information systems and technology indicates that the employee understands and consents to [the agency's] right to inspect and audit all such use as described in this policy."[39] As a result of this policy, the court held that the state employee "did not have any legitimate expectation of privacy with respect to the use and contents of his [work] computer," because under the agency's policy, employees have "no personal right of privacy with respect to their use of the agency's computers" and provides the state with a "right to access all of the agency's computers."[40]

The decisions of other federal courts that have addressed the issue support the proposition that actual and consistent use of log-on banners or computer-user agreements can eliminate any legitimate expectation of privacy of an employee with respect to his Internet communications using a government-owned information systems.[41]

References

1. ↑ *See, e.g.,* Katz v. United States, 389 U.S. 347, 361 (1967) (full-text) (Harlan, J., concurring); California v. Ciraolo, 476 U.S. 207, 214 (1986) (full-text) (stating that "Justice Harlan made it crystal clear that he was resting on the reality that one who enters a telephone booth is entitled to assume that his conversation is not being intercepted"); Smith v. Maryland, 442 U.S. 735, 740 (1979) (full-text) (stating that the *Harlan test* "embraces two discrete questions").
2. ↑ New Jersey v. T.L.O., 469 U.S. 325, 338 (1985) (full-text) (quoting *Hudson v. Palmer,* 468 U.S. 517, 526 (1984)).
3. ↑ *See id.* at 342 n.8 (discussing the individual suspicion requirement when privacy interests are minimal); *accord* Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 624-25 (1989).
4. ↑ *See, e.g.,* Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978); United States v. Caymen, 404 F.3d 1196, 1200-01 (9th Cir. 2005) (no reasonable expectation of privacy in the contents of computers the person has stolen or obtained by fraud).