

## **Your (un)Reasonable Expectations for Privacy**

*While law enforcement adapts to the challenges of the electronic era, expectations of privacy diminish*

**By Eric Salveggio**

As Americans, we have become so immune to the fact that we are awarded an immense amount of privacy that we are shocked, numbed, and even angered when we feel that our privacy rights have been violated. We understand that "over there", in other countries, others don't enjoy the same privileges as we do, but it's not at a cognitive, or even meta-cognitive, level; it's just "there" ... not "here". The issues surrounding the 9-11 tragedy shocked, numbed and angered us because, not only had our safety been threatened, but our perceived sense of privacy, "isolationism" at its finest, was horribly disturbed.

In this paper, we find another method of privacy that many take for granted as being a "right": Internet privacy at work and at home. We take for granted that under the 4th Amendment, we are immune to "illegal search and seizure," because, after all, it's *our* personal "stuff" ... isn't it?

### **The 4th Amendment**

*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.*

"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 helped bolster 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.

## **What It Used to Be**

Since its inception in 1791, the 4th Amendment has slowly taken a beating. Where law officials once had to almost beg for every (legal) wiretap, a citizen's privacy was held to the utmost. A court appointed order had to be in hand before any type of surveillance for legal purposes could be accomplished. The criteria once held to be sacred has slowly eroded into today's loosely held notion that we, the people, still have this same right.

## **What It Is**

In the past 10 years, millions of people have spent countless hours in front of computers, sending e-mail, surfing the 'Net, managing databases, making purchases, and a host of other activities.

Along with all of the normal activity that occurs, the crime world has also entered the fray, using today's technology for less than honest means and purposes.

Due to this, law enforcement has had to understand this new era, how it works, and how best to combat it. Many times, the assumed rights of the citizen have been stripped away in order to deal with this new threat.

## **Criteria for Determining What's "Reasonable"**

A search is constitutional if it does not violate a person's "reasonable" or "legitimate" expectation of privacy. *Katz v. United States*, 389 U.S. 347, 362 (1967) (Harlan, J., concurring.)

The following four criteria are generally used in determining whether or not we can expect our privacy to be rudely invaded:

1. **General Legal Principles:** Unless you live your life as a complete hermit, anything you do or say, knowingly, in a public place, does not constitute an expectation of privacy.
2. **Vantage Point:** As long as the police do not trespass, or try to illegally inhabit or occupy a space, any area that you can be seen from is considered 'fair game' to become a vantage point from which to place you under surveillance.
3. **The Degree of Privacy Awarded by Buildings and Places:** Any place in public, unless you happen to be in a phone booth, attending a sporting event in an enclosed arena, or at your favorite concert, is fair game to have you under surveillance.
4. **Technology:** Here's where a lot of us miss the boat: Because of the rapid growth in technology, a case brought before the Superior Court in 1973 agreed that, "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).

How This Applies To Technology

### **Patriot Act**

The Patriot Act was incorporated into the 2001 edition of "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations". Unless reenacted into law, the present day Patriot Act will die on December 31, 2005. The issue that will cause it to be kept alive is the fact that prosecutors and agents are urged to inform the Computer Crime and Intellectual Property Section (CCIPS) whenever use of these new laws and rulings help in a criminal case.

## **CCIPS**

The CCIPS manual is a plethora of rules and regulations for obtaining evidence, with many sections devoted to electronic search and seizure.

Some of the following areas covered:

- Reasonable Expectation of Privacy in Computers as Storage Devices
- Reasonable Expectation of Privacy and Third-Party Possession
- Private Searches
- Exceptions to the Warrant Requirement in Cases Involving Computers
- Workplace Searches
- Reasonable Expectation of Privacy in the Workplace
- Employer searches in Private-Sector Workplaces
- No-Knock Warrants
- Searching and Seizing computers Without a Warrant
- Sneak and Peek Warrants

## **Who Determines these Rules and Regulations**

As the issues raised by computer crime and investigations raise many new, heretofore unknown issues, the courts are struggling to interpret how a citizen's rights and the 4th Amendment are to be applied.

- The U.S. Attorney's office has at least one person who's been designated as a Computer and Telecommunications Coordinator (CTC). This person receives extensive training in computer-related crime, and is primarily responsible for the crimes found within their own district.
- The Criminal Division of the U.S. Dept. of Justice provides expertise through the Office of International Affairs, the Office of Enforcement Operations, and the Child Exploitation and Obscenity Section.

## **Expectations in our favor?**

Under our present laws, law enforcement agencies can't open a closed container to obtain evidence. The courts have looked at the issues surrounding electronic storage devices, and have ruled that these are akin to opening a closed container. Due to this, we can expect a reasonable level of privacy, as the contents could implicate us in the reasonable expectation of privacy in this information.

## **Matrix**

Anyone who knows how the Internet works, realizes all of the e-commerce information contains a wealth of information on people. All it takes is simply knowing how to get access to it.

Congress killed the Pentagon's "Total Information Awareness" data mining program, but now the Florida police have instituted a State-run equivalent, dubbed the Matrix. In this case, the system is supposed to enable investigators and analyst across the country finds

links and patterns in crimes more effectively and quicker by combining all police records with commercially available collections of personal information about most American habits.

### **What We Can Expect**

According to numerous cases already on the books, we are, indeed, protected, and can expect a reasonable amount of privacy when it comes to computer related issues. However, if any of what we do falls into the previously mentioned four categories, or we openly show, or talk about what we are doing, we forfeit our rights to any expectations of privacy. In *United States v. Gorshkov*, 2001 WL 1024026, at \*2 (W.D. Wash. May 23, 2001, and *Katz v. United States*, 389 U.S. 347, 351 (1967), it was ruled that the defendant did not have a reasonable expectation of privacy in use of a private computer network when undercover federal agents looked over his shoulder, when he did not own the computer he used, and when he knew that the system administrator could monitor his activities.

We also lose these rights whenever we relinquish our control of information to a third party; repair shops, handing out floppy disks or CD-ROMs, or even sending data across the Internet, including e-mail, instant messaging, and any type of Voice over IP (VOIP), which is becoming increasingly popular.

### **Conclusion**

What we can deduce from all this is that ignorance of the law will not preclude you from having your expectations of privacy not "violated".

Having these cases to use as a standard, we find that there really is no such thing as a reasonable expectation of privacy for electronic media. If law enforcement wishes to place us under surveillance, they may do so, as long as they are within the boundaries mentioned. While some people may actually get extremely angry over these facts, the truth is, if you have nothing to hide, then you have nothing to worry about, right?

**References:**

<http://www.notbored.org/privacy.html>

<http://www.cybercrime.gov/s&smanual2002.htm>

<http://www.cybercrime.gov>

United States v. Barth, 26 F. Supp. 2d 929, 936-37 (W.D. Tex. 1998) (finding reasonable expectation of privacy in files stored on hard drive of personal computer); United States v. Reyes, 922 F. Supp. 818, 832-33 (S.D.N.Y. 1996) (finding reasonable expectation of privacy in data stored in a pager); United States v. Lynch, 908 F. Supp. 284, 287 (D.V.I. 1995) (same); United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993) (same); United States v. Blas, 1990 WL 265179, at \*21 (E.D. Wis. Dec. 4, 1990) ("[A]n individual has the same expectation of privacy in a pager, computer, or other electronic data storage and retrieval device as in a closed container.").

United States v. Most, 876 F.2d 191, 197-98 (D.C. Cir. 1989) (finding reasonable expectation of privacy in contents of plastic bag left with grocery store clerk); United States v. Barry, 853 F.2d 1479, 1481-83 (8th Cir. 1988) (finding reasonable expectation of privacy in locked suitcase stored at airport baggage counter); United States v. Presler, 610 F.2d 1206, 1213-14 (4th Cir. 1979) (finding reasonable expectation of privacy in locked briefcases stored with defendant's friend for safekeeping). See also United States v. Barth, 26 F. Supp. 2d 929, 936-37 (W.D. Tex. 1998) (holding that defendant retains a reasonable expectation of privacy in computer files contained in hard drive left with computer technician for limited purpose of repairing computer)

<http://www.washingtonpost.com>

<http://www.aclu.org/privacy/Privacy.cfm?ID=14257&c=130>

*Eric Salveggio is Director of Network Engineering for the Palisades Campus of Virginia College in Birmingham, AL.*

*Source: Ubiquity, Volume 5, Issue 9, April 28 - May 4, 2004, <http://www.acm.org/ubiquity/>*