Email

Messages that are transmitted electronically from the sender's computer to one or more recipients by way of a network.

Users may often view email as private conversations with another person, in which no one else is participating; however, email is one of the least secure methods of communication available. In contrast, phone calls typically aren't recorded and stored. Even if they were, your employer and law enforcement would have to go to court to gain access to them. Emails are stored at several different locations: on the sender's computer, the Internet service provider's (ISP) server, and on the receiver's computer. Deleting an email from an inbox doesn't mean there aren't multiple other copies of it in existence. Emails are also vastly easier for employers and law enforcement to access than phone records. And because of their digital nature, they can be stored for very long periods of time.

Email privacy concerns include issues of unauthorized access of electronic mail. Unauthorized access of an individual's email may occur while an email is in transit, when it is stored on email servers, or when it is stored on a user's computer.

In the United States, Americans have a constitutional guarantee of the secrecy of correspondence. It is a matter of considerable debate as to whether email should receive the same kind of legal protection as paper letters sent through the postal service and under what circumstances. The very nature of email influences whether it should receive legal protection from any and all types of eavesdropping. These issues are increasing in importance as email continues to be such a popular means of communication.

Certain technological processes help curtail the unauthorized access to email. Because email messages are often transmitted through different nations that may have wide array of different regulations and restrictions pertaining to the access of other people's email, the user should be aware of the laws, practices, and realities of the countries through which their email is transmitted.

Email at the workplace

The general rule is that employees have no reasonable expectation of privacy when using email at their workplace. If an employer is using email at work, the employer is legally entitled to monitor it. Employers, unlike law enforcement, largely have an unfettered right to search through the email of their employees. Employers typically believe that sending email through their equipment could affect their business, which justifies searching and monitoring employee email.

Many employers require their employees to sign and acknowledge an employer computer and email use policy. This document may explicitly state that email may be used for work purposes, the computer system is the employer's property, email may be monitored, and the employee has no reasonable expectation of privacy in email use. Once signed by an employee, this policy gives the employer a contractual right that it can rely on if it wants to monitor an employee. Also, if a dispute arises over monitoring of email, the employer can point to the signed statement to show that it was unreasonable for the employee to think that email was private.

Even if a written policy does not exist, the employer may still monitor its employees' email. Courts have rarely found that the employee had a reasonable expectation of privacy to his or her email at work for several reasons. Some courts have held that email at the workplace is part of the work environment, similar to a fax or copy machine, in which the employee doesn't have a reasonable expectation of privacy. Other courts have found that emailing to colleagues at work was inherently work-related, and thus there could be no reasonable expectation of privacy.

Employers are concerned about misuse of email, including the fact that employees should be supposed to be working. Employers' monitoring of work email is a way to ensure that employees are using email appropriately.

Many employers are concerned about liability. If the employer is ever a party in a lawsuit, the opposing litigants may be entitled to review employee email. Employers are also concerned about workplace harassment claims. One way that employers protect themselves against lawsuits is to monitor email and prevent or deter computer-related harassment at the workplace. Many employers have software on their networks that seek emails that might be problematic.

The other main concern with liability is that old emails could be used years down the road in a lawsuit. What an employee says can be preserved for years, and unless the company has an established, reasonable practice of purging its emails, those emails can be a gold mine for anyone suing the company. Emails can be especially devastating because of the informal way that people write and send them, saying things in emails that they never would in professional correspondence.

Most public-sector employees have even less privacy rights in their email than most private-sector employees. Under different public records statutes and the Freedom of Information Act (FOIA), the public may gain access to much of the communications of a public employee. Also, because of the nature of public employees' jobs, courts are reluctant to hold that government employees have a reasonable right to privacy in workplace email.

Email from home and personal accounts

Unlike work emails, personal email from one's personal email account and computer is more likely to be protected because there is a much more reasonable expectation of privacy. But even personal emails may not be fully protected. Anonymous hackers may be intercept private accounts.

Because emails are stored locally, at the ISP, and on the receiving end, hackers or law enforcement can gain access to them at multiple points. While it may be difficult for law enforcement to gain legal access to one's personal computer and local copies of saved emails in one's personal computer, they may be able to get them easily from the ISP. Law enforcement officials with a warrant are permitted to seize electronic correspondence of those suspected of a crime. Under some circumstances, ISPs are legally able to scrutinize the email of individuals.

ISPs are also increasingly imposing end-user service agreements that users must agree to. These agreements reduce any expectation of privacy. They also often include terms that grant the ISP the right to monitor the network traffic or give records at the request of a government agency. For example, the service agreement for one popular ISP states: "Service Provider has no obligation to monitor the Service, but may do so and disclose the information regarding the use of the Service for any reason if Service Provider in its sole discretion believes that it is reasonable to do so, including to satisfy governmental or legal requests."

While sending personal email only from home greatly protects your privacy more than using email at work, the individual's email is vulnerable to interception by hackers. After the email leaves the sender's home, it goes over several online services and open networks before it reaches the recipient.

Legal protections for email privacy

Email privacy is derived from the Fourth Amendment to the U.S. Constitution and is governed by the "reasonable expectation of privacy" standard. Considering the open nature of email, the expectation of privacy may be less for email, especially work email, than for other forms of communication.

The Fourth Amendment provides that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." The Fourth Amendment is often envied to protect privacy rights against government activities.

The courts have found varying degrees of Fourth Amendment protections of email. In *O'Connor v. Ortega*, 480 U.S. 709 (1987), the administration at Napa State Hospital, after placing Dr. Magno Ortega on administrative leave during an investigation into possible misconduct, searched Ortega's office. Dr. Ortega sued the hospital, claiming that the search violated his Fourth Amendment rights. Both the federal district court and the circuit court found that the search did violate Ortega's Fourth Amendment rights. The U.S. Supreme Court disagreed. The Court based its decision on two factors: (1) whether Dr. Ortega had a reasonable expectation of privacy and (2) whether the search of Dr. Ortega's office was reasonable. The Court held that because Dr. Ortega had a private office, he had a reasonable expectation of privacy. However, the Court also found the search of his office was reasonable because it was work-related. The government's need to ensure efficient operation of the workplace, therefore, outweighs an employee's expectation of privacy, even if the privacy expectation is reasonable. Because work environments vary, a public-sector employee's expectation of privacy must be determined on a case-by-case basis. The court considered factors such as: (1) notice to employees, (2) exclusive possession by an employee of keys to a desk or file cabinet, (3) the government's need for access to documents, and (4) the government's need to protect records and property.

After the *Ortega* decision, the extent of constitutional protection afforded to emails is unclear. Unlike a locked desk or file cabinet, emails are not locked. The employer has access to all messages on the system.

In addition to Fourth Amendment protection of email privacy, federal statutory law provides additional protection. Interception of email transmission, capturing the email while it is sent from sender to recipient, is a criminal violation under the Electronic Communications Protection Act (ECPA), 100 Stat. 1848 (1986), codified as 18 U.S.C.A 2517(4). Although ECPA originally set up protections (such as a warrant requirement) to protect email, those protections have been weakened in many instances by the PATRIOT Act, 115 Stat. 272 (2001). ECPA also permits an ISP to search through all stored messages. Some ISPs temporarily store all messages that go through the system. In most cases, ECPA generally prevents the ISP from disclosing the messages to others. Law enforcement officials, with warrants or administrative subpoenas, may collect information about users from ISPs and also obtain access to the content of stored messages. Also, ECPA does not protect against hackers intercepting the message at the recipient's mailbox.

Email covered by ECPA loses its status as a protected communication in 180 days, meaning that a warrant is no longer necessary and the emails of individuals may be accessed by a simple subpoena instead of a warrant to order to access email from a provider. If the emails are stored on a user's personal computer instead of a server, those emails would still require the police to obtain a warrant first to seize the contents. This part of ECPA been criticized as obsolete. At the time ECPA became law, infinite storage at webmail servers was not available. In 2013, some members of Congress first proposed reforming the law.

The Email Privacy Act, HR 1852, 113th Cong. (2013), HR 699, 114th Cong. (2015), would amend ECPA to prohibit a provider of remote computing services or electronic communication services to the public from knowingly divulging to any governmental entity the contents of any communications that are in electronic storage or otherwise maintained by the provider. The Email Privacy Act also would have provisions under which the government may require, pursuant to a warrant, the disclosure by such a provider of the contents of such communications. It eliminates the different requirements depending on whether such communications were stored for fewer than, or more than, 180 days. It also requires a law enforcement agency, within ten days after receiving the contents of a customer's

communication, or a governmental entity, within three days, to provide the customer with a copy of the warrant and a notice that such information was requested by, and given to, the law enforcement agency or government entity.

State constitutional protection of emails

State constitutions in at least ten states (Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington) recognize the individual's right to privacy. Some of these state privacy protections reflect Fourth Amendment protections. The state constitutions, however, have more references to privacy. Courts have interpreted general constitutional provisions in other states without specific privacy provisions to have established privacy rights of various types. Similar to the rights granted by the U.S. Constitution, the privacy rights under state constitutions usually extend to protection from state government actions and do not cover the actions of private entities.

However, an important exception to these laws exists: provider exception. Under the provider exception, these laws do not apply to "the person or entity providing a wire or electronic communications service." This exception, for example, allows various free email providers (Gmail, Yahoo Mail, etc.) to process user emails to display contextual advertising.

Email sent by employees through their employer's equipment has no expectation of privacy; the employer may monitor all communications through its equipment. According to a 2005 survey by the American Management Association, about 55 percent of U.S. employers monitor and read their employees' email. Even attorney-client privilege is not guaranteed through an employer's email system; U.S. courts have rendered contradictory verdicts on this issue. Generally speaking, the factors that courts use to determine whether companies can monitor and read personal emails in the workplace include: (1) the use of a company email account versus a personal email account and (2) the presence of a clear company policy notifying employees that they should have no expectation of privacy when sending or reading emails at work, using company equipment, or accessing personal accounts at work or on work equipment.

Common law protection of email

Various parties have asserted email privacy protection under privacy common law arguments in various state court cases. Thus, state law governing email privacy has been evolving. Under the common law, email privacy is protected under the tort of invasion of privacy and the causes of action related to this tort. Four distinct torts protect the right of privacy: (1) unreasonable intrusion upon the seclusion of another, (2) misappropriation of another's name and likeliness, (3) unreasonable publicity given to another's private life, and (4) publicity that unreasonably places another in a false light before the public. Of these, the tort of "unreasonable intrusion upon the seclusion of another" is the most relevant to the protection email privacy.

Global surveillance

The documents leaked by ex-NSA contractor Edward Snowden indicated that many governments have programs for monitoring and intercepting communication, including email, on a massive scale. The legality, ethics, and propriety of these programs continue to be debated As part of this mass surveillance, the email of many innocent individuals with no terrorist connections have been intercepted and stored. Whistleblower and former National Security Agency (NSA) employee William Binney claimed that NSA has intercepted over 20 trillion communications, including many email communications, representing one aspect of NSA's warrantless surveillance efforts.

The American Civil Liberties Union (ACLU) and other privacy and civil liberties organizations have alleged that Verizon illegally granted the U.S. government unrestricted access to its entire Internet traffic without a warrant and

that AT&T had a similar agreement with NSA. While the Federal Bureau of Investigation (FBI) and NSA claim that all their activities were and are legally sanctioned, Congress passed the FISA Amendments Act of 2008 (FAA), granting AT&T and Verizon immunity from prosecution.

Maintaining email privacy

Unless the user takes affirmative steps to encrypt messages (a process by which sophisticated software uses cryptographic algorithms to garble the words in a message and then allows the recipient to unscramble and read the message, provided that the recipient has the correct digital key to reconstitute it), email cannot be regarded as a confidential method of transmitting information. Thus, encryption is the only way to ensure a high degree of privacy for email messages.

Commonly used public key technology has two keys: one that is unique and private, and one that is public and freely distributed to all users of a particular system. These keys work only when they are matched: What one scrambles, only the other can undo. These techniques can also verify the integrity of the data (that it wasn't altered) and authenticate it (ensure that the stated creator is the person who sent the message).

Gretchen Nobahar

Further Reading

Gelman, Robert B., and Stanton McCandlish. *Protecting Yourself Online: The Definitive Resource on Safety, Freedom, and Privacy in Cyberspace*. New York: HarperEdge, 1998.

Kent, Stephen T. *Who Goes There? Authentication through the Lens of Privacy*. Washington, DC: National Academies Press, 2003.

Levmore, Saul. *The Offensive Internet: Speech, Privacy, and Reputation*. Cambridge, MA: Harvard University Press, 2010.

Macdonald, Lynda A. C. *Tolley's Managing Email and Internet Use*. Croydon: LexisNexis UK, 2004.

Merkow, Mark S., and Jim Breithaupt. *The E-Privacy Imperative: Protect Your Customers' Internet Privacy and Ensure Your Company's Survival in the Electronic Age*. New York: AMACOM, 2002.

Mills, Jon L. Privacy: The Lost Right. Oxford Scholarship Online, 2008.

Sin, Yvonne Pui Man. *Email Privacy: Legal and Ethical Implication of Workplace Surveillance and Monitoring*. Auckland, New Zealand: Department of Management Science and Information Systems, University of Auckland, 2002.

Wugmeister, Miriam. *Global Employee Privacy and Data Security Law*. Arlington, VA: BNA Books, 2009.

See also: Computers and privacy; Constitutional Law; Electronic Communications Privacy Act (ECPA); Fourth Amendment of the U.S. Constitution; Home, Privacy of the; Law enforcement; USA PATRIOT Act; Workplace, privacy in the.

Employment eligibility verification systems

Systems intended to ensure that individuals holding jobs are authorized to work in the United States. U.S. law requires that companies employ only individuals who may legally work in the United States: U.S. citizens, or foreign citizens who have the necessary authorization. The diverse U.S. workforce contributes greatly to the vibrancy and strength of the U.S. economy, but that same strength also attracts unauthorized employment.

E-Verify is an Internet-based system that allows businesses to determine the eligibility of their employees to work in the United States. E-Verify is easy to use and is one of the best ways employers can ensure a legal workforce.

The E-Verify program allows employers to confirm the immigration status of new hires by checking their identity data against government databases. While not without controversy, E-Verify is widely accepted as a useful immigration enforcement tool, making companies accountable for employing only those who are authorized to work in the United States.

After several years of debate about unauthorized immigration to the United States, Congress enacted the Immigration Reform and Control Act (IRCA) of 1986. In 1986, there were an estimated 3.2 million unauthorized immigrants (illegal aliens) in the United States. IRCA com-