



Privacy

Background

Technology plays an enormous role in making the term “privacy” meaningful. Prior to the last century, invasion of privacy was limited by the physical abilities to see, hear, and remember events. As each new technology made the recording of events easier, privacy came under increasing threat. The camera, the telephone, the microphone, the tape recorder, the television, the computer, and most recently the Internet have all extended our abilities to communicate and made it more difficult to remain private. Yet, privacy was not defined as a “right” by the Supreme Court of the United States until 1965.¹

Traditionally, Congress has chosen not to pass any broad privacy laws, but to limit the government’s power and target specific issues as they arise. As a result, we have a “quilt” of laws and regulations such as the Fair Credit Reporting Act, the Family Education Rights and Privacy Act (FERPA), the Cable Communications Policy Act, and most recently the Children’s Online Privacy Protection Act (COPA). However, what *has* developed is a standard. The Code of Fair Information Practices was originally developed in 1973 by the Department of Health, Education, and Welfare to limit the government’s access to private information. It has evolved into the standard which both the government and private sectors use to measure privacy policy, and is comparable to international guidelines developed by the Organization for Economic Cooperation and Development (OECD). This last fact has increased in importance with the transnational nature of the Internet. The code states:

- There shall be no personal data record-keeping systems whose very existence is a secret.
- Means must be provided for a person to find out what information about himself or herself is in a record and how it is used.
- Means must be provided for a person to prevent information about himself or herself that was obtained for one purpose from being used or made available for other purposes without his or her consent. (Also referred to as third-party transfer.)
- There must be a way for a person to correct or amend a record of identifiable information about himself or herself.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must ensure the reliability of the data for its intended use and must take precautions to prevent misuses of the data.²

Privacy legislation promises to play a prominent role as the nation wrestles with the balance of homeland security and individual privacy, as well as the ongoing issue of identity theft. Increased concern for national security has emboldened the federal government to revisit laws that can negatively impact individual’s privacy. The tension between the need for security and the need for privacy is increasing.

While no new privacy-specific laws have been passed recently, proposed legislation still spur heated debate and serve as a necessary counterbalance to the immense pressure that improve security after the events of September 11.

Significance for EDUCAUSE Members

Privacy laws currently on the books, such as the Family Education Rights and Privacy Act (FERPA) passed in 1974 and the Health Insurance Portability and Accountability Act (HIPAA) passed in 1996, have had significant impact on information system management in higher education. Any new privacy laws,

including those impacting federal agencies, may ultimately impact higher education institutions receiving federal grants. The Federal Trade Commission (FTC) is reviewing financial privacy notice guidelines under the Gramm-Leach-Bliley Act to see what changes should be made to improve consumer understanding. Compliance with provisions under the USA PATRIOT Act and the proposed extension of Communications Assistance for Law Enforcement Act (CALEA) to Internet services can be costly, time-consuming, and confusing as they conflict with standard privacy policy.

Current EDUCAUSE Position

EDUCAUSE supports the general intent to improve the security of our networks and systems but in a way that has the least effect on our way of life. Generally, this means ensuring the data protections that are already allowed by law. Systems should be monitored only as necessary for their proper maintenance and only for activity levels, never for content. In this way, information can be made available to law enforcement through the proper legal channels, similar to phone records. EDUCAUSE opposes extending CALEA to apply to Internet service providers.

Leading the Privacy Effort at the Federal Level

The FTC is the regulatory agency that deals with privacy violations under its authority to prohibit “unfair or deceptive acts or practices in or affecting commerce.”³ They have several enforcement options available to them including cease and desist orders, injunctions, and significant financial penalties. In the case of FERPA, all federal funding can be withheld if a school is found out of compliance. The Federal Communications Commission (FCC) will decide on the petition by law enforcement to extend CALEA to Internet service providers. Ordinarily, privacy issues are introduced into the Congressional process as proposed legislation and assigned to the respective commerce or judiciary committees of the House and Senate. Once they become law they are assigned to either the FTC or the FCC to regulate and enforce.

Resources

Federal Trade Commission: Privacy Initiatives, <<http://www.ftc.gov/privacy/index.html>>.

Federal Communications Commission: CALEA, <<http://www.fcc.gov/calea/>>.

AskCALEA, <<http://www.askcalea.net>>.

EDUCAUSE Resources Center, <<http://www.educause.edu/Browse/647>>.

Protecting America’s Freedom in the Information Age: A Report of the Markle Foundation Task Force (New York: Markle Foundation, October 2002), <http://www.markle.org/downloadable_assets/nstf_full.pdf>.

Markle Foundation: Rules Governing Access to Private Sector Data, <<http://www.markletaskforce.org/privacyrules.html>>.

Endnotes

1. *Griswold v. Connecticut*.
2. United States Department of Health, Education, and Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary’s Advisory Committee on Automated Personal Data Systems* (Washington, D.C.: U.S. Government Printing Office, 1973).
3. Simon Lazarus and Brett Kappel, “Protecting Privacy from Prying Eyes,” *Legal Times*, May 1998, p. 14.