

Toward a U.S. Data-Retention Standard for ISPs

Concerns regarding online child exploitation may lead to a U.S. data-retention standard for Internet Service Providers (ISPs), including colleges and universities. A June 2006 letter written to congressional leaders and signed by the attorneys general from forty-nine states pleads for “Congress to dedicate the resources necessary to study this issue and to implement a meaningful national standard for ISP data retention that provides law enforcement with the tools necessary to combat the spread of internet-based crimes against children.”¹ In addition, the topic has been the focus of several congressional hearings and also of private meetings that the Department of Justice and the FBI held with representatives of commercial ISPs.

The context of the current debate has been sensationalized by stories of how law enforcement’s efforts to catch Internet predators have been thwarted because ISPs have deleted information critical to determining a suspect’s name and physical location. According to statistics provided by the National Center for Missing & Exploited Children, one in seven children is solicited for sex online.² Consequently, it is difficult for ISPs to resist data-retention requirements on the grounds that this is an undesirable, unfunded federal mandate. The government, however, has sent mixed messages regarding its intentions. U.S. Attorney General Alberto Gonzales has insisted that he is interested in the topic as a means of protecting children—a priority of the Bush administration. FBI Director Robert Mueller, in a meeting with the CEOs of ISPs in May 2006, indicated that

mandatory data retention would also be useful in the fight against terrorism.

Issues of data retention are not new for institutions of higher education. Public colleges and universities are often mandated to retain certain records to comply with state public records laws or Freedom of Information Act requests. Increasingly, these records include electronic documents and e-mail messages that pertain to official business. Institutions typically establish retention schedules both to comply with legal requirements and to satisfy internal business needs. At the same time, security concerns and the need to protect information systems and networks from attacks have resulted in increased monitoring and logging by IT departments.

Institutional policy discussions often translate into the need for “data destruction” practices to protect privacy and to avoid undue costs or eliminate the unnecessary burdens associated with information retrieval. Data destruction, however, is quickly falling out of favor, at least with respect to the ability to track Internet behavior that may help the government identify child exploiters or terrorists. But as more and more information about Internet activity is captured and stored, it also becomes a desirable source of information for third parties, including litigants in civil proceedings and law enforcement.

The scope of data to be retained is uncertain. Rep. Diana DeGette (D-Colo.), a House Energy and Commerce Committee member who has championed efforts to make data retention mandatory, maintains that she seeks to require ISPs to retain IP address information only so

that computers or communications related to child exploitation can be traced to a source. She insists that she is not expecting that ISPs will retain the *content* of communications. Concerns regarding the potential scope of data retention are also fueled by the recent passage of the European Union (EU) Data Directive, which will require “the providers of publicly available electronic communications services or of public communications networks” to retain data necessary to “trace and identify the source of a communication”; “identify the destination of a communication”; “identify the date, time and duration of a communication”; “identify the type of communication”; “identify users’ communication equipment or what purports to be their equipment”; and “identify the location of mobile communication equipment.”³

The appropriate duration of data retention is also under discussion. The EU directive requires member states to ensure that the data is retained for “not less than six months and not more than two years from the date of the communication.”⁴ During congressional hearings, Rep. DeGette has stated that she is developing legislation that would require retention of IP address information for one year. From congressional hearing testimony, it is evident that the current practice of commercial ISPs results in data-retention practices that range from a few days to several years, a situation that is also typical of higher education institutions. As of September 1, 2006, Comcast implemented a 180-day retention policy for IP address-assignment data. Previously, the retention period was 31 days—what Comcast deemed to be

the absolute minimum amount of time necessary for network management.⁵

It is also not clear if U.S. law will follow the European approach and limit data-retention requirements to public communication providers. That distinction may be a helpful approach for colleges and universities if it results in an exemption similar to the treatment of “private networks” under the Communications Assistance for Law Enforcement Act (CALEA). Although commercial ISPs are apparently the initial targets for data-retention requirements, it is difficult to imagine a system that will not eventually need to be extended to other entities that provide access to the Internet, entities such as the government, businesses,



and nonprofit organizations including colleges and universities.

The Center for Democracy & Technology (CDT) has outlined a number of reasons why mandatory data retention is “invasive, risky, unnecessary, [and] ineffective.” The CDT lists the following nine concerns:

1. Data retention laws threaten personal privacy and pose a security risk, at the very time the public is justifiably concerned about security and privacy online. . . .
2. Data retention laws create the danger of mission creep. . . .
3. Data retention laws are unnecessary—authority already exists to preserve records. . . .
4. The Internet and telecommunications industry is committed to cooperating with law enforcement, but the DOJ

and other law enforcement agencies have not effectively used the authority already at their disposal. . . .

5. Proceeding with data retention would require a full-scale re-examination of data privacy laws. . . .
6. A data retention database would principally serve as a honeypot for trial lawyers in civil cases. . . .
7. Data retention laws are not likely to be effective. . . .
8. Data retention laws undermine public trust in the Internet. . . .
9. Data retention laws are burdensome and costly.⁶

The United States Internet Service Provider Association (US ISPA) identifies

data preservation “as the preferred mechanism to minimize the risk of deletion of records and communications that may be necessary during an investigation of a crime.” Current law, as contained in Title 18 U.S.C. Section 2703(f), outlines the process by which law enforcement can contact

ISPs to request the preservation of identified records or communications related to a particular person. The information cannot be deleted for 90 days, during which time law enforcement obtains the proper legal process.⁷ US ISPA supports fine-tuning the existing data-preservation regime and opposes a more cumbersome—and perhaps unnecessary—data-retention regime. As evidence of their commitment, the online companies AOL, Yahoo!, Microsoft, EarthLink, and United Online in June 2006 announced that they would join the National Center for Missing & Exploited Children to fund a new Technology Coalition “to develop and deploy technology solutions that disrupt the ability of predators to use the Internet to exploit children or traffic in child pornography.”⁸

The details surrounding data retention are controversial and complex. The

hype associated with the legitimate need to protect children from online exploitation creates a difficult political context for robust debate. Institutions of higher education will also be conflicted because security concerns and internal business needs are causing colleges and universities to capture and store greater amounts of information about their constituencies. The ability to use this growing amount of information for monitoring and surveillance—the “policing of the Internet” by an institution for internal administrative purposes as well as by external authorities—also threatens the value that the educational community places on privacy, autonomy, and individual freedom. In any case, the temptation to use computers and networks as a means to trace communications and hold individuals accountable for misbehavior is certain to be the subject of ongoing, intense policy debates.

Notes

1. See <http://www.ago.state.co.us/press_releases/drletterfinal.pdf>.
2. Janis Wolak, Kimberly Mitchell, and David Finkelhor, *Online Victimization of Youth: Five Years Later* (Alexandria, Va.: National Center for Missing & Exploited Children, 2006), p. 1, <http://www.missingkids.com/en_US/publications/NC167.pdf>.
3. European Union Directive 2006/24/EC on the “retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks,” <<http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2006/L105/L10520060413en0540063.pdf>>.
4. Ibid.
5. Testimony of Gerard J. Lewis Jr. before the Subcommittee on Oversight and Investigations of the House Committee on Energy and Commerce, *Making the Internet Safe for Kids: The Role of ISPs and Social Networking Sites*, June 27, 2006, <<http://energycommerce.house.gov/108/Hearings/06272006hearing1954/hearing.htm>>.
6. “Mandatory Data Retention: Invasive, Risky, Unnecessary, Ineffective,” memo from CDT’s Nancy Libin, staff counsel, and Jim Dempsey, policy director, to “Interested Persons,” June 2, 2006, <<http://www.cdt.org/privacy/20060602retention.pdf>>.
7. United States Internet Service Provider Association, “The US Data Preservation System: Title 18 U.S.C. Section 2703(f),” <[http://www.usispa.org/pdf/Data PreservationSystem.pdf](http://www.usispa.org/pdf/Data%20PreservationSystem.pdf)>.
8. AOL, “Online Industry Leaders Announce New Effort to Use Advanced Technologies to Help Combat Child Exploitation,” press release, June 27, 2006, <http://press.aol.com/article_display.cfm?article_id=1008>.

Rodney Petersen is Policy Analyst and Security Task Force Coordinator for EDUCAUSE.