CENTER FOR
DEMOCRACY
&
TECHNOLOGY

1634 I Street, N.W.#1100
Washington, DC, 20006
http://www.cdt.org

June 2, 2006

TO: Interested Persons
FROM: Nancy Libin, Staff Counsel
Jim Dempsey, Policy Director
RE: Mandatory Data Retention – Invasive, Risky, Unnecessary, Ineffective

Legislation has been proposed at the state and federal level to require providers of Internet services to retain for up to one year records to permit the identification of subscribers to such services, and the Department of Justice recently told Internet industry representatives that it is considering a two-year mandatory data retention proposal. The full scope of the concept remains undefined, but it could encompass not only ISPs but also website operators, telephone companies, cable companies, wireless carriers, employers who provide employees with Internet access, hotels, libraries, universities, and WiFi hotspot providers. These proposals raise serious concerns about privacy, security, cost, and effectiveness.

CDT has long been at the forefront of efforts to empower parents and other caretakers to protect children from offensive content and dangerous conduct online. We fully support the criminalization of child pornography and we believe that law enforcement agencies at the federal, state and local levels should be well-trained and have sufficient resources to pursue child pornography and abuse cases. We also recognize the legitimate need law enforcement has for information to fight terrorism. However, for the reasons set out below, we believe that a data retention requirement is not likely to contribute in a significant way to protecting children and fighting terrorism and poses other risks that well outweigh any possible benefits.

1. Data retention laws <u>threaten personal privacy and pose a security risk, at the very time the public is justifiably concerned about security and privacy online</u>.

   - One of the best ways to protect privacy is to minimize the amount of data collected in the first place. A data retention law would undermine this important principle, resulting in the collection of large amounts of information that could be abused and misused.

   - Mandatory data retention laws will create large databases of information that trace personal contacts and relationships and will make subscribers' personal information vulnerable to hackers or accidental disclosure.

- At a time when identity theft is a major concern and security vulnerabilities in the Internet have not been adequately addressed, data retention would aggravate the risk of data breaches and unauthorized use.

- The Internet activity of Members of Congress, law enforcement officials and other government agencies would also get swept up in the proposed retention of Internet data. For instance, data about communications between agencies and undercover operatives would be retained. Retention, given the threat of unauthorized access, thus poses risks to homeland and national security.

2. Data retention laws create the danger of mission creep.

- It is all but certain that the vast databases that ISPs and telecom providers will create will be tapped by law enforcement for other purposes unrelated to child porn investigations.

- Service providers themselves might be tempted to use the stored information for a range of currently unanticipated purposes.

3. Data retention laws are unnecessary – authority already exists to preserve records.

- Already, under current law, any governmental entity can require any service provider (telephone company, ISP, cable company, university) to immediately preserve any records in its possession for up to 90 days, renewable indefinitely. 18 USC §2703(f).
- Data preservation orders are mandatory – service providers must comply.
- Data preservation orders do not require judicial approval and do not need to meet any evidentiary threshold. They can be issued by any governmental entity.
- There has been no showing that this "data preservation" authority is inadequate.
- There is no showing that ISPs fail to cooperate with data preservation requests.

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.

- DOJ has failed to follow-up on allegations of online child sexual abuse, but this has not been due to lack of evidence. Justin Berry, the now 19-year old whose story in the *New York Times* triggered the current wave of concern, testified at length before the House Commerce Committee about the failure of DOJ to follow-up on information he provided to the Child Exploitation and Obscenity Section, including names, credit card numbers and computer IP addresses of approximately 1,500 people who paid to watch child pornography from his sites. http://energycommerce.house.gov/108/Hearings/04042006hearing1820/Berry.pdf

- Calls for data retention mandates are based on a misunderstood incident in Colorado where law enforcement responded too slowly to serious and specific allegations.

- The Colorado incident that prompted recent support of mandatory data retention involved an ISP that was unable to provide an IP address in a child porn investigation. In that case, however, the prosecutor did not act on the investigation for 4 months, after which time the ISP had deleted the sought-after information.

5. Proceeding with data retention would require a full-scale re-examination of data privacy laws.

   - The European Union enacted a data retention rule last year but it also has detailed rules governing the privacy of electronic communications information in terms of both governmental access and corporate use and disclosure. The US does not have a general privacy law that protects the data that would be collected and retained.

   - In particular, the Electronic Communications Privacy Act (ECPA) sets very low standards for governmental access to data and places no limits on the use that ISPs can make of the non-content information they collect and maintain about their subscribers. Service providers can, unless they make a privacy promise to the contrary, disclose subscriber identifying information for any purpose, except to a governmental entity. Mandating large-scale data retention would upset the balance in ECPA and would require a larger re-examination of how that law works.

6. A data retention database would principally serve as a honeypot for trial lawyers in civil cases.

   - Already, the vast majority of requests that ISPs and others receive for customer information come not from the government but from private litigants in divorce cases, copyright enforcement actions, and commercial lawsuits.

   - Whistleblowers and journalists would also be among those whose records were subpoenaed.

7. Data retention laws are not likely to be effective.

   - The current data preservation law is preferable to data retention because the data preservation request can specify exactly what information is needed for the investigation at hand. Data retention laws, on the other hand, take a "one-size-fits-all" approach that is unsuited to the dynamic nature of Internet investigations.

- Data retention laws are likely to be both over-inclusive and under-inclusive at the same time – forcing service providers to store multiple terabytes of useless information while possibly missing the information that would be useful in a particular investigation.

- Retention of more data than is necessary to achieve law enforcement objectives will be counterproductive, drowning companies and investigators in irrelevant and potentially misleading information that will be very difficult to search or use.

- Criminals will always be able to thwart data retention laws by finding ways to prevent their data from being traced—using public facilities, using proxies and other anonymizing technology.

8. Data retention laws undermine public trust in the Internet.

   - Subscribers are less likely to use services that compromise the privacy and security of their personal information. Since data retention would apply to all Internet services, most of the impact would fall on legitimate service providers. Ordinary users engaging in everyday activity might hesitate to use a range of online services.

9. Data retention laws are burdensome and costly.

   - Data retention laws would require investments in storage equipment and force ISPs to incur large annual operating costs. Companies would also incur the cost of hiring employees whose sole responsibility would be to conduct searches for and provide information to law enforcement and civil litigants.

   - Currently, Internet access is relatively affordable and therefore available to many. The huge costs associated with data retention would be passed on to consumers, inhibiting efforts to expand Internet access.

   - Data retention laws could force websites that currently offer free content to the public to start charging fees for access to their sites.

For more information, contact Nancy Libin, 202-637-9800 x 113.