

Mandatory Data Retention Poses Major Concerns, May Have Little Benefit

November 13, 2006

The Attorney General and the FBI Director have said that Internet Service Providers and others should be required to maintain for some extended period of time data identifying their customers' online activity. Among the Members of Congress who have embraced the idea is Congresswoman Diana DeGette (D-CO), who introduced and then withdrew a proposal earlier this year. The Justice Department has had several meetings with industry representatives and privacy groups to discuss the concept of data retention legislation. The full scope of the mandate 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.

During House Energy and Commerce Committee hearings on ISPs and child safety earlier this year, some ISP representatives testified that their companies always have retained, or had begun to retain, certain subscriber identifying information for extended periods of time in anticipation of—or perhaps to obviate—data retention legislation. For instance, Comcast announced that it would begin retaining IP addresses assigned to its subscribers for 180 days instead of 31 days, which had been its policy. Earthlink stated that it retains “RADIUS” logs¹ for several months in a “live,” immediately accessible database and stores the logs off-site in an archived format for up to seven years.

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.

For the reasons set out below, however, we seriously doubt whether a data retention requirement would be likely to contribute in a significant way to protecting children or

¹ Remote Authentication Dial In User Service <http://en.wikipedia.org/wiki/RADIUS>

fighting terrorism. Instead, a mandate would pose other risks that seem likely to outweigh any possible benefits, and it might actually harm, rather than enhance national security and law enforcement efforts to find child predators online. Indeed, data retention proposals raise serious concerns about privacy, security, cost, and effectiveness.

Before Congress takes the radical step of enacting mandatory data retention legislation, it should require the administration to show how the existing data preservation law is insufficient, whether a data retention requirement is likely to be effective, the effect of a data retention requirement on personal privacy and data security, and what the costs associated with data retention would be for government and industry. At the very least, Congress should consider several alternatives and amendments to existing laws that would better focus law enforcement *and* protect data privacy and security.

CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for a wide range of computer and communications companies, trade associations, and public interest organizations interested in communications privacy and security issues. CDT has invited Department of Justice officials to meet with DPSWG to explore in greater detail the government's needs and industry's role in protecting children online. CDT believes that, before legislation is considered, all stakeholders need a better understanding of how the government conducts investigations related to child pornography, child exploitation and related offenses, including such questions as: What information is most relevant to the government's investigations? What are the current practices and experiences in storing and accessing that information? What better ways might there be to get that information to the government? What are the technological tools available or in development to identify child pornography or situations of potential abuse? Until these questions are addressed, legislation is premature.

Core Concerns with Data Retention Legislation

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.
 - 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. Retention, given the threat of unauthorized access, thus poses risks to law enforcement and to homeland and national security.

2. Data retention laws are likely to have only limited benefit and, in fact, could impede law enforcement's ability to track and apprehend criminals.

- The current data preservation law is preferable to data retention because a 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.
- 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. A data retention law therefore would be most effective in capturing the data of innocent people, not criminals, and it could hurt law enforcement by driving criminals to use technologies that would render even existing data preservation laws ineffective.
- 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.
- Commercial ISPs would retain detailed records of all communications to, from and between members of police departments and the FBI. This data would be an attractive target to criminals and terrorist groups and would increase the risk of exposure of undercover investigators and confidential informants.
- Data retention laws could prompt service providers to store data “off-shore,” where it would be out of the immediate reach of law enforcement and where access would be subject to the laws of other countries, defeating the whole purpose of the mandate.

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

- The vast databases that ISPs and telecom providers will create could 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.
 - 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 last summer 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>
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 the EU 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 privacy law that adequately 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 secondary 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, and government agencies can access the data without judicial approval. 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 could serve as a honey pot for trial lawyers in civil cases.
 - Already, the vast majority of requests that ISPs and other online service providers 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 also would be among those whose records could be subpoenaed.

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. Because 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 would be 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 and training employees whose sole responsibility would be to conduct searches for and provide information to law enforcement and civil litigants. Training ISP employees in the proper handling and use of data would be essential to ensure admissibility of this data in court.
 - As one example, AOL UK estimated that its compliance with the EU data retention directive would cost at least \$40 million to implement and another \$14 million per year to maintain.
 - The costs associated with data retention would be passed on to consumers, inhibiting efforts to expand Internet access to poorer communities.
 - Data retention laws could force websites that currently offer free content to the public to start charging fees for access to their sites and could put small ISPs out of business and discourage new entrants to market.

- The potential costs will increase exponentially with the growth of the Internet and the inevitable cross-border requests pursuant to information-sharing treaties between the US and other countries.

Possible Alternatives to Data Retention Legislation

There are other, less burdensome but more effective measures that Congress, the Justice Department, and child protection advocates should consider:

- Allow the National Center for Missing and Exploited Children (NCMEC) to issue data preservation orders, or alternatively, require entities to retain information immediately upon making a referral to NCMEC under 42 USC §13032. (Currently, only government entities can issue data preservation orders under 18 USC §2703(f).) (Note that under current law, ISPs are permitted to disclose non-content information to NCMEC *without* any judicial process. *See* 18 USC §2702(c)(5).)
- Place a federal prosecutor with authority to issue subpoenas at NCMEC so that information can be obtained immediately after service providers make referrals. This would assist law enforcement in obtaining the information it needs without having to wait for referrals from NCMEC.
- Require companies to include IP address (and any available subscriber identifying information) in initial report to NCMEC under Section 13032 to expedite and facilitate investigations.
- Increase resources for staffing and training of law enforcement and for necessary improvements to technical support and infrastructure.

Policy Issues Congress Must Consider Before It Legislates

While we remain opposed to mandatory data retention legislation, the following are some questions that should be addressed before Congress considers legislation.

- What information should companies have to retain? Companies should not be forced to retain information that they don't already generate and save (for some period of time) for business purposes. The entities to be covered and the type of information to be retained would have to be very precisely and narrowly defined. It seems there is no reason, for example, to retain any information other than IP addresses assigned to customers.
- What should be the standard for government access to the data? Transactional information related to Internet communications is currently available to the government with a subpoena or a National Security Letter, neither of which requires judicial approval. In the case of data retained for the benefit of the government,

shouldn't the statute require the government to obtain at least a court order under 18 USC 2703(d) before getting access to the data? While IP addresses currently are available with a subpoena, Internet records like IP addresses are much more revealing than traditional subscriber identifying information, especially since they can be combined with other information routinely stored by search engines and content providers.

- What obligations should ISPs have to maintain the integrity and security of the data?
- Should ISPs be precluded from using retained information for secondary purposes without first obtaining customer consent? Should ISPs be allowed to use the information for *any* secondary purpose? Under current law, ISPs are permitted to use their customers' non-content information and to disclose it to "any person other than a governmental entity," meaning that ISPs could lawfully use or disclose any information retained pursuant to the data retention mandate to any non-governmental entity. (18 USC §2702(c)(6)).
- Should legislation provide a statutory remedy—such as an exclusionary rule—to defendants whose electronic communications or records were obtained in violation of the statute? Similarly, should legislation impose penalties on those who make improper requests for or misuse data obtained under the mandate?
- Should a data retention mandate be coupled with a data destruction mandate? Should the government be required to delete information it obtains pursuant to the mandate, after such information is no longer needed for the investigation for which it was obtained?
- What types of Internet access providers will the statute cover? Will the coverage be limited to actual network providers (Earthlink, AOL, etc.)? Extending coverage to small access providers like libraries, coffee shops, hotels and other WiFi hotspots would add huge costs with little benefit.
- Will government access to the data be limited to certain investigatory purposes? Because the justification put forth so far has focused on child pornography, the government should not have access to the data for other purposes without Congressional authorization, except when emergencies involving immediate danger of death or serious physical injury to any person justify disclosure of the information. Furthermore, the government should be prohibited from using this information for data mining or other predictive purposes. The government should only get access to the information relevant to a particular, ongoing investigation.
- What kind of oversight is appropriate? Is a sunset provision appropriate? Congress should receive periodic reports showing the number of requests made, the number and types of investigations in which the information was used, and the effectiveness of the data retention mandate in combating child porn.

- In order to ensure public confidence and government accountability and to deter abuse, should law enforcement be required to notify the persons whose information it obtains? Legislation could require after-the-fact notice, unless a senior law enforcement officer certifies that such notice would jeopardize an ongoing investigation.

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