3-4-2012

Politics, Privacy, and Child Pornography: The Battle Over Data Retention and H.R. 1981

Agatha M. Cole
Cardozo Arts & Entertainment Law Journal

Politics, Privacy, and Child Pornography: The Battle Over Data Retention and H.R. 1981

Posted on March 4, 2012, by admin

Author: Agatha M. Cole, Staff Editor, Cardozo Arts & Entertainment Law Journal

In August of 2005, a Florida investigator on the Internet Crimes Against Children (ICAC) taskforce—a national network of federal, state, and local law enforcement agencies dedicated to preventing online child pornography and other Internet crimes against children—received a video depicting the rape of a two-year old child. ICAC investigators traced the video to an IP address in Colorado associated with Comcast, one of the largest Internet service providers in that state. The only information needed to determine the location of the computer used to post this video was the record revealing which Comcast subscriber had been assigned to that particular address when the video was posted, just four months earlier. Unfortunately, by the time investigators requested the subscriber data, Comcast had already discarded the relevant IP address assignment records for that time period. The Comcast controversy is a solemn example of a situation where the availability of IP address data could have made all the difference. Instead, a dangerous child predator is still out on the loose, and the infant in the video could be the victim of ongoing sexual abuse. Making matters worse, it is not clear whether authorities receiving a similar lead today would fare any better than they did in this instance.

IP address records can provide critical information in a criminal investigation. In the law enforcement context, IP address data is often required to associate criminal activity on the Internet with a real-world access point. Law enforcement agencies claim that the Comcast incident is not an isolated occurrence, and that missing IP address records represent are a recurring obstacle for law enforcement when trying to determine the origination point of certain online activities in child sex exploitation investigations.

In the United States, federal law does not require ISPs to retain IP address information or any other data for law enforcement purposes. ISPs may freely set their own policies regarding when to discard IP address records. Some ISPs retain IP address records for extended periods as a matter of corporate policy, while other providers do not maintain such records or only retain them for a short period of time. In the absence of legally defined retention periods or industry wide standards, the length of time ISPs retain such records varies from one provider to the next.

Assuming an ISP retains IP address records, however, it is relatively easy for law enforcement to gain access to them under current law. Section 2703(c)(2) of the Stored Communications Act enables law enforcement and other government entities to obtain "basic" subscriber information, such as IP address assignment records, with a mere subpoena. Subpoenas are

routinely granted by court clerks without any showing of cause, suspicion, or relevancy to an investigation. Government access to IP address data is therefore relatively unrestrained by federal law. In addition, there is no requirement that the subject of a government inquiry be notified that his or her records were sought by law enforcement, rendering the process as opaque as it is unfettered.

The retention of IP address records is a highly controversial topic among Internet policy experts. Determining the appropriate legal framework for the storage and maintenance of electronic records pertaining to Internet traffic is a particularly complex task because of the numerous stakeholders involved. Law enforcement agencies generally support data retention because such records can aid them in criminal investigations, whereas privacy advocates tend to oppose data retention to the extent that widespread collection and storage of individuals' data poses a threat to civil liberties on the Internet. Politicians are primarily concerned with the ostensible centrality of such records in child pornography investigations. Meanwhile, ISPs worry about the potential burden of any new proposal on their operational expenses.

Although no federal law requires ISPs to maintain or retain IP address records for any specified amount of time, Section 2703 of the Stored Communications Act requires ISPs to preserve evidence specifically identified by law enforcement as relevant to a particular case or investigation. This provision compels electronic communication providers, including ISPs, to take "all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process" upon request by a government entity. Under the same subsection, ISPs must retain such records for a 90-day period, which is renewable for another 90 days upon further request by the government entity.

Most ISPs seem comfortable with the data preservation framework. In fact, some even publish manuals with examples of requests or forms to help law enforcement file data preservation requests. ISPs tend to prefer data preservation over compulsory data retention, since a mandate would require many of them to overhaul current processes and acquire supplemental storage space. But data preservation has its shortcomings, since it is only useful when law enforcement can identify records that are relevant to a particular investigation *before* the provider deletes them. The Department of Justice argues the preservation framework is inadequate, because preservation requests often come too late.

Certain ISPs have amended their retention policies in recent years due to growing pressure from law enforcement after highly publicized incidents such as the Comcast controversy. After the incident, Comcast lengthened its retention period for IP address data to 180 days, and Verizon now keeps such data for one year. But other ISPs continue to have unclear or inconsistent policies that leave both law enforcement and users guessing about how long such data is retained. As a result, law enforcement agencies, the Department of Justice, and several child welfare advocacy groups have called upon Congress to enact new compulsory data retention requirements to help combat online child pornography.

On May 25th, 2011, Rep. Lamar Smith and Rep. Debbie Wasserman Schultz introduced H.R. 1981, the Protecting Children From Internet Pornographers Act of 2011. The bill amends section 2703 by requiring the retention of temporary IP address assignment records "for a period of at least 18 months." The purpose of the retention mandate is "to aid law enforcement officials in their fight against child sexual exploitation," but the scope of access to those records is not limited to investigation of crimes against children. Simply put, the logged data could be used to aid law enforcement in the investigation of any type of crime; not just child pornography. The data retention mandate in H.R. 1981 would apply to a wide range of communications providers. However, the bill carves out an important exception for IP addresses "transmitted by radio communication." In other words, the bill exempts wireless providers from the retention requirement. The bill also includes a "Sense of Congress" provision stating that records retained pursuant to the new law should be "stored securely to protect customer privacy and prevent against breaches of the records." Although that provision has no substantive legal force, it expresses the representatives' view that cybersecurity is an important aspect of the new proposed framework.

H.R. 1981 is the first bill of its kind to have successfully passed through Committee assignment. Furthermore, H.R. 1981 was introduced by party leaders from both sides of the aisle, increasing the likelihood that it could pass in the House. The bill was referred to the House Judiciary Committee, and passed by a vote of 19-10 in July 2011. It will soon be considered by the House membership in its entirety. H.R. 1981 has a long list of supporters, including the Department of Justice, child protection advocacy groups, and several law enforcement associations. However, numerous public interest groups, legal scholars, and Internet businesses oppose the retention mandate.

Opponents of the bill are concerned about the potential for limitless government intrusions that could occur if a retention mandate were imposed without placing further restrictions on access. Civil liberties and privacy rights advocates argue that H.R. 1981 reaches too far "in tracking and storing information about all Internet users," by enabling the government and private entities to track everything we do online.

H.R. 1981's most vocal opponents include the American Civil Liberties Union (ACLU), the Center for Democracy & Technology (CDT), and the Electronic Frontier Foundation (EFF). These groups claim that the widespread collection and storage of electronic records about private individuals harms users' privacy rights, "both vis-à-vis the government as well as private actors," and creates chilling effects on freedom of expression on the Internet. Data retention also runs counter to many privacy advocates' support of data minimization principles. Data minimization is the principle that companies should retain only data, which is justifiably necessary for a specific and legitimate purpose, but purge everything else in the interest of protecting users' privacy and reducing the potential for harm from a security breach. Professor Chris Hoofnagle stresses that formal data minimization requirements such

as retention limits advance privacy by impairing "the ability of companies and law enforcement to create long-term profiles about people."

Rep. Lamar Smith counters these claims by explaining that H. R. 1981 mirrors telephone data retention requirements. In 1986, the Department of Justice petitioned to extend the required retention period for telephone toll call records to assist with law enforcement activities. The FCC responded by changing the retention requirement from 6 months to 18 months. To date, telephone service providers in the United States are required to retain a record of the caller name, address, phone number, date, and time of any toll calls for which it produces a bill for a minimum of 18 months. According to Rep Smith, H.R. 1981's 18-month retention requirement is identical to the toll call record retention period, and "merely applies to the Internet what has applied to telephones for decades." Although IP address data and telephone toll call records are both characterized as non-content data by common law interpretations of the Stored Communications Act, the Congressman's analogy oversimplifies the similarities between the two types of records. IP address data has the capacity to reveal more information than toll call records, since it can be compared to website logs to identify a subscribers' online activities; whereas toll call records reveal nothing about the content of phone conversations, showing only subscriber information associated with a particular phone number.

Critics of the bill also argue that cybersecurity risks (i.e. the threat of accidental disclosure or interception by independent bad actors such as hackers or other malicious third parties) accompanying mass scale records retention outweighs the public safety interest in the mandate. The threat of cyber-attack and data security breach is a constant concern for ISPs and other Internet businesses. While ensuring that the appropriate level of security is put into place by ISPs is extremely important, it is impossible to guarantee that any data is ever completely free from the threat of cyber-attacks. Cybersecurity is an inescapable problem for any organization that stores individual's personal data. However, allowing cybersecurity fears to overshadow the debate over data retention is self-defeating, since the availability of IP address records helps combat the very cybersecurity threats at issue, by making it easier to identify hackers and other bad actors on the Internet.

In any event, the likelihood of H.R. 1981 becoming law is quite low, given Congress' inability to pass legislation in election years, and the bill's irreconcilable flaws, such as its exception for wireless providers. However, the likelihood of a similar data retention law passing in the near future is increasing, and warrants a lengthier discussion of how such a proposal could further the interests of all stakeholders involved.

The current debate over data retention demonstrates the difficulty of balancing law enforcement and public safety interests against individuals' privacy interests. Yet the current debate seems to gloss over one very important consideration, which is that data of all kinds,

including, but not limited to IP address data, is increasingly retained by all sorts of entities for various reasons.

Given the centrality of data to Internet businesses and the emerging role of data in our economy and society at large, the current debate over IP address records retention—which is overwhelmingly characterized by data minimization arguments—seems irrelevant and futile. The prevalence of data retention, as a business practice, is trending upwards because the potential benefit of having access to information, weighed against the cost of maintaining data, falls increasingly in favor of retention, in large part due to the increasing marketability of data and the decreasing costs of storage. Viewed in this light, data retention is an inevitable aspect of the information economy, and the current arguments against H.R. 1981 miss the point.

As noted by Professor Dierdre Mulligan, our growing cultural and practical dependence on services that generate records containing personal information requires a reassessment of constitutional protections constraining "government investigation into citizens' private acts whenever those acts are recorded or can be inferred from data collected in the private sector." Privacy concerns cannot be effectively or efficiently dealt with by attempting to prevent data retention or promote data minimization. The more important question, then, is not whether the government should define retention periods for this or other types of data, but rather, how to build a sustainable framework that will ensure the best possible outcome for all stakeholders. Reframing the question as such would enable policymakers to consider how a data retention mandate might actually serve to advance individuals' privacy interests.

Perhaps imposing a data mandate, against all common sense notions about data minimization, could actually be good for privacy. Imposing a retention requirement could lead to increased public awareness and regulatory scrutiny, which in turn, might result in stronger privacy for such data. If data is consistently retained, it will bolster concerns about security and access, which is where privacy advocates should be concentrating their efforts anyways. Privacy advocates should treat H.R. 1981 as an opportunity to advance their interests through a retention mandate instead of rejecting the concept wholesale. Rather than glossing the surface by taking a data minimization stance, privacy advocates should support sustainable progress by shifting the discussion from whether data retention threatens privacy to one about how to protect sensitive data from government abuse, deceptive private sector use, and independent bad actors.

The absence of legal safeguards against overreaching government entities and the "outdated and inadequate standards" of the Stored Communications Act means that data subject to retention requirements "could be obtained by law enforcement with almost no restrictions or limitations." For this reason, the privacy issues raised by a data retention mandate can only be comprehensively addressed by another type of reform which is not at all addressed in H.R.

1981—the imposition of reasonable safeguards, restrictions, and limitations on when and how this data could be accessed by law enforcement.

Any proposal regarding a new data retention framework is both incomplete and unacceptable from a public policy perspective, unless it addresses not only retention issues, but also the laws governing how IP address data is accessed by law enforcement. As noted by the CDT in a hearing on data retention this past January, "[p]roposals to mandate data retention cannot be viewed in a legal vacuum, but rather must be considered in light of the very limited privacy protections that are currently afforded to the data held by service providers."

One plausible solution would be to require law enforcement to obtain a warrant to obtain such data. Subjecting IP address data to a warrant requirement would be both reasonable and practical. It is reasonable in the sense that it is the standard mechanism for balancing individuals' interests in privacy against public safety and law enforcement interests in preventing and punishing criminal conduct. It is also practical, in that the foundation and framework already exists and applies to similar types of information.

Law enforcement advocates may argue that imposing a warrant requirement would halt investigations where speedy action was needed, but the warrant requirement would be subject to the same general exceptions as in any other type of investigation—namely exigency (i.e. the emergency doctrine) and the plain sight exceptions to the warrant requirement. In other words, if the circumstances were so exigent that obtaining a warrant would put an investigation at risk, then that would constitute an exception within which law enforcement could seek the data without a warrant. Similarly, data that was publicly available or arguably in plain sight, would also be subject to an exception. Another option would be to amend the Stored Communications Act by removing the "basic subscriber data" provision in subsection (c)(2), so that IP address data would no longer constitute an "exception" to the "D order" requirement that requires a slightly higher showing of cause than a subpoena but less than a warrant, for other types of data covered by §2703.

In sum, resisting the inevitable collection, maintenance, and storage of data is an ineffective and unsustainable strategy for privacy advocates in our increasingly information-driven economy. It is therefore more important than ever to focus on laws governing access to personal data. As such, legislators working towards a comprehensive data retention solution need not only remove the wireless exception to from H.R. 1981 but must also amend section 2703 of the Stored Communications Act to ensure that any retained data will be subject to adequate privacy protections.
