Written Testimony

of

Kate Dean

United States Internet Service Provider Association

Before the

U.S. House of Representatives

Committee on the Judiciary

Subcommittee on Crime, Terrorism and Homeland Security

"Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes"

January 25, 2011

My name is Kate Dean and I am appearing here today to represent the United States Internet Service Provider Association ("US ISPA") where I am the executive director. US ISPA is a unique-member driven organization that was founded in January 2002 based on successful collaboration by service provider attorneys on the first USA PATRIOT Act. The association was established to focus on a discrete set of policy and legal concerns common to major Internet service, network and portal providers. US ISPA works primarily on law enforcement compliance and security matters – including ECPA, CALEA, and cybersecurity – and notably, in the fight against online child exploitation.

With our focus on law enforcement compliance issues, it is only natural that US ISPA members are interested in participating in discussions regarding data retention. In fact, our members and US ISPA itself have participated in many efforts seeking to address data retention, including past dialogues between industry and the Department of Justice and with state and local law enforcement through the Internet Crimes against Children ("ICAC") Taskforces and the National Association of Attorneys General. We welcome the opportunity to continue the dialogue today.

We are interested in hearing from fellow panelists about the challenges that law enforcement face when conducting investigations that may rely on data from our member companies. We hope that through open discussion of these issues, we may be able to develop solutions that can address law enforcement's needs without any unnecessary negative impact on business interests or the privacy of our customers.

Over the years US ISPA has carefully examined data retention proposals, and has come to the understanding that a blanket legal requirement to retain Internet usage data for established time periods is certain to present significant challenges to the communications industry, both for well-established companies and newer online media enterprises, as well as unintended consequences which are incapable of precise identification. Nevertheless, US ISPA has achieved success in connection with targeted legislative directives aimed at a specific law enforcement challenges. Once such recent success grew out of US ISPA and its members' efforts to help law enforcement and other constituencies battle crimes against children.

It is safe to say that US ISPA and its members are industry leaders in the fight against online child exploitation. In 2005, the organization led the way by developing and publishing Sound Practices for Reporting Child Pornography, created through a joint project between US ISPA and the National Center for Missing and Exploited Children ("NCMEC") to educate the Internet Service Provider ("ISP") community on its obligations to report incidents of apparent child pornography. US ISPA recently updated its Sound Practices to reflect the changes to reporting and preservation procedures introduced by the PROTECT Our Children Act, passed by Congress in 2008. US ISPA strongly supported that Act and its legislative acknowledgment of US ISPA's long recommended practices for child pornography reporting. US ISPA and its members provided draft language, brainstormed ideas, and testified in hearings to support the efforts to clarify provider child pornography reporting obligations.

Our members were also active in the Online Safety and Technology Working Group ("OSTWG") created by Congress that same year. The OSTWG was tasked with examining the state of online safety education, parental controls, industry reporting mechanisms and data retention. The OSTWG report was presented to Congress in June 2010 and is available online at the National Telecommunications and Information Administration website. US ISPA members have also been active in efforts such as the Internet Safety Technical Task Force, the Technology Coalition, the Virginia Attorney General's Internet Safety Task Force, and the Financial Coalition against Child Pornography.

US ISPA has also worked on these issues directly with state and local law enforcement. Members frequently interact with the ICAC Taskforces, conducting training and attending meetings and conferences. In addition, US ISPA was instrumental in working with the National Association of Attorneys General to develop ISP Sound Practices for Subpoena Compliance. The ISP Sound Practices for Subpoena Compliance provides the ISP community with guidance regarding how companies can respond to law enforcement requests in a manner that assists law enforcement within the framework of the Electronic Communications Privacy Act ("ECPA").

US ISPA member companies continually demonstrate their commitment and leadership through industry efforts to promote cooperation with law enforcement. Members maintain 24x7 response capabilities, offer law enforcement guides to lawful data disclosures under ECPA, conduct training for investigators and prosecutors, and maintain an open dialogue with all levels of federal, state and local law enforcement.

As this long history of contribution and cooperation makes clear, among industry associations, US ISPA is exceptionally committed to supporting law enforcement efforts to bring to justice those who use the Internet for criminal benefit, and most of all, those who harm children. And we fully recognize and appreciate the critical role that electronic evidence plays in those efforts.

It is our hope that by discussing the challenges associated with generalized data retention proposals, we can further a productive dialogue about how industry and law enforcement can continue to work together to increase the chances of successful investigations and prosecutions.

Indeed, beginning the discussion with uniform mandatory data retention proposals may be counter-productive. Every time industry has seriously examined how it might operationalize broad data retention mandates, it has concluded that such an undertaking is dramatically overbroad and fraught with legal, technical and practical challenges. I would like to highlight a few of those challenges.

Mandatory data retention presents complex challenges and risk

First, I would like to address the issue of over breadth. Mandatory data retention requirements potentially require an entire industry to retain billions of discrete electronic records due to the possibility that a tiny percentage of them might contain evidence related to a crime. While we certainly agree that the potential criminal activity could be serious and should be investigated, we think that it is important to weigh that potential value against the impact on the millions of innocent Internet users' privacy. The privacy issues that will be raised by a data retention proposal could include questions regarding the legal standard by which law enforcement and other parties could subpoena such data and whether retention obligations would create new needs for additional privacy and security regulation. Indeed, retention could bring with a whole new rash of complex regulatory and legal requirements that go far beyond simply saving data.

Potential legal considerations aside, from a practical perspective the sheer volume of data alone makes the task of gathering and storing such data daunting. Many providers have hundreds of thousands of users, some millions, and others hundreds of millions. There are more than 250 million Internet users in North America alone. These users access and use their networks all day, every day of the year. As the technology industry innovates, new devices, such as e-readers, tablets and game devices, continue to multiply the number of ways that each of these users can access the Internet. Today, it is not uncommon for a user to use Internet-based services through multiple devices simultaneously. Access options are multiplying as well. Wired or wireless, network providers now include hotels, airlines, municipalities, libraries, universities, and the family-owned coffee shop on the corner. Imagine how many log-ins a top-tier service provider sees over a 24-hour span today. Now imagine how many log-ins they'll see in a 24-hour span in 6 months. The growth could be exponential.

Maintaining exponentially-increasing volumes of data, in a searchable format that would enable companies to quickly locate a targeted user's data amidst exabytes of information, would be extremely complicated, and burdensome. While storing huge volumes of data may be possible, providers have concerns about ensuring the integrity and availability of that data to respond to legal demands. The sheer complexity of systems required to perform these tasks increases the probability of crashes, failures, and delays. Thus, despite a provider's efforts to comply with the data retention obligation, the data, through no fault of the provider, may still not be available to law enforcement.

Perhaps the biggest concern for both providers and law enforcement may be the risk impairing provider response times for ordinary legal requests and, more importantly, that their ability to respond promptly in true emergencies could suffer. Those who work day-to-day with law enforcement know how important it is that a provider be able to call up data in seconds in cases involving an emergency where time is of the essence. Data from ISPs can be critical in emergencies, such as child abductions, and providers know that in such cases hours, even minutes, could mean the difference between a child returned home safely and one who never makes it home. For this reason, the longer search times that are likely to result from a data retention mandate are a grave concern.

Finally, we would like to note that many of these challenges have plagued the European Union's attempted implementation of its Data Retention Directive (Directive 2006/24/EC). Legislation implementing the Directive has been the subject of much litigation and, in March of last year, Germany's national data retention law was declared unconstitutional by its Federal Constitutional Court. The EU's Article 29 Data Protection Working Party not long ago issued a report describing the difficulties companies face interpreting and attempting to comply with the varying data retention requirements in each EU country. As we discuss this issue here today, a similar dialogue is taking place within the EU as they re-assess their approach to data retention. Not only are shorter time periods under consideration, but they are also re-examining whether they should abandon broad-based retention in favor of the targeted preservation system used here in the U.S.

Data preservation is a powerful tool for law enforcement that exists today

U.S. law enforcement has long had mechanisms at its disposal to preserve electronic evidence that might be useful for criminal or civil investigations.

The preservation authority in the Stored Communications Act (18 U.S.C. § 2701 *et seq.*) was enacted into law in 1996 and has been used in a wide range of criminal investigations over the past 15 years. Section 2703(f) allows law enforcement, by letter, fax, or email to direct service providers to preserve records and other electronic evidence in their possession pending the issuance of a court order or other legal process. Providers must retain the records requested for 90 days, and this initial period can easily be extended for an additional 90 days upon a renewed request by law enforcement. Thus, today, information and evidence believed to be important to a law enforcement investigation can be preserved with little or no burden on the government to issue formal legal process or even demonstrate relevance.

Preservation authority is a powerful, targeted tool available to law enforcement today that, from the perspective of US ISPA's members, strikes the appropriate balance between the government's need to preserve evidence for a pending investigation and the avoidance of undue burden on ISPs by compelling data retention well beyond the time periods necessary to meet their business needs.

Let me return to the recent success that I alluded to at the beginning of my testimony: a targeted legislative solution that USISPA and its member companies were instrumental in achieving in the context of crimes against children. As this Subcommittee is well aware, Congress recently further refined investigative data preservation authority in this area tool in the PROTECT Our Children Act (18 U.S.C. § 2258(h)). Now, whenever a provider makes a report to the CyberTipline, the report itself will include the basic digital data that law enforcement considers critical to identifying the perpetrator of child pornography crimes.[1]

[1] This data includes identifying information concerning the individual who appears to have committed the crime (such as email address, Internet Protocol address, and any self-reported

Law enforcement need not issue a preservation request in connection with each provider report of apparent child pornography to NCMEC's CyberTipline in order to ensure that important investigative data is preserved. In addition, the statute requires providers to automatically preserve for 90 days both the data contained in the CyberTipline report and additional data that Congress determined to be key to solving crimes against children. Upon notice of NCMEC's receipt of its report, providers must preserve any images or digital files commingled among the images of apparent child pornography within a particular communication or user-created folder or directory.

When the CyberTipline report is made, this electronic evidence is delivered to NCMEC and forwarded to law enforcement, and almost simultaneously preserved by the service provider, without a law enforcement preservation request and even *before* any criminal investigation has begun. Mandatory data retention is therefore assured with respect to all of the evidence accompanying CyberTipline reports, plus all of the associated evidence preserved by the provider in the user's account.

US ISPA recommends that Congress carefully assess the effectiveness of automatic data preservation under section 2258A, once law enforcement has accumulated substantial first-hand experience using the preserved data in prosecuting crimes against children. Only if data preservation proves ineffective in this context should Congress consider a much broader scheme of mandatory data retention which would apply more than 99 percent of the time to records of lawful conduct having nothing at all to with child pornography.

Examining data retention.

Before the Members of this Subcommittee consider imposing a broad mandate on American businesses that abandons the targeted approach of data preservation, we think that a great deal of further discussion is needed. We think that the topics that are critical to address in such discussions are covered entities, scope and duration, liability and cost.

1) Covered Entities

Congress must consider which types of service providers would be subject to any mandate to retain data. A comprehensive mandate would extend to all "electronic communication service" and "remote computing service" providers, as those terms are defined in ECPA. It would encompass a wide spectrum of businesses, from the nation's largest telecommunications companies down to the neighborhood coffee shop offering free WiFi access. It would also include organizations such as employers, universities and

---

identifying information); information as to when and how a subscriber uploaded, transmitted, or received apparent child pornography, or when and how it was reported to or discovered by the provider; geographic location information, such as a billing address, zip code, or Internet Protocol address; the image of apparent child pornography; and the complete communication containing the image, including data relating to its transmission and other data or files contained in or attached to the communication.

government agencies that offer Internet access to their employees or students. Organizations that diverse probably could not fit under a "one size fits all" data retention mandate without adversely impacting small businesses or even larger enterprises that lack the technology resources, surplus revenue, and technical expertise required to comply with the mandate. Yet at the same time, any data retention scheme that does not apply to all these different types of entities would likely fail because it would be so easy for those bent on engaging in criminal activity to avoid creating electronic trails simply by choosing which "on ramp" to the Internet to use.

2) Scope and Duration

Congress must also consider how to define the specific types of data that companies subject to the mandate must retain. Companies generally retain data that they need for business purposes and discard data that is of no commercial value to them. Many providers of online access services require their users to present credentials (such as a username and password) to securely identify themselves. If authentication is successful, the provider assigns a temporary IP address that enables the user to access the Internet or other online resources. Most providers retain this authentication data for billing or security purposes. Some providers, for example, free municipal WiFi systems, do not require authentication at all and thus have no authentication data to retain.

Duration of mandated data retention, like scope, is critical to assessing technical feasibility and cost. Data preservation under the Stored Communications Act and the PROTECT Our Children Act works well because no re-engineering of storage technology or redesign of search techniques has been necessary. Providers are able simply to store limited sets of data, already in their possession, that law enforcement has identified specifically in the preservation request. By contrast, retention of all data subject to mandate for all users of the providers' service gives rise to an entirely different class of technical challenges, creating resource, compliance and cost burdens that increase exponentially the longer the retention period is.

3) Liability and Privacy Concerns

Providers have well-founded concerns over the increased risks of liability associated with a broad legal obligation to retain data. Apart from the risks of data corruption, technical failures and delays engendered by the need to warehouse and manipulate vast quantities of data, the twin concerns of data privacy and security will likely bring additional obligations and risks on top of a data retention mandate. US ISPA is concerned that a data retention mandate would thus bring with it a complex regulatory framework that would impose new, and as of now unforeseen, costs, legal risks, and burdens.

With regard to data privacy and security, we would like to note that there is on-going discussion on both of these issues that could result in new requirements for industry. The recent Federal Trade Commission Staff Report on privacy recommended minimization and rapid deletion of IP address and other data that might reasonably identify Internet users. Similarly, a draft privacy bill circulating in the Senate Commerce Committee would limit the

retention of IP address and other data tied to IP addresses for only so long as necessary for service delivery or fraud prevention. Others urge congressional action to impose federal cybersecurity requirements on providers, to be enforced by private lawsuits for breach of contract or by civil enforcement actions by government agencies. US ISPA is concerned that a data retention mandate would create a "Catch-22" situation involving conflicting requirements, or a cumbersome regulatory framework that would impose new legal risks, burdens and cost to online businesses.

For providers, it will be critical that Congressional action in these areas take into account liability concerns, as well as the interaction of new legal requirements imposed on providers with existing and future legal obligations at the federal, state, and international levels.

4) Cost

Each decision made with respect to coverage, scope, duration and liability will impact the costs associated with data retention. Because the data that industry would be required to maintain is not needed for business purposes – otherwise providers would maintain it without a legal mandate to so do – all costs incurred would be exclusively to satisfy the data retention requirement.

There is no doubt that a data retention mandate will be expensive, but the costs go well beyond mere dollars. Members of the Subcommittee should consider whether providers, especially small and medium-sized companies, can absorb the costs of storing exabytes of data, of no commercial value to them, without undermining their ability to raise capital, serve their existing customers and acquire new ones, and deliver innovative products and services in a rapidly changing environment. Even under the narrowest of mandates, expert technical resources would be diverted from business innovation in order to build, maintain and secure massive data storage and retrieval systems. Cost recovery could address some of the potential negative impact of a data retention requirement, but in many ways reimbursement falls short of compensating industry for the opportunity costs of having their experts diverted away from focus on innovating the next generation of Internet-based services. Nevertheless, effective cost recovery mechanisms are an important part of the conversation.

A Potential Better Way

As Congress considers this complex issue, we suggest an alternative approach that would build on progress in data preservation and voluntary industry efforts on data retention. From our experience working with the data preservation provisions in the PROTECT Our Children Act, we think that there are further opportunities to innovate around the preservation model to address law enforcement needs. In addition, further coordination between industry and law enforcement could help ensure that these methodologies are being used to the their full potential. Finally, we believe that law enforcement continues to need further resources to support child exploitation investigations.

We believe that these approaches hold the greatest promise for improving evidence-gathering and prosecution in child pornography prosecutions, while avoiding many of the difficulties and complexities raised by data retention mandates.

In closing, US ISPA remains committed to continuing the dialogue with law enforcement about how we can contribute to the fight against child exploitation. We do not think that data retention is the best place to focus our energies. Based on our recent experience with the innovative new approach to preservation in the Protect Our Children Act, we believe that preservation is still the best approach to ensuring data is available for law enforcement investigations. We have important questions that would need to be answered by any data retention proposal, including who would be covered, what types of data would have to be saved and for how long, and what types of protections, additional obligations, and costs would come with a retention mandate. We also have serious concerns about the identifiable costs to innovation, privacy, and speed of investigations, and fears about the unknown and unanticipated collateral damage that could be caused by such an obligation.

We thank you for this opportunity to present US ISPA's views on this topic and look forward to continuing to work with the Subcommittee Members and your staff on these issues.