KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

MEMORANDUM

To: Interested Persons

From: John Morris, Greg Nojeim & Erica Newland
Center for Democracy & Technology

Re: Data Retention Mandate in H.R. 1981

Date: July 19, 2011

As detailed below, the Center for Democracy & Technology (CDT)[1] has significant concerns about H.R. 1981, the "Protecting Children from Internet Pornographers Act of 2011." Although we have concerns about a number of the sections of the bill, this memo is focused on Section 4 mandating "data retention."

CDT strongly agrees that child pornography is a horrific crime, and we have long supported increasing the resources available for its prosecution. CDT has spent extensive time examining the challenges raised by child pornography and seeking ways to fight this crime that are consistent civil liberties and with openness, competition, and innovation on the Internet. CDT testified in January of this year at the Subcommittee's hearing on "Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes."

In that testimony, we expressed our firm belief that mandatory data retention would cause significant harms and would (because of already overtaxed investigative resources) not likely increase the number of child pornographers that this country is able to prosecute and put in prison. In addition to our general concerns about any data retention mandate, we also have specific concerns about the language of H.R. 1981, which we believe is overbroad and would have an especially detrimental effect on Internet use in this country. We have outlined both our general and specific concerns below.

1. The need for ECPA reform.

Proposals to mandate data retention cannot be viewed in a legal vacuum, but rather must be considered in light of the privacy protections that are currently afforded to the data held by service providers. The Electronic Communications Privacy Act (ECPA) was a forward-looking statute when enacted in 1986, specifying standards for law enforcement access to electronic communications

[1] The Center for Democracy & Technology is a non-profit public interest organization dedicated to keeping the Internet open, innovative and free. We have long worked to protect children in the online environment while at the same time also protecting online users' privacy and civil liberties. CDT has offices in Washington, D.C., and San Francisco.

and associated data, and affording important privacy protections to subscribers of emerging wireless and Internet technologies. However, as underscored by hearings held last year by the Constitution Subcommittee, technology has advanced dramatically since 1986 and ECPA has been outpaced. The statute has not undergone a significant revision since it was enacted in 1986 – eons ago in Internet time.

Under ECPA, data mandated to be retained could be obtained by the government with almost no restrictions or limitations. The data would be available with a mere subpoena and no notice need be made to the record subject; the legal process would involve no proof of specific facts and no review by a judge. Before considering whether to require ISPs and other providers of electronic communications service to retain *more* information about users, Congress should enact reforms to update ECPA to ensure that data that is already retained is adequately protected against disclosure.

2. Data retention mandates would raise general privacy concerns and free speech concerns.

Mandatory data retention would harm Americans' privacy rights, vis-à-vis both the government and private actors. Beyond inappropriate invasion of privacy, mandatory data retention could also aggravate the problem of identity theft. Furthermore, retention would harm Americans' free speech rights – surveys suggest that it would likely chill Americans from accessing sensitive content online. Additionally, we believe mandatory data retention - even if limited in scope - is a risky and costly path to go down, and one that would invite more and more tracking of innocent Americans' Internet usage.

3. H.R. 1981 would reduce the availability of Internet access and would increase the digital divide.

In at least two different ways, H.R. 1981 would directly harm the broad availability of Internet access – especially free or low cost "WiFi" access – and would particularly harm the ability of underserved populations to reach the Internet:

a) H.R. 1981 would significantly reduce the availability of free WiFi and hurt small businesses.

Although in theory aimed at Internet Service Providers, Section 4 of H.R. 1981 would in fact reach far beyond large network providers and would directly burden *any* small business and any library or other non-profit that offers "WiFi" Internet access to users or visitors. Even though the ISPs providing service to those entities would be required to record the "temporary" network address assigned to the entity, those small establishments in turn *also* assign temporary addresses to their own users (even users who just stop in for a cup of coffee). The bill as currently drafted would require thousands and thousands of small businesses and non-profit organizations to buy new equipment and start maintaining a federally-mandated tracking database.

The implications of this far-reaching mandate would be sweeping. Locally-owned coffee shops may not be able to afford the equipment and staffing necessary to comply with this regulation of their businesses. Some would no longer be able to provide free WiFi, or perhaps any WiFi, to their customers. Libraries would similarly have to invest significant amounts of

taxpayer dollars to purchase the equipment and maintain the staff necessary to comply with such a data retention mandate. Municipalities that have begun to offer free public WiFi would likely cancel these ambitious projects. If H.R. 1981 were to pass, the rapid expansion of free WiFi – in malls, doctor's offices, airports, and other places – that this country is currently experiencing would crawl to a halt and could reverse direction. And in many cases, these free WiFi services are the only way that underserved populations can reach the Internet. If data retention mandates are to be considered at all, it is critical that they be limited to ISPs.

b) H.R. 1981 would burden small ISPs and would reduce broadband penetration in the US.

Many parts of rural America receive broadband services from small ISPs, without which they would remain stuck with slow dial-up services, unable to take advantage of large amounts of the content and services offered through the Internet today. Many of these ISPs operate with very small profit margins; even a six-month retention requirement – with the investment in new equipment and staffing that such a requirement would necessarily entail – will run some of them out of business. The impact of the 18-month requirement found in H.R. 1981 would be even more severe. Passing this bill could reduce broadband deployment in the United States. Congress should look to protect small providers from the burdens of the bill.

4. More generally, H.R. 1981 would sweep in a vast number of small businesses, churches, and other organizations.

Because the draft bill relies on the extraordinarily broad term "electronic communication service" (ECS) provider, it could sweep in literally millions of entities and force them to replace their hardware and start maintaining a federal tracking database. As originally drafted, H.R. 1981 would apply to almost anyone (likely including individuals in their homes) who purchases broadband service or otherwise operates a network within a company or organization. The bill would apply to any organization that operates a network for employee business use, and therefore would cover the vast majority of private companies, non-profits, and even churches. Moreover, the equipment that is used by virtually every home broadband subscriber issues "temporarily assigned network addresses" within the home, so homeowners would fall under the mandate in the bill. The economic burden placed on American businesses and homeowners would be breathtaking.

We understand that some language may be added to the H.R. 1981 intended to limit it to entities that have customers and subscribers. That new language would likely protect homeowners, but many small businesses would still be affected. Because of the extremely broad nature of the term "ECS," it is vital that the bill be limited to reach only ECS's that actually operate as ISPs (and not to any entity that happens to operate an internal network).

5. The inclusion of the term "remote computing services" in Section 4 is an invitation to confusion and litigation.

H.R. 1981 is confusing and internally inconsistent because it imposes data retention mandates not only on electronic communication service providers (ECS), but also on providers of "remote computing services." Remote computing service (RCS) providers when acting as such do not generally provide "temporarily assigned network addresses." Covering them in the section is an invitation to confusion among RCS providers in the growing cloud computing

industry, and would likely lead to uncertainty and litigation about the scope of this provision. Indeed, the RCS language could well, as a wholly unintended consequence of H.R. 1981, impose a significant burden on the emerging cloud computing service industry, by suggesting that wholly-internal redirection of customers to remote servers must be tracked and logged. It is vital that the obligation imposed on RCS providers to retain temporarily assigned network addresses be dropped from the bill.

6. The 18-month retention period is excessively long.

The longer the retention period, the more deleterious the impact of the law on small ISPs, businesses, libraries, and other entities that offer free WiFi access. The 18-month period apparently derives from the FCC rule that requires carriers to retain billing information for 18 months for toll calls. But, critically, when the FCC rule was adopted the phone companies *already retained* the long-distance calling records for their own billing purposes, so the FCC mandate did not create any major new burdens on those providers. ISPs and other ECS providers, in contrast, have no similar reason to create these systems, and thus H.R. 1981 would create a vast new unfunded federal mandate on large and small businesses.

Finally, in Europe – where the Data Retention Directive requires that providers retain all sorts of data for a 6-24 month period – studies have made clear that the usefulness of retained data for law enforcement investigations falls off sharply after six months and again after twelve months. There has been significant discussion in Europe about reducing the permitted retention period to six months. It's also worth noting that many European countries and courts are backing away from the Data Retention Directive entirely. At least three national courts (in Germany, Romania, and the Czech Republic) have struck down their national data retention mandates on constitutional or human rights grounds, making the future of data retention in Europe unclear.

7. Data retention mandates will not help law enforcement investigate and prosecute more child pornography cases.

At present, data *preservation* – which is already part of the law – remains an appropriate alternative to data retention. 18 U.S.C. 2703(f) already requires ECS and RCS providers, upon request of a government entity and without any judicial intervention, to preserve all records or other evidence – including temporarily assigned network addresses – in their possession for renewable 90-day periods. In the child pornography context, data preservation is automatic in cases where service providers report possible child pornography to the National Center for Missing and Exploited Children (NCMEC). Although data preservation may not be useful in every case, it allows law enforcement to focus surveillance on those individuals who have been targeted for investigation, rather than putting at risk the privacy of all Americans.

Moreover, it is clear that law enforcement agencies already have far more child pornography cases on their plates than they can investigate and prosecute. In other words, even if a vast data retention regime were imposed on American ISPs, and even if data were retained for a lengthy period of time, law enforcement agencies would still not be able to investigate and prosecute more child pornography cases. Although in 2008 Congress recognized the need for more resources (authorizing for appropriation an additional $300 million over five years), none of those funds has been appropriated. In light of the continuing critical lack of resources to prosecute child pornography cases, and the significant problems raised by

data retention, we believe Congress should not impose these new costs on ISPs and small businesses to implement a data retention regime.

We appreciate your consideration of the above points. To discuss these issues and concerns further, please contact John Morris (jmorris@cdt.org), Greg Nojeim (gnojeim@cdt.org) or Erica Newland (enewland@cdt.org) by e-mail or at 202-637-9800.