The NetChoice Coalition
Promoting Convenience, Choice, and Commerce on The Net

Steve DelBianco, Executive Director
1401 K St NW, Suite 502
Washington, DC 20005
202-420-7482
www.netchoice.org

October 13, 2011

Honorable Eric Cantor
H-329, The Capitol
House of Representatives
101 Independence Ave SE
Washington, DC 20540

RE: **Opposition to HR 1981, Federal Data Retention Mandate**

Dear Majority Leader Cantor:

NetChoice opposes HR 1981 which forces ISPs to create and retain an evidentiary trail for all Americans who pay to access the Internet so that the government can investigate users' online activities – often without a warrant or court ordered subpoena. This raises serious privacy concerns for customers of paid Internet services while failing to achieve its main purpose of protecting children.

HR 1981 Creates a Real Threat to American Privacy

Under HR 1981, every time a user accesses the Internet, whether at home, in a hotel, in a coffee shop, or anywhere they use their smartphone, a unique IP address is assigned in order to connect that user to the web. HR 1981 requires companies providing paid Internet access to retain a record of each IP address linked to the identity of that customer for the past 18 months.

Dangers of HR 1981

- Creates Threat to American Privacy
  - Government Tracking of Honest Americans
  - Misuse of Data in Lawsuits
  - Misuse of Data by Criminals
- Undermines Federal and Congressional Privacy Initiatives
- Leaves Large Loopholes for Criminals
- ISPs Already Work with Law Enforcement to Protect Children

Government Tracking of Honest Americans

This bill would enable the government to find out where an American is every time an American checks their email, goes online with their smartphone, or pays to access the Internet in a hotel room or airport. It would enable the government to identify if an American visited a website and where and when they traveled for the past year. Forcing companies to store this for government uses opposes the goals of the 4th and 5th Amendments to the Constitution: preventing the government from unlawful searches of citizens.

Misuse of Data in Lawsuits

The information HR 1981 requires ISPs to collect could be misused in lawsuits. Attorneys could subpoena this information to build their cases. Picture the attorney in a divorce or a child custody case that subpoenas this information to discover the opponent's location information.

Misuse of Data by Criminals

This repository of IP addresses with customer IDs creates a honey pot of consumer information that is susceptible to misuse. This misuse could occur through a data breach, employee theft, and discovery for litigation. Data breaches appear to be increasingly frequent and having all this user information stored in a few locations makes a very tempting target for criminals.

Undermines Federal and Congressional Privacy Initiatives

The Federal Trade Commission and the Department of Commerce have espoused the need for consumer choice in the tracking of their information. This need for consumer choice is repeated by House Representatives Bono-Mack, Markey, Rush, Stearns, and Speier as well as Senators Kerry, Leahy, McCain, and Rockefeller.

And today most Internet companies and web browsers already allow their customers to opt-out of having their web-surfing information tracked or stored. These policies recognize the consumer's right to maintain control over their information and are an important tool in securing user trust.

But HR 1981 would prevent these efforts to increase consumer choice by forcing ISPs to track their customers. By forcing ISPs to retain these IP addresses the law would prohibit anonymous Internet browsing and undermine current government efforts to increase online privacy for Americans.

Leaves a Large Loophole for Criminals

HR 1981 makes a distinction between free and paid services, requiring only the latter to retain data. This leaves a loophole for criminals to engage in their bad behavior without being tracked by HR 1981. Since HR 1981 does not mandate IP address retention for free Internet access available at coffee shops, hotels, and municipal Wi-Fi networks, if a criminal wants to skirt HR 1981, they need only go grab a cup of coffee.

In essence, HR 1981 creates an unwatched back alley for criminals using free Internet access while placing honest paying Americans under surveillance.

ISPs Already Work with Law Enforcement to Protect Children

Existing efforts already achieve the goals of HR 1981. Presently, when an ISP reports a tip to the National Center for Missing and Exploited Children (NCMEC), the ISP automatically preserves all of the online evidence law enforcement will need to pursue the case. Further, current Data Preservation laws require all Internet services (both free and paid) to preserve all data pertaining to a customer when approached by law enforcement. This provides police with

time to gather additional evidence and secure the necessary court orders (like a warrant) to obtain the evidence.

Moreover, when tracking illegal internet activity today, law enforcement is ten times more likely to ask ISPs for the person behind an email address or chat name, as opposed to an IP address used to post something to a public website. ISPs already comply with these requests from law enforcement, and will start preserving a user's IP connectivity logs whenever law enforcement makes a specific request. These processes more accurately represents our justice system, where data is only collected on a potential criminal when they are *suspected* of a crime, rather than, under HR 1981, where data is gathered on all Americans *in case* they become a suspect in a crime.

Existing efforts are effectively protecting children. Free and paid Internet services have a strong and effective working relationship with law enforcement. On a weekly basis, the NCMEC receives around 3,500 tips on potential online child predation – to date it has received 1,015,252. Today, law enforcement does not have the resources to keep up with the current volume of evidence being provided to them by ISPs. This existing working relationship obfuscates the need for additional laws that will complicate this working process.

HR 1981 Threatens American Privacy and Undermines Congressional and Federal Privacy Efforts

HR 1981 will only threaten the privacy of Americans while undermining current Congressional and Federal privacy efforts. Worst of all, the loopholes in HR 1981 leave a back alley for criminals, free of government oversight, while placing honest Americans under the scrutiny of the government.

Thank you for considering our views and please let me know if we can provide further information.

Sincerely,

Steve DelBianco
Executive Director, NetChoice
cc: Members of the House Majority

NetChoice is a coalition of trade associations and e-Commerce businesses who share the goal of promoting convenience, choice and commerce on the Net. More information about NetChoice can be found at www.netchoice.org