TECHFREEDOM DigitalLiberty CEI Competitive Enterprise Institute

The Honorable Lamar Smith
2138 Rayburn House Office Building
U.S. House of Representatives
Committee on the Judiciary
Washington, D.C. 20515

The Honorable John Conyers, Jr.
2426 Rayburn House Office Building
U.S. House of Representatives
Committee on the Judiciary
Washington, D.C. 20515

Dear Chairman Smith and Ranking Member Conyers:

As public interest groups dedicated to free enterprise and constitutionally limited government, we write to members of the United States House of Representatives Committee on the Judiciary to express our serious concerns to regarding H.R. 1981, a bill that would impose a broad data retention mandate on all U.S. commercial Internet service providers (ISPs). The legislation, while well-intentioned, would burden small businesses, hinder innovation, undermine cybersecurity, endanger free speech, harm Americans' privacy and set a dangerous international precedent—all without appreciably advancing law enforcement objectives or benefiting criminal investigations.

H.R. 1981, as modified by the recent managers' amendment, would require all providers of commercial Internet access to collect and store Internet Protocol address assignment data (the unique identifier assigned to computers and other devices connected to the Internet) on all customers for at least one year. This mandate would impact an extraordinarily broad array of businesses of all sizes that offer Internet service to the public for a fee. Americans access the Internet not only at home but also at coffee shops, hotels, restaurants, offices, and at numerous other venues. Requiring all firms that sell Internet access to log temporary network address data as prescribed in the legislation would impose substantial costs. As with all burdensome regulations on the private sector, consumers themselves ultimately bear most of the costs incurred by companies in complying with the data retention mandate. Thus, the bill would directly hinder Congress's laudable objective of promoting the deployment and adoption of broadband at a time when many Americans are struggling to make ends meet. Lawmakers should be working aggressively to remove burdensome regulations on Internet service providers, rather than creating costly new mandates.

Retaining IP address assignment data—something many wireline ISPs currently do voluntarily—simply is not technically feasible for many providers given their network configurations. In particular, many wireless ISPs are not designed in a manner that lends itself to data retention. Although H.R. 1981 provides a six-month grace period for providers that currently lack the technical capacity to retain addresses, the bill does nothing to mitigate the significant costs that thousands of providers will face in redesigning their networks and purchasing expensive equipment to comply with the retention mandate. While the bill initially exempted wireless providers, that exemption was removed by managers' amendment.

Promoting global Internet freedom is a top priority of the State Department. H.R. 1981, however, follows in the footsteps of repressive governments such as China, which recently enacted a similar retention mandate covering wireless Internet service providers to facilitate its suppression of dissidents. America should take the moral high ground: citizens are innocent until proven guilty. A blanket mandate requiring providers to retain network address information pertaining to *all* citizens—the vast majority of whom have never been charged with a criminal offense—amounts to a "digital dragnet" of staggering proportions. It violates the constitutional rights of the innocent to due process and anonymous expression.

The bill would also create significant new security threats for Internet service providers and their users. Providers currently face mounting threats from hackers and other cyber-criminals, and spend enormous resources on cybersecurity. A data retention mandate would vastly expand the quantity of information collected and stored by Internet providers, painting a giant bulls-eye on the many service providers that do not currently collect or store sensitive consumer data. Cyber-attacks originating in China have already exploited similar vulnerabilities in U.S.-based online services stemming from congressional mandates. H.R. 1981 would make it easier for the Chinese government to suppress dissidents who use U.S.-based tools to circumvent China's "Great Firewall"—the very tools the State Department is promoting heavily.

H.R. 1981's unintended consequences might be worth the cost if the bill were actually likely to further its stated objective of keeping children safe from predators. However, an extensive body of empirical evidence, including the experiences of other nations in which similar laws have been enacted, strongly suggests that H.R. 1981 is not likely to result in any appreciable decrease in crimes committed against children. In 2006, the European Union instituted a Data Retention Directive requiring member states to pass compliant laws to combat terrorism and crime. However, there is little evidence the mandate has been effective. A 2011 analysis of German federal crime statistics, for instance, found that data retention mandates did nothing to help solve crimes. Even the European Data Protection Supervisor, the official EU watchdog responsible for ensuring that government bodies respect citizens' privacy, concluded in May 2011 that no sufficient justification exists for the EU's broad and disproportionate mandate.

Congress is rightly concerned about the horrific crime of child exploitation, but the proper response to such concerns is a narrowly-tailored approach that preserves Internet freedom and minimizes burdens on the private sector while enabling law enforcement to bring child predators to justice. Congress should start by giving the Department of Justice the funding it needs to complete the study it was required to produce nearly two years ago identifying the "factors indicating whether the subject of an online investigation poses a high risk of harm to children." In general, Congress should ask whether law enforcement has the funding it needs to prosecute child exploitation effectively and strengthen penalties for such heinous crimes.

Sincerely,

Competitive Enterprise Institute (www.cei.org)

TechFreedom (www.techfreedom.org)

Americans for Tax Reform's Digital Liberty (www.digitalliberty.net)