Majority Leader Mitch McConnell
Minority Leader Harry Reid
United States Senate

Chairman Richard Burr
Vice Chairman Dianne Feinstein
Select Committee on Intelligence
United States Senate

Chairman Charles Grassley
Ranking Member Patrick Leahy
Committee on the Judiciary
United States Senate

4 August 2015

We the undersigned human rights and civil liberties organizations and trade associations write to convey our significant concerns with a provision in the Intelligence Authorization Act for Fiscal Year 2016 (S. 1705). Section 603 of the Act would require all providers of Internet communications services to report to government authorities when they obtain "actual knowledge" of apparent "terrorist activity" on their services—a broad term that could encompass both speech and conduct.

Unfortunately, this provision would create strong incentives for providers to over-report on the activity and communications of their users, in order to avoid violating the law. This provision risks bringing wholly innocent people under the scrutiny of the U.S. government in a procedure that includes no limits on the use of the reported information and no safeguards against abuse. Such a reporting requirement would create a chilling effect on constitutionally protected speech and would impermissibly burden individuals' First and Fourth Amendment rights. Further, online service providers are already permitted under law to make voluntary reports to law enforcement in emergency circumstances and when a communication appears to pertain to the commission of a crime.[1]

We understand the serious concerns that motivate this provision; however, the reporting obligation described in Section 603 has several fundamental flaws:

Section 603 creates a vague obligation that would likely lead to significant over-reporting by providers. The provision would require providers to report apparent "terrorist activity," an undefined but potentially very broad category of speech and conduct. This vague requirement would leave providers uncertain as to the content or other activity that would trigger this obligation. Electronic communication service providers, which include user-generated content hosts, cloud services, Internet service providers, [and others] support online expression and exchange of information that is "as diverse as human thought"[2] – a diversity that makes it incredibly difficult, if not impossible, for a provider to accurately judge the context of every communication, or the intent of every speaker, whose speech touches its service. Whether a given comment is a true threat of violence, an expression of a sincerely held religious belief, or a simply joke among friends is a determination that providers are ill-suited to make, particularly when the consequence is reporting a person to the government under the suspicion of involvement in terrorist

[1] 18 U.S.C. § 2702(b)(7)-(8).
[2] Reno v. ACLU, 521 U.S. 844, 852 (1997).

activities. Providers who obtain actual knowledge of the content of communications and other activity on their services will face a strong incentive to report a broad range of content and exchanges in order to remain in compliance with the law, potentially bringing an unnecessarily large number of innocent individuals under heightened government scrutiny. The potential for this scrutiny will unavoidably exert a chilling effect on protected speech and will burden individuals' First Amendment rights to speak and to access information.

Providers would be required to report the content of private communications directly to the government. Section 603 would require providers to submit the "facts and circumstances" associated with alleged terrorist activity to "appropriate authorities" to be designated by the Attorney General. Undoubtedly, the "facts and circumstances" in some cases will include the contents of private communications – emails, private messages on social media, files and photos stored on cloud services – which law enforcement would ordinarily be required to obtain a warrant to access. If Section 603 thus requires operators to turn over such communications to the government, it would conflict with existing protections for individual privacy in the Electronic Communications Privacy Act and under the Fourth Amendment. Further, there are no limitations in the provision regarding what may be done with the information in the provider's report, creating the prospect that people's personal information and communications would be stored in a government database, linked to suspicion of involvement in terrorist activity, in perpetuity. Nor does Section 603 include any provision for providing notice to reported users, meaning that individuals who come under government scrutiny for involvement in "terrorist activity" would have no opportunity to contest these allegations to the government.

Section 603 would damage user trust in U.S.-based businesses on a global scale. By creating a broad reporting obligation on online service providers subject to U.S. jurisdiction, this provision will impair the ability of U.S.-based businesses to provide services to users in the U.S. and abroad. Trust in U.S. providers was damaged around the world after revelations of the vast scope of the surveillance conducted by U.S. intelligence agencies. Many providers have worked diligently in the intervening years to regain their users' confidence in the privacy and security of their services. These efforts would be thoroughly undermined by the creation of a new obligation on these providers to inform on their users directly to the U.S. government based on an undefined set of criteria and with no protections for users' rights. Moreover, for providers who operate online communications services such as social media, email, or instant messaging services, it will be trivial for their users – in the U.S. and overseas – to leave their service for a competitor who is not subject to U.S. jurisdiction.

Section 603 will be ineffective. The reporting requirement in Section 603 is likely to be ineffective for a number of reasons. Cautious providers who over-report would contribute an unmanageable glut of false leads and inaccurate reports that would waste law enforcement resources to assess. Bad actors, along with wholly innocent users concerned about their privacy, can switch to "offshore" services that are not subject to Section 603's reporting obligation.

It is also not clear that the reporting mandate in Section 603 is necessary. Providers already may report evidence of the commission of a crime to law enforcement. Under the

Electronic Communications Privacy Act, a provider may voluntarily disclose the content of communications to law enforcement if the provider inadvertently becomes aware of the content and believes it to pertain to the commission of a crime.[3] ECPA further permits the reporting of communications content to a governmental entity if the provider has a good-faith belief that it is necessary to do so in an emergency situation.[4]

Section 603's reporting requirement threatens individuals' constitutional rights to privacy and freedom of expression and would burden U.S.-based providers without providing a clear benefit to law enforcement. For these reasons, we urge you to reject this flawed provision and to remove it from the Intelligence Authorization Act.

Signed,

American Civil Liberties Union
American Library Association
Association of Research Libraries
Bill of Rights Defense Committee
Campaign for Liberty
Center for Democracy & Technology
Center for Financial Privacy and Human Rights
Computer & Communications Industry Association
The Constitution Project
Constitutional Alliance
Consumer Action
Consumer Federation of America
Consumer Watchdog
Defending Dissent Foundation
Distributed Computing Industry Association
Electronic Frontier Foundation
Fight for the Future
FreedomWorks
Global Network Initiative
Human Rights Watch
Internet Infrastructure Coalition
National Association of Criminal Defense Lawyers
NetChoice
New America's Open Technology Institute
Project Censored/Media Freedom Foundation
Restore the Fourth
RootsAction.org
Software & Information Industry Association
TechFreedom
TechNet
X-Lab

[3] 18 U.S.C. § 2702(b)(7).
[4] 18 U.S.C. § 2702(b)(8).