April 19, 2016

The Honorable Richard Burr
Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20515

The Honorable Dianne Feinstein
Vice-Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20515

Dear Chairman Burr and Vice-Chairman Feinstein:

We write to express our deep concerns about well-intentioned but ultimately unworkable policies around encryption that would weaken the very defenses we need to protect us from people who want to cause economic and physical harm. We believe it is critical to the safety of the nation's, and the world's, information technology infrastructure for us all to avoid actions that will create government-mandated security vulnerabilities in our encryption systems.

As member companies whose innovations help to drive the success and growth of the digital economy, we understand the need to protect our users' physical safety and the safety of their most private information. To serve both these interests, we adhere to two basic principles. First, we respond expeditiously to legal process and emergency requests for data from government agencies. Second, we design our systems and devices to include a variety of network- and device-based features, including but not limited to strong encryption. We do these things to protect users' digital security in the face of threats from both criminals and governments.

Any mandatory decryption requirement, such as that included in the discussion draft of the bill that you authored, will to lead to unintended consequences. The effect of such a requirement will force companies to prioritize government access over other considerations, including digital security. As a result, when designing products or services, technology companies could be forced to make decisions that would create opportunities for exploitation by bad actors seeking to harm our customers and whom we all want to stop. The bill would force those providing digital communication and storage to ensure that digital data can be obtained in "intelligible" form by the government, pursuant to a court order. This mandate would mean that when a company or

user has decided to use some encryption technologies, those technologies will have to be built to allow some third party to potentially have access. This access could, in turn, be exploited by bad actors.

It is also important to remember that such a technological mandate fails to account for the global nature of today's technology. For example, no accessibility requirement can be limited to U.S. law enforcement; once it is required by the U.S., other governments will surely follow. In addition, the U.S. has no monopoly on these security measures. A law passed by Congress trying to restrict the use of data security measures will not prevent their use. It will only serve to push users to non-U.S. companies, in turn undermining the global competitiveness of the technology industry in the U.S. and resulting in more and more data being stored in other countries.

We support making sure that law enforcement has the legal authorities, resources, and training it needs to solve crime, prevent terrorism, and protect the public. However, those things must be carefully balanced to preserve our customers' security and digital information. We are ready and willing to engage in dialogue about how to strike that balance, but remain concerned about efforts to prioritize one type of security over all others in a way that leads to unintended, negative consequences for the safety of our networks and our customers

Signed,

Reform Government Surveillance

Computer & Communications Industry Association

Internet Infrastructure Coalition (I2C)

The Entertainment Software Association