



July 8, 2015

The Honorable Charles E. Grassley
Chairman
U.S. Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Richard Burr
Chairman
U.S. Senate Select Committee on Intelligence
221 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Patrick J. Leahy
Ranking Member
U.S. Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Dianne Feinstein
Vice Chairman
U.S. Senate Select Committee on Intelligence
221 Hart Senate Office Building
Washington, D.C. 20510

Dear Chairman Grassley, Chairman Burr, Ranking Member Leahy, and Vice Chairman Feinstein:

On behalf of BSA | The Software Alliance¹ (BSA), I write to express our appreciation for both the U.S. Senate Committee on the Judiciary and the U.S. Senate Select Committee on Intelligence holding hearings today on the issues of encryption, technology, and the legitimate roles of law enforcement and security agencies. We believe these hearings will foster a constructive public dialogue about these important topics, which are a crucial concern to the technology companies BSA represents, their customers at home and abroad, and government agencies charged with protecting our security.

This letter provides the perspective of BSA members—companies that develop and offer essential software, security tools, communications devices, servers, and computers that drive the American and global information economy, and that improve our daily lives.

Today's consumers use technology and store massive amounts of personal information and highly sensitive business information in dramatic new ways. A safe and secure data storage system is critical to all of our daily lives. The data stored with technology companies often is highly personal—and users rightly view it as their own. The data a single user stores with a technology provider can display the sum of her private life. Anyone with access to that data would be able to recreate her movements, her communications, her purchases, and even her thoughts, as revealed, for example, in her web queries. While many of our laws are designed to protect the sanctity of the information an individual secrets inside her home, individuals may consider the data they store with technology companies as being even more sensitive.

BSA members earn users' trust by providing essential security technologies that protect users against cyber threats. That is why BSA members create, develop, and deploy products and services that incorporate robust security measures in response to our users' demands. These security measures include the encryption of data both at rest and in transit, including user-controlled encryption features.

¹ BSA's members include: Adobe, Altium, Apple, ANSYS, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, Datastax, Dell, IBM, Intuit, Microsoft, Minitab, Oracle, salesforce.com, Siemens PLM Software, Symantec, Tekla, The MathWorks, and Trend Micro.

Those features put control in the hands of the user, and in so doing help increase both security and user trust.

Our member companies are fully committed to the important mission of law enforcement in keeping Americans safe and investigating criminal activity and stand ready to do their part. At the same time, companies need both clarity about their obligations and the freedom to innovate to meet users' demands.

Our goal is to ensure our users' information remains truly private and out of the hands of bad actors. To achieve this goal, we need safeguards that responsibilities imposed on technology companies do not endanger the security of our users' information, or network security more broadly.

Some have proposed solutions that would limit the use of security technologies, build in flaws, or dictate design and capabilities by requiring master encryption keys. Unfortunately, these are not real solutions. Rather, they are recipes for further problems. Such proposals would actually undermine the effectiveness of the security tools we use to keep our users' information safe and secure. These proposals would weaken our ability to protect users' information from cybercriminals, undermine the viability of information tools, and harm the consumer trust equation. Importantly, requiring technology that provides law enforcement access to information also risks undermining the security of all electronic communications and digitally stored information. Put simply, proposals to require a "back door" into encrypted information would leave users more vulnerable to cybercrimes.

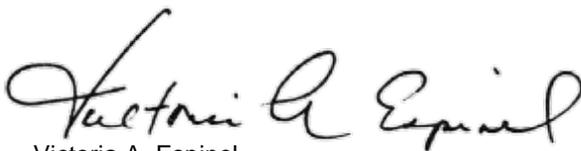
Calls for the weakening of encryption controls may also have international repercussions, which would further degrade many security measures protecting U.S. consumers. It is a reality that national borders do not limit threats to our citizens. Criminals, terrorists and other determined actors from around the world pose real and immediate threats to our safety and security. Other countries pay close attention to obligations that the U.S. government places on U.S. technology companies operating in the global marketplace. Internationally, calls for weakened encryption embolden some regimes to leverage similar policies, which put at risk fundamental human rights and can create artificial commercial disadvantages for U.S. companies and barriers to market access. We need to ensure that we can support any new standards adopted in the U.S. if other countries adopted the same standards. While we may have faith that U.S. law enforcement will responsibly exercise its discretion under any new authorities, we must be conscious that other countries may adopt the same standard and yet exercise their discretion quite differently.

Consumers use devices and cloud services to create and store personal data in a way that was hardly contemplated just a few years ago. Electronically stored information often is even more intimate and sensitive than physical records individuals would have stored in their homes or businesses at the turn of the century. Their expectation of privacy and security in digital information has, rightly, grown along with its prevalence.

Responsible technology providers want to assist law enforcement in legitimate investigations, in ways that are consistent with protecting consumer privacy and the security of the network and provide ample breathing room for innovation and meeting legitimate customers' needs.

We very much look forward to working with you, the law enforcement community and relevant stakeholders.

Sincerely,



Victoria A. Espinel
President and CEO