



805 15th Street, NW, Suite 708, Washington, D.C. 20005
Telephone 202.650.5100 | Fax 202.650.5118
www.technet.org | @TechNetUpdate

April 19, 2016

The Honorable Tim Murphy
Chairman
Oversight and Investigations Subcommittee
House Energy and Commerce Committee
Washington, D.C. 20515

The Honorable Diana DeGette
Ranking Member
Oversight and Investigations Subcommittee
House Energy and Commerce Committee
Washington, D.C. 20515

Dear Chairman Murphy and Ranking Member DeGette,

TechNet, the national, bipartisan network of innovation economy CEOs and senior executives, thanks you for holding today's hearing, "Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives."

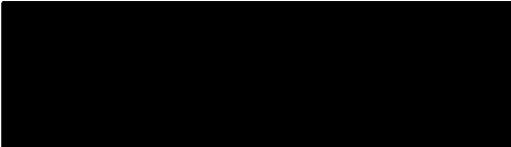
As the debate on encryption continues, we urge the committee to recognize that strong encryption is a commercial necessity that underpins millions of daily transactions and allows companies to safely store and move sensitive information. We have concerns over calls for weakened encryption and the privacy, security, economic, and competitive implications of these actions.

We are pleased that the committee has put together an expert discussion that can consider the legitimate rights and needs of consumers, businesses, governments, and the American economy. Our smartphones, and the other devices that we depend on, are essential parts of our lives. They hold our most personal information, including our health and financial data. This information needs to be protected from those who would seek to compromise our privacy and security.

At TechNet, we have great respect for the job that the FBI and other law enforcement agencies do. We fully understand that our nation faces grave threats and that we must be vigilant in protecting our homeland. Tech companies often work with law enforcement to provide expeditious access to data that companies possess through a valid legal process and emergency requests.

The challenge facing many technology companies, and now Congress, is that when a company does not have access to data, new legal requirements to create access points could force companies to eliminate security features from their products that would be counterproductive for both our nation's security and economic leadership. From a security perspective, once a vulnerability is established, it could be exploited by others who do not share the FBI's good intentions. The result: common transactions will become easy prey for bad actors, and customers around the world could lose faith in the trustworthiness of American products and choose alternatives that don't have the same vulnerabilities.

We appreciate the time that the Committee is taking to bring these issues to the public. We hope that the hearing will address the value of encryption and serve as a catalyst for a dialogue to chart a way forward on the complicated set of legal and technical issues surrounding encryption. TechNet is committed to finding balanced solutions that protect the safety and privacy of our citizens without damaging public trust, undermining security, and hindering economic growth and job creation. We are willing to work with Congress to achieve to these goals.



Linda Moore
President and CEO