June 1, 2015

James Comey
Director
Federal Bureau of Investigation
United States Department of Justice
604 4th Street NW
Washington, DC 20035

Dear Director Comey,

We appreciate the Federal Bureau of Investigation's (FBI) hard work and dedication to keeping Americans safe and secure. Thank you for having Assistant Director Amy Hess testify before the House Committee on Oversight and Government Reform's Subcommittee on Information Technology (IT) during a hearing titled "Encryption Technology and Potential U.S. Policy Responses." As Members on the Committee with computer science degrees, we found the testimony both enlightening and troubling.

Democracy will always have to strike a balance between security and liberty. While we recognize the challenging role of law enforcement in helping to strike that balance, we strongly, but respectfully, disagree with the FBI's proposal to force private sector companies to weaken the security of their products and services by creating a "backdoor" that allows law enforcement to circumvent encryption technology. There are at least three reasons why the FBI and other federal agencies should not pursue this proposal.

First, the FBI's proposal would be a change in the relationship between our government, our citizens, and our private sector. While we recognize that there is a role for the private sector in cooperating with law enforcement to address security threats, this is not the best or most effective way. There is a difference between private companies assisting law enforcement and the government compelling companies to weaken their products to make investigations easier.

Second, any vulnerability to encryption or security technology that can be accessed by law enforcement is one that can be exploited by bad actors such as criminals, spies, and those engaged in economic espionage. It is important to remember that computer code and encryption algorithms are neutral and have no idea if they are being accessed by an FBI Agent, a terrorist or a hacker. During our oversight hearing, it was clear that none of the witnesses were willing to assert that a backdoor would be completely air-tight and secure. Moreover, demanding special access also opens the door for other governments with fewer civil liberties protections to demand similar backdoors.

Finally, it is our belief that backdoors can be easily circumvented by terrorists and criminals who can purchase outside encryption applications or communications devices from foreign manufacturers who do not have to follow U.S. law. While we certainly understand the FBI's concerns about this encryption technology, we do not believe that the American private sector should simply stifle its innovation.

As computer science majors and members of the IT Subcommittee, we strongly urge the FBI to find alternative ways of addressing the challenges posed by new technologies.

Sincerely,

WILL HURD
Chairman
House Oversight and Government Reform
Subcommittee on Information Technology

TED W. LIEU
Member
House Oversight and Government Reform
Subcommittee on Information Technology

cc:

Rep. Jason Chaffetz, Chairman, House Oversight and Government Reform Committee
Rep. Elijah Cummings, Ranking Member, House Oversight and Government Reform Committee
Rep. Robin Kelly, Ranking Member, House Oversight and Government Reform Subcommittee on Information Technology
Rep. Blake Farenthold, Member, House Oversight and Government Reform Subcommittee on Information Technology
Rep. Gerald E. Connolly, Member, House Oversight and Government Reform Subcommittee on Information Technology
Rep. Mark Walker, Member, House Oversight and Government Reform Subcommittee on Information Technology
Rep. Paul Gosar, Member, House Oversight and Government Reform Subcommittee on Information Technology
Rep. Tammy Duckworth, Member, House Oversight and Government Reform Subcommittee on Information Technology
Rep. Rod Blum, Member, House Oversight and Government Reform Subcommittee on Information Technology