

CHARLES E. GRASSLEY, IOWA, CHAIRMAN

ORRIN G. HATCH, UTAH  
JEFF SESSIONS, ALABAMA  
LINDSEY O. GRAHAM, SOUTH CAROLINA  
JOHN CORNYN, TEXAS  
MICHAEL S. LEE, UTAH  
TED CRUZ, TEXAS  
JEFF FLAKE, ARIZONA  
DAVID VITTER, LOUISIANA  
DAVID A. PERDUE, GEORGIA  
THOM TILLIS, NORTH CAROLINA

PATRICK J. LEAHY, VERMONT  
DIANNE FEINSTEIN, CALIFORNIA  
CHARLES E. SCHUMER, NEW YORK  
RICHARD J. DURBIN, ILLINOIS  
SHELDON WHITEHOUSE, RHODE ISLAND  
AMY KLOBUCHAR, MINNESOTA  
AL FRANKEN, MINNESOTA  
CHRISTOPHER A. COONS, DELAWARE  
RICHARD BLUMENTHAL, CONNECTICUT

## United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

KOLAN L. DAVIS, *Chief Counsel and Staff Director*

KRISTINE J. LUCIUS, *Democratic Chief Counsel and Staff Director*

February 16, 2016

### Via Electronic Transmission

The Honorable Sally Q. Yates  
Deputy Attorney General  
U.S. Department of Justice  
950 Pennsylvania Ave., NW  
Washington, DC 20530

The Honorable James B. Comey, Jr.  
Director  
Federal Bureau of Investigation  
935 Pennsylvania Ave., NW  
Washington, DC 20535

Dear Deputy Attorney General Yates and Director Comey:

I write today in response to your answers to my Questions for the Record (QFRs) from the Judiciary Committee's July 8, 2015 hearing entitled "Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy." At that hearing, you both testified about the public safety threat resulting from widespread inviolable encryption. Various senators expressed similar concerns about the problem, but numerous experts and outside commentators have also noted the benefits of encryption and raised issues with advancing legislative solutions.

Your recent QFR responses appear to indicate that this problem may be getting worse. For instance, Director Comey stated that as a consequence of widespread encryption, "the data on the vast majority of the devices seized in the United States may no longer be accessible to law enforcement even with a court order or search warrant." On February 9, 2016, Director Comey highlighted an example of this problem when he testified before the Select Committee on Intelligence that a cellular telephone from one of the terrorists who killed 14 people in San Bernardino, California in December 2015 remains encrypted today. Moreover, as Director Comey referenced in response to another QFR, Apple Inc. is now claiming that complying with court orders – even when it has the technical

capability to do so and has regularly done so in the past – “would cause reputational harm.”

Nevertheless, I have yet to see any concrete progress on the Going Dark problem from the Obama Administration. When pressed for solutions at the July 8 hearing, Deputy Attorney General Yates stated that the Administration intended to pursue a collaborative and cooperative approach with technology providers. She further stated in response to my QFRs that “[t]he Department of Justice continues to work with companies and industry groups to address these issues, and those efforts have intensified in the last few months.” But at the same time, the Department of Justice (DOJ) has been unwilling to establish a deadline or timetable to assess the effectiveness of its case-by-case approach. Deputy Attorney General Yates’s QFR response in fact stated both that “we do not have a deadline in mind for any particular action” and “[t]he Administration is not seeking legislation at this time” to address the problem. Such statements only reinforce the concerns I set forth in a letter to the Department dated October 8, 2015, which cited two *Washington Post* articles from September of last year casting doubt on the Administration’s commitment to address this problem. And, as noted above, the Administration’s current posture appears to have encouraged at least one technology provider to go out of its way to refuse to assist law enforcement even in circumstances where it once helped to provide lawful access to encrypted devices in response to court orders.

In order to better understand and assess this problem, Congress needs accurate information. This was a point on which there was bipartisan agreement at our hearing in July. But here your responses to my QFRs are woefully inadequate. In order to more fully understand the nature and scope of this problem, I submitted questions that called for specific information from DOJ and the FBI about the providers that have refused to comply with court orders. I also explained the importance of the Administration providing Congress with any and all quantitative data on the Going Dark problem – including all available statistical data concerning the impact of encryption on access to both “data-in-motion” and “data-at-rest.” But rather than providing specific information and quantitative data, your QFR responses merely indicate that DOJ and the FBI are “improving enterprise-wide quantitative data collection” to “improve and streamline data collection metrics.” Yet your responses imply that some data has already been or can readily be collected and that information related to the “data-at-rest” problem is readily available.

I therefore request that DOJ and FBI immediately provide any and all currently available quantitative data concerning the scope and impact of encryption on both the “data-in-motion” and “data-at-rest” problems. Congress and the American people need this information to understand the effect of widespread inviolable

encryption on the government's ability to investigate and prosecute criminal offenses and to prevent terrorist attacks. In addition, Congress and the American people have a right to know whether any providers have changed their mind as a result of the Administration's strategy of engaging companies and industry groups directly. Therefore, please provide a list of all the providers that the Administration has approached since July 2015 pursuant to this strategy, and identify whether each one has responded and in what way.

As I have stated before, I strongly believe that the Administration should use every lawful tool at its disposal and vigorously investigate each and every potential solution to this serious issue. Members of the Committee have offered their support and personal assistance in your ongoing efforts with technology providers, and I ask to continue to be regularly advised – quarterly, at a minimum – of the status of those negotiations. I understand that any single solution – including any single legislative solution – to this problem may be imperfect. But I request that the Administration keep Congress apprised of any progress, or lack thereof, in its efforts to maintain its ability to execute lawful, court-authorized investigative techniques, such as warrants and wiretaps, which are essential to enforcing the rule of law and protecting the American people.

Sincerely,



Charles E. Grassley  
Chairman