JASON CHAFFETZ, UTAH
CHAIRMAN

ONE HUNDRED FOURTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
MINORITY (202) 225–5051

http://oversight.house.gov

Opening Statement
Rep. Robin Kelly, Ranking Member

Subcommittee on Information Technology
Hearing on "Encryption Technology and Potential U.S. Policy Responses"

April 29, 2015

Thank you, Mr. Chairman and thank you to our witnesses for appearing on today's panel.

Recently companies, like Apple and Google, have announced plans to incorporate automatic encryption for their mobile devices.

Encryption will become the default privacy feature on their mobile devices, making their content unreadable and inaccessible without the user selected passcode.

As a society, we rely on mobile devices to manage and protect many aspects of our lives—personal, professional, and financial. Privacy on our smartphones is critically important. Hackers are a concern, as is unrestricted government surveillance.

According to a May 2014 study on trends in the U.S. smartphone industry, Android and Apple control 52.1% and 41.9% share of the market. Their move towards automatic encryption will have a significant effect on the industry standard for privacy protections.

The move toward automatic encryption has been criticized as seriously hindering law enforcement operations. Criminals, like non-criminals, use mobile devices to manage the many aspects of their lives, some of which can provide evidence of a crime.

Today, many criminal cases have a digital component and law enforcement entities increasingly rely on the contents of mobile devices to further an investigation or prosecution of serious crimes and national security threats.

The FBI, local law enforcement departments, and prosecutors, have all expressed concerns with automatic encryption. They envision a number of scenarios in which the inability to access data kept on mobile devices will seriously hinder a criminal investigation. They do not want to be in a position to tell a victim of a crime or the family of a victim that they cannot save someone or prosecute someone because they cannot access the content of a mobile device.

There is a balance to be struck here.

It is important that the government's policy approach ensures privacy protections, and it is important that law enforcement, under tightly controlled circumstances, have the ability to investigate and prosecute crimes. I look forward to hearing today's testimony.

Thank you, Mr. Chairman. I look forward to continue working with you to examine policy issues related to advancements in information technology.

Contact: Jennifer Hoffman, Communications Director, (202) 226-5181.