Senate Committee on the Judiciary
Responses to Questions for the Record from Senator Grassley
Washington, D.C.

Cyrus Vance, Jr., District Attorney, New York County, New York

---

Question 1: Correspondence with Apple and Google

In your written testimony and during the hearing, you spoke about your interactions with Apple and Google, and follow-up letters that you sent to these companies containing a series of detailed questions about the "Going Dark" issue.

a. **Please describe in further detail your interactions with these companies.**

b. **Have you received a response from either company? If so, please describe in detail the response. If not, have you contacted them about the timing of any response?**

c. **If and when you receive a response, would you please forward a copy to the Committee?**

Response to Question 1(a).

Given my deep concerns on the harm to local law enforcement caused by Apple's and Google's new policies that would render the information on smartphones effectively beyond the reach of search warrants, my Office contacted Apple and Google to set up separate meetings with each company. On March 19, 2015, I, along with two members of my Office, two representatives from the United States Secret Service, and two representatives from the

Alabama Office of Prosecution Services participated in separate meetings with Apple and Google at their headquarters in California.

The representatives from Apple who participated in the meeting included: i) Jane Horvath, Senior Director of Global Privacy; ii) Pat Burke, Privacy Counsel for Enforcement; iii) Cathy Foster, Corporate Government Affairs; and iv) Mike Foulkes, Director, State and Local Government Affairs. I shared my concerns about the impact of Apple's decision on my Office and other state and local law enforcement agencies, explaining that state and local law enforcement handles ninety percent of the criminal cases in the United States and that a huge percentage of them involve evidence derived from smartphones. I explained that the availability of information on the cloud is not an adequate substitute for information on smartphones for pursuing criminal investigations, exoneration efforts, or prosecutions.

Apple explained that its decisions regarding smartphone encryption were based principally on security and market considerations, with the latter relating in large part to growth in foreign markets. Apple offered that efforts by Congress or a state legislature that would cause United States-based technology companies to limit encryption in any way might cause those companies to re-locate outside of the United States.

Our second meeting was held with Google. The representatives from Google present at the meeting included: i) Kent Walker, Senior Vice President and General Counsel; ii) Richard Salgado, Legal Director, Law Enforcement and Information Security; iii) Nicole Jones, Sr. Law Enforcement and Security Counsel; iv) Betsy Masiello; and v) Eric Grosse. As we had done with Apple, we shared with Google our concerns about the impact on state and local law enforcement of policies that would render the information on smartphones

effectively beyond the reach of search warrants. As had Apple, Google raised concerns about how limits on encryption would be exploited by foreign governments, and noted that information on smartphones had been used by repressive governments to oppress human rights activists. Google also referred to harm to its "brand" allegedly caused by publicity surrounding activities of the National Security Agency.

On March 31, 2015, and April 1, 2015, I sent letters to Apple and Google, respectively, setting forth questions that arose from our meetings with them. I have attached a copy of both my letters. (Copies of the letters were also attached as exhibits to my written testimony before your Committee.) I had hoped that the letters would foster a dialogue, but neither company has responded. I remain hopeful that a dialogue and a solution are possible.

Response to Question 1(b).

As noted above, to date I have not received a response from either Apple or Google.

Response to Question 1(c).

I will promptly forward to the Committee a copy of any response to my letters should I receive one.

Question 2: Exonerations of the Innocent

In your testimony, you spoke about how the "Going Dark" problem seriously affects your ability to obtain evidence to prosecute criminals. Can you also describe how the "Going Dark" problem impacts law enforcement's ability to exclude individuals suspected of criminal wrongdoing or otherwise exonerate innocent people? Do you have any real-world examples of this?

Response to Question 2.

As you are aware, any evidence that helps us to prosecute criminals also helps us to exonerate the innocent, including the wrongly suspected or accused. A case from my office that illustrates the point arose when the police discovered a person dead in his apartment with a gunshot wound to the head.

My office obtained a search warrant and an "unlock order" from a court for certain phones found at the scene of the crime. We sent the phones to Apple, which unlocked them. The phone data helped to establish that what we had initially thought to be the timeline of the events was wrong, and that a person whom we had initially suspected had not, in fact, been involved. A contact in one of the unlocked iPhones was eventually traced to another individual, who later confessed and pled guilty to the killing. He is currently serving a sentence of 17 years and 6 months imprisonment. *People v. Rosario,* Indictment 01859/2010, New York State Sup