

November 18, 2015

Tim Cook, Chief Executive Officer  
Apple  
1 Infinite Loop  
Cupertino, CA 95014

Sundar Pichai, Chief Executive Officer  
Google Inc.  
1600 Amphitheater Parkway  
Mountain View, CA 94043

Dear Mr. Cook and Mr. Pichai,

We write to express our deep concern with the new encryption software installed on Apple and Android cell phones. Our foremost duty as State attorneys general, district attorneys, and law enforcement officers, is to protect the citizens we serve. Even with a valid search warrant, the current encryption measures utilized in your phones make it impossible to access evidence of a crime. Without law enforcement access to this vital information, you have created a safe harbor for criminals where they may operate freely, without fear of punishment, retribution, or consequence. Your encryption software puts the families we strive to protect at risk.

There are numerous examples where, but for the evidence recovered from a cell phone, a criminal conviction could not have been achieved. One such example is the Steubenville, Ohio rape cases which garnered national attention, due to the graphic nature of the crimes as depicted by evidence obtained from personal cell phones.

Ohio investigators confiscated and analyzed more than a dozen cell phones. The analysis uncovered hundreds of incriminating text messages and pictures, revealing beyond a reasonable doubt that an incapacitated high school girl was publicly sexually assaulted by her peers. Several witnesses documented various parts of the heinous acts on their personal cell phones and two young men discussed the acts on social media and through text messages. A text recovered from one of the perpetrators phones described the victim that night as "like a dead body." In another, the perpetrator texted the victim a photo on his phone depicting the victim lying naked, in a basement, incapacitated, and covered in what appeared to be bodily fluids. The perpetrator informed the victim that the picture was taken by him. But for the evidence recovered from personal cell phones, that high school girl and her family would likely never have seen justice served.

Additionally, the new Apple and Android encryption methods place our national security at risk. As FBI Director James B. Comey and Deputy Attorney General Sally Quillian Yates' joint statement to the Senate Judiciary Committee highlighted, "[t]hese encrypted direct messaging platforms are tremendously problematic when used by terrorist plotters. [W]e may not be able to identify and stop terrorists who are using social media to recruit, plan, and execute an attack in our country..." Tragically, Paris may have fallen victim to the concern expressed by Director Comey and Deputy Attorney General Yates. The Wall Street Journal reported that there is a "growing belief among intelligence officials that the terrorists behind Friday's Paris attacks used encrypted

communications” to aide in their terrorist attacks. Senator Richard Burr (R., N.C.) chairs the Senate Intelligence Committee and stated “[i]t is likely that end-to-end encryption was used to communicate in Belgium and France and Syria” because no direct communication among the terrorists was detected.

We respect the fundamental right of individuals to engage in private communications, regardless of the medium or technology. However, it is paramount to protect both the fundamental right of people to engage in such communication and, at the same time, protect the public from criminal actors. As Daniel F. Conley, Suffolk County (MA) District Attorney, stated to Congress, “when we talk about warrant-proof encryption, let’s be very clear who will benefit from it: perpetrators of every violent, sexual, or financial crime in which handheld technology is used.”

We urge you to reconsider the encryption technology you are utilizing and we would like to work with your respective organizations to develop a technology that both protects consumer privacy and allows law enforcement, with a valid search warrant, to gather crucial evidence. We invite you to work with us to find an acceptable technological middle-ground where both the fundamental right to private communications and the protection of all citizens from criminal actors are properly balanced.

Very respectfully yours,



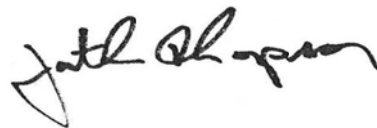
Mike DeWine  
Ohio Attorney General



William J. Fitzpatrick, President  
National District Attorneys Association



Reynaldo Tariche, President  
FBI Agents Association



Jonathan F. Thompson, Executive Director and CEO  
National Sheriffs’ Association

cc: Jane Horvath, Senior Director of Global Privacy, Apple  
Kent Walker, Senior Vice President and General Counsel, Google Inc.