Opinions

Apple and Google threaten public safety with default smartphone encryption

A customer holds an iPhone 6 on display at the Fifth Avenue Apple store on the first day of sales in Manhattan, New York September 19, 2014. (Adrees Latif/Reuters)

By Cyrus R. Vance Jr. September 26

Cyrus Vance Jr., a Democrat, is district attorney of Manhattan.

Apple and Google , whose operating systems run a combined 96.4 percent of smartphones worldwide, announced last week that their new operating systems will prevent them from complying with U.S. judicial warrants ordering them to unlock users' passcode-protected mobile devices.

Each company tweaked the code of its new and forthcoming mobile operating systems — iOS 8 and Android "L," respectively — for this explicit purpose. "Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession," reads a new section of Apple's Web site. "Keys are not stored off of the device, so they cannot be shared with law enforcement," a Google spokeswoman stated.

While these maneuvers may be a welcome change for those who seek greater privacy controls, the unintended victors will ultimately be criminals, who are now free to hide evidence on their phones despite valid warrants to search them.

On the losing end are the victims of crimes — from sexual assault to money laundering to robbery, kidnapping and homicide — many of whom undoubtedly are these companies' own loyal customers.

When news of these changes was reported, I did a brief survey of my office's recent cases to see which defendants Apple and Google would have

The Most Popular All Over

ST. LOUIS POST-DISPATCH
Weariness of...

HONOLULU STAR-ADVERTISER
Tropical Storm...

THE ATLANTIC
The...

THE BALTIMORE SUN
Jameis Winston's attorney...

TAMPA BAY TIMES
Watch it and...

protected had their passcode-locked smartphones been running iOS 8 or Android “L” at the time of their arrests. I found:

●Multiple violent gang members who discussed in a smartphone video their plans to shoot a rival. The video was taken shortly before the members mistakenly shot an innocent bystander. The evidence would later be used to implicate two dozen of the gang’s members in additional murders and shootings.

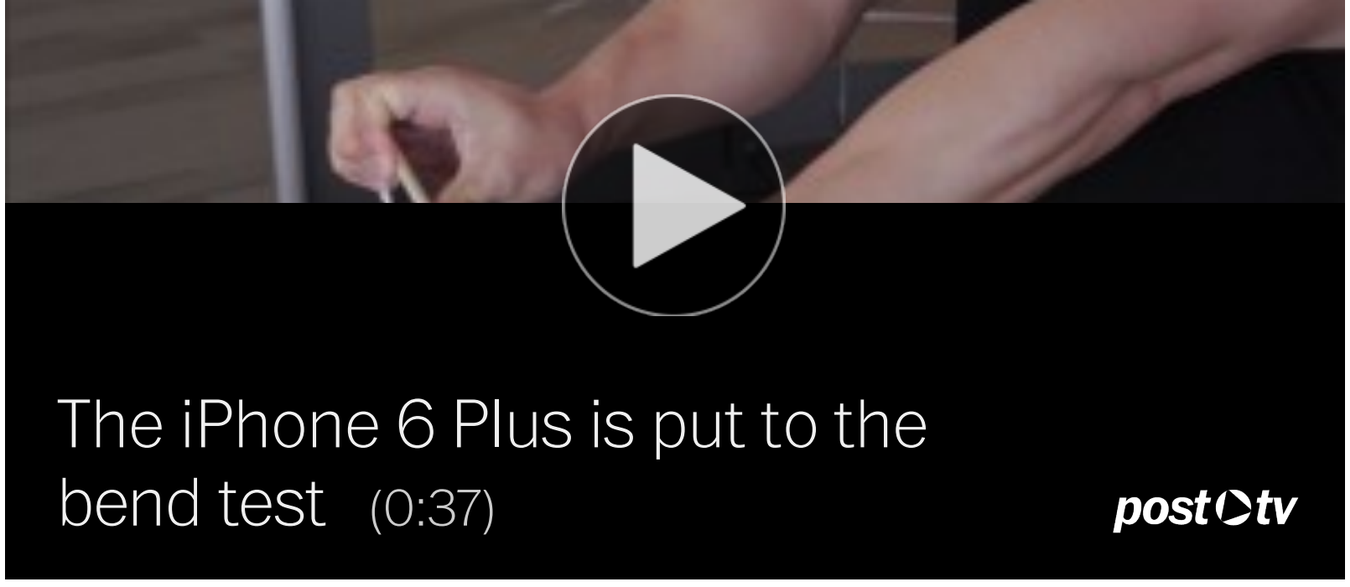
●A vile “up-skirter” who was observed by police inside a major subway station walking up and down stairs behind women wearing skirts, with two iPhones angled upward in his hands. A warrant allowed us to search the phones, which revealed exactly what you would think, as recorded by the perpetrator at multiple stations throughout New York.

●An identity thief whose smartphone contained the bank account numbers, blank check images, account activity screen shots and tax return information of several individuals.

Today, nearly every criminal case has a digital component. Much of the evidence required to identify, locate and prosecute criminals is stored on smartphones. None of the above cases could be prosecuted as effectively if the perpetrators had smartphone software incorporating Apple and Google’s privacy guarantees.

Apple and Google have brought their products to a new level of privacy, and of course privacy is critically important to our society. But the protection of privacy is found in the Constitution, which requires warrants issued by neutral, detached judges and supported by probable cause before law enforcement can obtain information from a mobile device. Absent certain narrow exceptions, my office cannot search a mobile device without a warrant. Neither can the other thousands of state and local prosecutors offices throughout the country. The warrant requirement assures that peoples’ possessions and privacy remain secure in all but exceptional circumstances.

Apple’s and Google’s software updates, however, push mobile devices beyond the reach of warrants and thus beyond the reach of government law enforcement. This would make mobile devices different from everything else. Even bank security boxes — the “gold standard” of the pre-digital age — have always been searchable pursuant to a judicial warrant. That’s because banks keep a key to them.



An employee of iPhone warranty provider SquareTrade demonstrates that he is able to bend the Phone 6 Plus with his hands. The test was conducted in response to complaints that Apple's new smartphones are warping in owners' pockets. (SquareTrade)

I am aware of no plausible reason why these companies cannot reverse these dangerous maneuvers in their next scheduled updates to iOS 8 and Android “L.” Apple’s and Google’s software should not provide aid and comfort to those who commit crimes. This is not a matter of good or bad corporate citizenship. It is a matter of national public safety.

When threats to the common public safety arise, we ask Congress to do everything within its constitutional authority to address them. The provision of cloaking tools to murderers, sex offenders, identity thieves and terrorists constitutes such a threat.

Absent remedial action by the companies, Congress should act appropriately.

Read more about this topic:

The Post’s View: Supreme Court sets out privacy boundaries for cellphones

Alan Charles Raul: After NSA revelations, a privacy czar is needed

Eugene Robinson: Demand the return of your privacy from the NSA