Testimony of
Daniel F. Conley
Suffolk County District Attorney
Massachusetts

Encryption Technology and Potential U.S. Policy Responses

Committee on Oversight and Government Reform

Subcommittee on Information Technology

Wednesday, April 29, 2015

Chairman Hurd, Ranking Member Kelly, members of the subcommittee, my name is Dan Conley and I am the elected District Attorney of Suffolk County, Massachusetts, which includes the city of Boston. I am also currently a board member of the National District Attorneys Association (NDAA), the largest association representing the voice of prosecutors across the country. I appreciate the invitation to testify before you today on a critical issue facing state and local law enforcement from around the country.

Last year, when Apple announced its new iOS 8 operating system, it touted the fact that this technology would not allow law enforcement, even with a court order, to access information on its mobile phones, computers, iPads and other devices. Google also stated that its new operating system would make its mobile devices inaccessible to law enforcement officials, even with a warrant signed by a judge. What's more, this inaccessibility has been presented not as a bug to be fixed but as a selling point to be featured.

In America, we often say that none of us is above the law. But when unaccountable corporate interests place crucial evidence beyond the legitimate reach of our courts, they are in fact placing those who rape, defraud, assault and even kill in a position of profound advantage over victims and society. One of my colleagues, Cy Vance, the District Attorney for New York County, has been a leading voice on this issue. He's met directly with representatives from Google and Apple to listen to their concerns, express our own, lay out the facts, and find a solution, but has been unable to move them from their position. So I am here today to ask Congress to help us find a solution because what Apple and Google are doing is dangerous and should not be allowed to continue.

As a prosecutor, one of my most important duties is to ensure that the evidence we present in court is gathered fairly, ethically, and legally. There is a very good reason for this: the penalty for overreach is suppression of the evidence. If a search is illegal, if a warrant is flawed, then the evidence it yields is excluded and we cannot use it. Under the Fourth Amendment to the Constitution, we as Americans enjoy a presumptive right to privacy that may only be violated under certain, clearly-defined circumstances. Among those circumstances is when there are

specific, articulable facts that would lead a reasonable person – and a judge – to believe that the place to be searched will yield evidence of a crime.

In short, the Fourth Amendment allows law enforcement access to the places where criminals hide evidence of their crimes, once the legal threshold has been met. In decades past, these places were car trunks and safety deposit boxes; today they are computers and smart phones.

Law enforcement agencies like mine undertake these lawful searches to solve crimes that have occurred and prevent further crimes from taking place. We don't monitor what web sites people visit, or aggregate data about people's personal health, wealth, or shopping habits. That, frankly, is the purview of companies like Apple and Google. Their nominal commitment to privacy rights would be far more credible if they were forbidding themselves access to their customers' interests, search terms, and consumer habits, but as we all know, that's not a step they're willing to take. Instead, they're taking full advantage of their customers' private data for commercial purposes while building an impenetrable barrier around evidence in legitimate, court-authorized criminal investigations.

Apple and Google are using an unreasonable, hypothetical narrative of government intrusion as the rationale for the new encryption software, ignoring altogether the facts as I've just explained them. And taking it to a dangerous extreme in these new operating systems, they've made legitimate evidence stored on handheld devices inaccessible to anyone, even with a warrant issued by an impartial judge. For over 200 years, American jurisprudence has refined the balancing test that weighs the individual's rights against those of society, and with one fell swoop Apple and Google has upended it. They have created spaces not merely beyond the reach of law enforcement agencies, but beyond the reach of our courts and our laws, and therefore our society.

Let me give you an idea what this means in practical terms. In every major city with mass transit, prosecutors have been confronted with a rising number of men who use their phones to take pictures and videos up female passengers' skirts. The practice is called "upskirting," and it violates the right that every person has to privacy beneath our own clothes. If the offender's

phone can't be searched pursuant to a warrant, then the evidence won't be recovered and this practice will become absolutely un-chargeable as a criminal offense. But this isn't nearly the worst of it.

Three years ago, we were investigating a child pornography case that led us to a Boston-area teacher. These cases, which re-victimize child rape victims every time an image or video clip is shared, have skyrocketed in the past decade with the advent of faster, more powerful technology. Early on in this particular case, we believed the teacher was merely trading child pornography, but after obtaining and executing search warrants on his electronic devices we recovered evidence that he was actually abusing children and recording his crimes. After a multi-jurisdictional investigation, he was indicted and sentenced to a 45-year federal prison sentence. But if his phone had been encrypted with the technology at issue today, that evidence would have been beyond our reach and he would have been above the law.

Human trafficking and commercial sexual exploitation of children is also on the rise in America and globally, aided and abetted by the same technology. It's moved off the street corner and into motels with Wi-Fi access, with victims, including children, advertised for sale on web sites accessed through handheld devices. With these operating systems, those devices would become warrant-proof and the evidence they contain unreachable by investigators. I don't believe that Apple or Google set out to design a system to enable human trafficking, but that's precisely what these new systems do.

So when we talk about warrant-proof encryption, let's be very clear about who will benefit from it: perpetrators of every violent, sexual, or financial crime in which handheld technology is used. I would be hard pressed to think of any homicide solved in recent years where significant, critical evidence wasn't recovered from a cell phone. We've uncovered massive economic and financial fraud schemes and disrupted vast drug trafficking rings, none of which could have been stopped, let alone solved, had law enforcement – with the blessing of the courts - been blocked from exercising the legal and legitimate means to do so. This isn't rhetoric. It's reality.

Apple and Google operating systems run a combined 96.4% of smartphones worldwide, and as of March, 78% of all Apple devices are running iOS 8. This means law enforcement is unable to access data on 78% of all pin-locked Apple devices, and that number is growing every day. It is a myth that law enforcement has some secret means to decrypt these devices. It is also patently false to claim that this same data can be downloaded from the cloud when most of it is never uploaded to begin with.

This is not an issue of mass data collection. Whatever some advocates might claim about the search warrants granted each year to federal, state and local law enforcement, those warrants are authorized by independent judges, they are based upon an established legal principle, and they affect only the tiny, tiny percentage of the population against whom there is specific, articulable evidence of criminal activity. Let's remember, the vast majority of people are leading honest, upstanding lives every day. We're not interested in what's on their phones. Even Apple's own estimates show that only 0.00571% of customers had information disclosed due to government information requests.

And while some might point to overreach and intrusion by the NSA as justification for designing phones that block out entirely the government's ability to gain access to them, I think the vast majority of Americans recognize that over-reacting and shutting off access to these phones under and any and all circumstances will not only make it monumentally harder to solve crimes and hold criminals accountable in the digital age, but will also make it infinitely more difficult to detect and prevent terrorist threats.

It is ironic that what Google and Apple are doing is, in many ways, a response to what occurred at the NSA, but it is state and local law enforcement and the tens of millions of Americans we protect and victims we serve who are now bearing the brunt of it. We recognize that Google and Apple are global companies with a worldwide customer base, but whatever goodwill or support they believe they will earn with these dangerous operating systems will erode rapidly as victims of physical and economic predation find their paths to justice blocked while those who hurt and exploit them are protected.

Let's also be clear about another unintended consequence of these operating systems: by cutting off law enforcement and society's legitimate interests in obtaining evidence to hold the guilty accountable, it also cuts us off from crucial evidence that speaks to factual innocence. While the evidence obtained from a smart phone will often place an individual at the scene of a crime or provide other evidence of guilt, that same information eliminates other people from the realm of possible suspects. In the past decade, the technology driving exonerations of wrongly convicted defendants has been DNA science. But the day is not far off when a piece of digital evidence obtained from a cell phone will prove to be the key that frees an innocent man.

What these companies are doing is unprecedented, and for good reason: they are substituting their own interests for 200 years of jurisprudence and the independent judgment of our courts, our legislatures, and our Congress as to how the Fourth Amendment to the Constitution should be balanced and applied.

In addition, I can think of no other example of a tool or technology that is specifically designed and allowed to exist completely beyond the legitimate reach of law enforcement, our courts, our Congress, and thus, the people. Not safe deposit boxes, not telephones, not automobiles, not homes. Even if the technology existed, would we allow architects to design buildings that would keep police and firefighters out under any and all circumstances? The inherent risk of such a thing is obvious so the answer is no. So too are the inherent risks of what Apple and Google have devised with these operating systems that will provide no means of access to anyone, anywhere, anytime, under any circumstance.

Like most Americans, I too am a customer of these companies and I hold my privacy rights dear. As the head of one of the largest District Attorney's Offices in the country, I also understand the value of, and strongly encourage the use of, secure encryption technology to prevent hacking, theft, and fraud. I think most people recognize however, that balance must be struck between an individual's privacy rights and the legitimate interests of society to protect itself and bring dangerous criminals to justice. Apple and Google need to recognize this, too.

I will conclude today by pointing out that for weeks now in Boston and all across the country, we have been following the trial of one of the terrorists whose actions at the Boston Marathon two years ago left four people dead and hundreds more grievously injured. Cell phone evidence – much of it volunteered but some obtained only through a warrant - was critical to understanding what happened, how it happened, and who did it. Were law enforcement blocked from obtaining that evidence, or if other companies were allowed to make their own determinations as to what video or other evidence law enforcement was and was not permitted to see, the apprehension of those responsible for the Boston Marathon bombings would have been very much in doubt. Again, I don't believe that Apple or Google intend to create "safe space for terrorists", but make no mistake, that would be the result and those are the stakes.

Therefore, I respectfully urge Congress to prohibit the sale of digital devices that cannot be accessed pursuant to court orders. I would further urge Congress to update the Communications for Law Enforcement Assistance Act, or CALEA, to cover smartphones and ensure that there is a reasonable solutions for law enforcement to gain legal access to crucial evidence. Thank you for your time and attention and I am happy to take any questions you might have.