DA Vance Addresses the 6th Annual Financial Crimes and Cybersecurity Symposium
Remarks as Prepared | November 18, 2015

Good morning. Thank you Tom [Baxter] for that kind introduction. Thank you and your staff for hosting us today and, above all, thank you for your critical work securing the capital markets in New York.

This morning we have assembled the leaders of the financial, cyber, regulatory, technology, and law enforcement communities, representing more than a hundred domestic institutions as well as partner organizations from the United Kingdom and Canada. When we were planning this conference, I imagined extending a very different welcome to you this morning. But I hope you will not mind if I dispense with the pleasantries, and begin by stating emphatically that never before have your skills been more vitally needed.

Two weeks ago, I was in Paris, where I met with Paris' chief prosecutor, Francois Molins, and with Alice Cherif, Chief of the Cyber Section of the Paris Prosecutor's Office. I am truly humbled by the presence of *Procureur* Cherif with us this morning, and I would ask her to rise so that we might stand with her in solidarity.

President Hollande spoke without hyperbole when he described the war against terror as the war of civilized peoples against barbarity. The expertise of you in the audience this morning will be critical to winning that war. And that is because you, together with your colleagues and with partners in law enforcement, have the tools, the experience, and the intelligence, to help defeat the terrorists, and to protect our communities from attack. When terrorists strike, they seem at first to come from nowhere, and the strike seems to come without warning. But in fact, terrorists rely on three things, and each one makes them vulnerable to detection and arrest: they need funding; they need coordination; and they need communication.

With respect to funding, the vigilance of your compliance offices will help to ensure that money remains out of the hands of terrorists, and that when any employee, anywhere detects suspicious activity, that the intelligence is recorded and reported. For my part, you have my pledge that we will review those suspicious activity reports, and that every scrap of useful intelligence will be put to use. And I pledge as well that when international sanctions are violated, we will bring the full force of the law against those who violate them.

The second vulnerability of terrorist cells comes in coordination. Even a homegrown violent extremist has to get materials from somewhere, information from somewhere else, and inspiration from a purveyor of hatred. Detecting this information is very much akin to the criminal investigation of any major crime. It plays to our strengths in local law enforcement. The NYPD has 35,000 pairs of eyes in the streets, and we have some of the best and the brightest attorneys and investigators waiting for them when they get to the DA's Office. And so, this summer, we formed the Manhattan District Attorney's Office Counter Terrorism Program, which is housed in our Major Economic Crimes and Rackets Bureaus. I named three Counter Terrorism Coordinators to lead our Program, and to interact with the Joint Terrorism Task Force on which we sit, as well as to coordinate all counterterrorism matters with the NYPD, federal agencies, and foreign law enforcement. The goal of our Program is simple: leverage the vast amount of intelligence we accumulate as we investigate and prosecute our more than 100,000 cases a year to help detect and investigate all local threats, in close coordination with our federal partners.

Another way we support our partners in the fight against terror is by investing in the tools law enforcement needs to prevent the next attack. Last year, we invested $90 million in criminal forfeiture funds to equip New York City police officers with 41,000 mobile devices, including tablet computers for every patrol car and handheld devices for every cop. Our initiative is bringing all of the terror- and crime-fighting information currently available to NYPD officers at the precinct onto one mobile platform for the first time. Officers are getting real-time 911 call data, warrant information, photographs of missing persons and suspects, and fingerprint scanning available to them at the swipe of a finger. They can run a universal search across all of NYPD's databases while standing on a street corner. They can translate written and spoken conversations in more than 200 languages. But perhaps most importantly, given current events, they're getting counterterrorism alerts and deployment information transmitted directly to them in the field, providing critical information and updates in a timely and coordinated manner. With 35,000 of New York's Finest equipped with 21st Century, real-time tools, we believe we can reduce the likelihood of a terrorism suspect slipping through our fingers.

The third vulnerability of terrorists comes in communications. Their every phone call, every text, every Facebook posting, increases the likelihood of detection. But here, our battle is not only against the terrorists, but against the misdirected efforts of the mobile device industry as well. Most people today live their lives on smartphones, and, in this regard at least, criminals are no different. While in the past, criminals may have kept evidence of their crimes in file cabinets, closets and safes, today that evidence is more often found on their smartphones.

What information have we been able to retrieve in our investigations? Text messages between sex traffickers and their customers; a video of a murder victim being shot to death; personal identifying information bought and sold by cyber criminals. In fact, in matters of everyday crime, it is the rare case in which smartphone information is *not* useful.

But now, the smartphone providers have locked their phones in a way that even they cannot defeat. The full-disk encryption of smartphones since September of 2014 has presented an enormous setback to us, particularly in local law enforcement, which accounts for 95% of the criminal cases filed in the country every year. Both Apple and Google advertise as a selling point for their phones that nobody – not law enforcement with a valid warrant, not even Apple and Google themselves – can download encrypted data from their phones. Apple told its customers, quote: "we can no longer bypass your passcode, and therefore we can no longer access your data. So it's not technically feasible for us to respond to government warrants for the extraction of data on your device." In short, they said, we have redesigned our devices so that even we will no longer be able to comply with law enforcement warrants.

It's hard to overstate the impact on our ability to conduct criminal investigations. In just the fourteen months since the new encryption features were introduced, in forensic evaluations done just in our office's cyberlab alone, 111 victims of crime have seen their quest for justice delayed or destroyed by full-disk smartphone encryption. We've had 111 search warrants issued by judges that we couldn't execute, because the perpetrators – of attempted murder, sex trafficking, assault, and robbery – used iPhones that we were unable to unlock.

This week, every law enforcement entity in every major city around the world is intensifying its initiatives against terrorism. Every tip will be investigated, every lead will be followed. But every

time one of those trails leads to an encrypted cellphone, it may go cold. This is what Director Jim Comey of the FBI, our Keynote Speaker today, calls the "going dark" problem.

As a prosecutor, I have no higher public policy priority than to persuade Congress to enact sensible statutes that will protect legitimate privacy concerns, while giving law enforcement the ability to access cellphones when necessary to prosecute serious crimes and fight terrorism. I understand that Apple and Google did not take their actions in a vacuum. The public is angry, and at times understandably angry, at some highly-publicized cases of overreaching in intelligence-gathering. I have no doubt that full-disk encryption is a strong branding and public-relations move for Apple and Google in the wake of Edward Snowden's disclosures. But ultimately, the line between an individual's right to privacy and the legitimate needs of law enforcement should not be decided by the marketing departments of smartphone companies. That line should be defined by legislatures and the courts.

And here's one important point: Lawful access to criminal evidence on smartphones has nothing to do with the kind of mass surveillance or bulk data collection disclosed by Mr. Snowden. That is not the access state and local law enforcement seeks or expects. What we in state and local law enforcement are talking about, is targeted requests for information, authorized after an impartial, judicial determination of probable cause, granting a search warrant for particular evidence stored on a specific mobile device. The warrant requirement, enshrined in the Fourth Amendment and defined over two centuries, sets the balance in our society between personal privacy and public safety.

Today my Office is releasing a Report on Smartphone Encryption and Public Safety, and with it, our blueprint for a way forward. We've been working on this report for several months, in consultation with foremost experts in cryptology, technology, and law enforcement investigations, to craft a solution that we believe is both technologically *and* politically feasible.

Our report is designed to do a few things: to demonstrate the importance of evidence stored on smartphones to public safety; to dispel certain myths that many privacy advocates hold about our position; to encourage an open discussion with tech companies, privacy advocates, and lawmakers; and most importantly, to propose a solution that protects both privacy *and* safety.

That solution, set forth in our Report, is simple: make smartphones amenable to search warrants. Do it with a federal law that says that any smartphone made or sold in the U.S. must be able to be unlocked – not by us, but by the designer of the operating system – when the designer is served with a search warrant.

Our solution requires no new technology or costly adjustments. In fact, our report makes clear what kind of access we do not seek. We do not want a backdoor for the government. We do not want a "key" held by the government, and we do not want to collect bulk data on anybody.

Our blueprint occupies a rare middle ground in the debate over lawful government access to smartphone communications. Let me be clear. The proposal outlined in our report is not a wish list, not a list of changes in the law we would like to see in an ideal world. On the contrary, the proposal presents a bare minimum for us to continue critical investigations within the rule of law. At this point, I must note that the tragedy in Paris has started a conversation about encrypted and vanishing apps, which is a danger apart from that addressed in our report.

To read our report, please ask a member of our staff here today for a copy, or read it online at Manhattan DA Dot Org.

I believe ultimately we will prevail in the battle against terrorism, and I believe that ultimately, the tech community wants to do the right thing – to leverage the awesome power of the tools they have created – to promote public safety. We saw the public-minded impulse of the tech community in the immediate aftermath of the Paris attacks. From Facebook's activation of "Safety Check," to Uber's suspension of surge pricing to get people home safely, to AirBnb's disaster response tool to shelter stranded Parisians, to Google's offering free international calls to Paris. The list goes on. I hope the same spirit of public-mindedness will lead smartphone providers to negotiate a solution to this problem.

I know that I am joined in this hope by Commissioner Adrian Leppard of the City of London Police, who is seated beside me and who joined me and French prosecutor Francois Molins recently for a *New York Times* op-ed on this very topic. Under the leadership of Commissioner Leppard, the City of London Police and Manhattan District Attorney's Office have identified many overlapping interests in protecting our residents against the pervasive and dynamic threats we both face. Last year on this stage, Commissioner Leppard and I announced an innovative partnership to exchange information and personnel. Already, our agencies, working together, have taken down a multi-million dollar securities fraud ring and an international "e-ticketing" scam with arrests on both sides of the Atlantic.

And just last month, Commissioner Leppard and I, together with the Center for Internet Security, announced the formation of a new Global Cyber Alliance – a transnational, multi-sector effort to neutralize cyber risks by sharing attack data and developing new methods to protect our residents and institutions. Already, more than 50 organizations have joined the Global Cyber Alliance, including many of your institutions, whom I am deeply grateful to have as partners. Earlier this year, Commissioner Leppard saddened colleagues in London *and* Manhattan, with his announcement that he will be retiring from active law enforcement duty after 31 years in service. Fortunately for us, he will be staying on with the Global Cyber Alliance, and we are enormously grateful for that. In 2011, Adrian began his current post as Commissioner of Police for the City of London. In addition to policing the "City Of London" – which is the historic, financial center of today's London – Adrian also oversees the U.K. National Fraud And Cyber Intelligence Bureau, the International Fraud Academy, and the Economic Crime Directorate – a team of two-hundred specialists that investigates the most serious financial- and cyber-fraud cases in the U.K.

Given the cross-border nature of the crimes that Adrian has prosecuted and prevented, his work has helped to make not just Londoners, but also New Yorkers, safer. Our partnerships like the Global Cyber Alliance are forward-looking, cross-sector, trans-national partnerships that will serve us well into the 21st century. Neither would have been possible without the energy, vision, and leadership of Adrian Leppard. Adrian, please come up. It is my honor to present you with a small token of our appreciation.

Thank you, Adrian. I had planned on presenting you with a key to the City, but I've been informed that even that has been encrypted.

A moment ago I talked just a bit about our Keynote Speaker, FBI Director Jim Comey. Jim has been an outspoken, fearless advocate not only on our need for lawful access to criminal evidence

on smartphones, but on so many issues of importance to public safety in our communities. He is also the leading voice within law enforcement calling upon us all to bring about a new era of racial sensitivity. Director Comey is a native of Yonkers, just a few miles north of Manhattan. He's a graduate of the College of William & Mary and the University of Chicago Law School. He has served an Assistant U.S. Attorney, both here in Manhattan and in Virginia, and in 2003, he because the nation's Deputy Attorney General.

President Obama nominated Jim to be FBI Director in July of 2013. There has, quite possibly, never been a better partner for state and local law enforcement at the FBI than Jim. At Jim's direction, our federal partners are now more engaged and more attuned to what is happening in in states and cities across the country than ever before. And our agencies are working together more seamlessly than ever before. It's my great honor and privilege to introduce our friend, partner, and Keynote Speaker, Director Jim Comey of the FBI.

###