DA Vance Delivers Opening Remarks at Manhattan District Attorney's Office's 7th Annual Financial Crimes & Cybersecurity Symposium

Remarks as Prepared for Delivery | November 17, 2016

Thank you Michael Held for that kind introduction. Thank you and your entire staff for hosting us today. And thank you for all you do every day to secure the capital markets in New York.

Thank all of you for being here at our seventh annual symposium. Today in this room we have 350 senor leaders from financial, cyber, regulatory, technology, and law enforcement communities. You represent 148 organizations and you came here today from seven countries, including the UK, France, Singapore, Canada, Israel, and Australia. And thank you to all of our speakers today.

We have a lineup of the world's foremost leaders in the fight against terror, cyber, and financial crimes with us. Thank you Homeland Security Secretary Jeh Johnson for being here. Thank you to City of London Police Commissioner Ian Dyson – joining us from England, Paris Prosecutor Francois Molins – joining us from France, and Europol Director Robert Wainwright – joining us from The Hague.

We'll also hear from the legendary Bill Moyers, our dear friend and former NYPD Commissioner Bill Bratton, NYPD Deputy Commissioner for Intelligence and Counter-Terrorism John Miller, U.S. Attorney Robert Capers, our state Superintendent of Financial Services Maria Vullo, and many other critical players.

They're here today, as you are, to share insights and best practices, to develop new partnerships, and to assess our collective efforts as we confront emerging threats to our residents and institutions around the world. In many ways, these emerging threats – which we've been gathering annually since 2010 to assess – have arrived.

When I was a rookie Assistant District Attorney in the 1980s, computer crime meant someone stole a whole desktop computer from an office. In 2016, cybercrime is the fastest growing crime category in New York, and a clear and present danger is to our residents, our institutions, and our way of life.

Every day now we are bombarded with stories of large-scale, institutional cyberattacks and data breaches. In recent years, these attacks have crossed over into the public consciousness, touching the lives, personal identifying information, and intimate secrets of millions. Most recently it was the Democratic National Committee hack. Or last year, the federal Office of Personnel Management. Or in 2014, Target and Sony Pictures.

The attacks are coming fast, furious, organized, and sophisticated, as is true for all tech-enabled crimes. What is new here is the attackers' increasingly diverse goals, and their rate of success in achieving them.

Cybercrime used to be about stealing money – or about stealing data to sell for money. That still represents the typical fact pattern in the tens of thousands of cybercrime and identity theft cases my Office prosecutes each year. But when you compare those motives with the aims underlying this year's most notorious attacks, it is easy to see that today's breaches represent something far more sinister.

Cyber attacks are being deployed by hostile foreign actors – perhaps governments − to achieve political ends or to unleash chaos and uncertainty on our shores. In some of these attacks, data is not being bought or sold – it is being dribbled out, over key moments in the civic life of our country, to undermine faith in our democratic processes, and maximize disruption. These attacks form a new, different and distinct crisis, and in a moment I will talk about the work we are doing to shut down the cyber vulnerabilities that enable them to flourish.

Cybercrime is second only to terrorism in its potential to disrupt the functioning of our society. And terrorism itself is now a fact of life in some of our jurisdictions. Many of you here today are engaged in the fight against terror and terrorism finance – whether you're an intelligence expert in law enforcement, or an anti-money laundering specialist at a financial institution. My Office is also helping to prevent attacks – by investigating threats in-house, by feeding the counter-terrorism community with actionable intelligence, by disrupting terror finance, and by investing in the tools that law enforcement needs to prevent the next attack.

Today we will hear from Francois Molins, who is my counterpart in Paris. At this very symposium last year, we begin the day with a moment of silence to commemorate the 90 men and women who lost their lives at the Bataclan Theatre, and to support Francois's efforts to apprehend the madmen responsible.

This past weekend, the Bataclan Theatre reopened with a concert by Sting. Life in Paris will never quite be the same, but thanks to Francois and his brave colleagues, Parisians are beginning to regain a sense of normalcy. Under his leadership, the Paris Prosecutor's Office – charged with investigating not one, but five, major terror attacks since 2012 – has become a worldwide model for major city prosecutors who want to contribute to the fight against terror in our own nations.

We have so much to learn from them, which is why we are announcing today a brand new partnership between the Manhattan District Attorney's Office and the Procureur de la République de Paris. A partnership not only to share intelligence, but to work together, hand in hand, on joint investigations of transnational crimes affecting Manhattan and Paris residents. Not only that, we will offer secondments – or exchanges of personnel. Beginning in the first quarter of 2017, participating Manhattan DA staff will become fully embedded members of the Paris Prosecutor's Office, and vice versa.

Our partnership with Paris is modeled on a similar one we created with the City of London Police in 2014. Our London partnership was the first initiative of its kind between local prosecutors in the U.S. and foreign law enforcement.

Under our partnership with the City of London Police – led by Commissioner Ian Dyson, who is joining us for the first time today – our agencies have developed joint investigations culminating in several major indictments, including an international "e-ticket" scam with arrests on both sides of the Atlantic, and a multi-million dollar securities matter involving dozens of victims. It's also enabled the cross-pollination of strategies, and in the case of cybercrime, an entirely new way of doing business.

Some time ago, I sat down with the Commissioner of the City of London Police to discuss our budding partnership. We talked about ways to collaborate and, in so doing, to better protect our respective cities. It wasn't long until we figured out that the same people stealing from London residents in cyberspace are also stealing from people in New York. It became clear to us that the cross-border, mass-victim character of cybercrime required us to change the paradigm of traditional crime fighting significantly. We could prosecute these cases until we were blue in the face, but we wouldn't be bending the overall curve in terms of the massive rise in cyber attacks.

That is why I am not up here listing the dozens of cybercriminal rings, both local and international, that my Office has prosecuted successfully, or going on at length about the multi-million dollar, 17,000 square-foot Cyber Lab that we opened yesterday to house our 75 full-time staff members dedicated to cybercrime investigation and prosecution. Because the truth is, systemically, these cutting-edge investigations and prosecutions alone will only get us so far. Given the sheer volume of cybercriminal attacks, prosecuting these cases, even the big ones, is not going to reverse the trend.

As a world community, the key to defeating cybercrime lies not in prosecuting it, but preventing it. That is why, last year, together with the City of London Police and the Center for Internet Security, I announced the creation of the Global Cyber Alliance, and I committed $25 million dollars from our criminal forfeiture proceeds to support its work.

GCA, as it is known, is a cross-sector, non-profit alliance working proactively to reduce cyber risks worldwide. Its mission is to build an international community to confront the serious cyber risks we all face, and to implement real solutions that will have measurable positive impact. One year in, we are well on our way. GCA has more than 120 global partners from 18 countries and 21 economic sectors, and our ranks are growing each day.

GCA's President, Phil Reitinger, is here with us today. He's doing a remarkable job building out the organization, bringing the world community together, and implementing solutions. Please approach Phil if you'd like to join GCA, or learn more at global cyber alliance dot org.

I'd also like to recognize former Mayor Mike Bloomberg, who is providing GCA's New York City headquarters for free. And I am equally grateful to the City of London for donating office space for GCA's headquarters there.

Out of these offices spread halfway across the globe, GCA is already tackling its first major cyber risk, which is phishing. Almost every big hack you read about starts with a well-crafted email sent to the right person or people in an organization, who clicks on an attachment, and the hackers are "in". Every day, phishing schemes compromise consumers, companies – and most recently and infamously – a presidential campaign chairman. Phishing attacks represent a majority of the current attacks we all face, and the leading cause of economic damages relating to cyber breaches.

So today, together with our GCA partners, we are announcing the release of powerful, open-source tools to combat phishing that organizations large and small can download and implement for free. The solutions deployed in these tools – "DMARC" and DNS filtering, are proven approaches that, when implemented, reduce the risk of phishing exponentially. DMARC is a combination of protocols that prove that an email hasn't been spoofed. It neutralizes cyber attacks by ensuring that spammers and phishers can't send fraudulent email from a "spoofed" email address to you or your organization.

Last month, GCA worked with partners to deploy a beta version of our DMARC tool in their organizations. When GCA implemented DMARC at a health care company, it found that one out of every 200 emails being sent to the company were false. If DMARC were deployed globally with similar results, our tool could block over 500 million spoofed email messages every day.

Our goal in distributing these free tools is nothing short of global implementation. So, alongside our tool, you'll find an online guide to make it easier for your organization to adopt DMARC. Already, more than 35 government entities and seven healthcare organizations who have heard about our DMARC tool have expressed interest in implementing it. I am so pleased to announce today that these resources are now available to anyone, and they are free.

The second phishing solution GCA is building is called a DNS "Internet Immune System," which organizations will use to block access to malicious websites. GCA and its partner, Packet Clearing House, have built a global DNS infrastructure to deploy this solution, and it's already functioning on four continents today. Over the following months, this system will be made globally available, at no cost to anyone who wants to use it.

GCA is an example of the public and private sectors working together to combat the most pervasive digital threats we face. Sometimes, in this endeavor, the public and private sectors experience a little more friction. Sometimes we disagree on exactly what solves what, and what makes things even worse.

I'll give you an example. In September 2014, Apple announced that its new mobile operating system, iOS 8, would be designed so that Apple would no longer have the ability to extract data from its devices, even if presented with a search warrant directing it to do so. Google, which makes the Android operating system, quickly followed suit.

Law enforcement and crime victims' advocates came out immediately to warn the companies and Congress that placing smartphone data beyond the reach of search warrants – in a class all by itself – would pose an obvious and significant risk to public safety.

At least year's Symposium, I announced the release of my Office's Report on Smartphone Encryption and Public Safety. In addition to proposing legislation, our Report illustrated some of the legal and practical problems for law enforcement and crime victims posed by default device decryption, and it asked Apple to explain the cybersecurity benefits – if any – so that policymakers could fairly weigh the pros and cons.

Since then, while terrorism cases like San Bernardino have generated the lion's share of the media coverage, the impact of default device encryption has been felt most profoundly on the local level, in the investigation of domestic crimes occurring every day across the U.S.

In my Office alone, 423 Apple iPhones and iPads lawfully seized since October 2014 remain inaccessible due to default device encryption. Approximately 10% of our warrant-proof devices pertain to homicide or attempted murder cases, and 9% to sex crimes. And while we've been locked out of approximately 34% of all Apple devices lawfully recovered since October 2014, that number jumped to approximately 42% of the devices recovered in the past three months.

With over 96% of all smartphones worldwide operated by Apple and Google, and with devices running older operating systems rapidly aging out, the trend is only poised to continue. In other words, the risks associated with warrant-proof encryption remain, and are growing.

So today, my Office is releasing version 2.0 of our Report on Smartphone Encryption and Public Safety, and with it, our recommendations for a sensible and moderate way forward. Version 2.0 of our Report studies Apple's own experience and public statements about device encryption, and – in consultation with experts on both sides of the debate – concludes that Apple's method of data extraction before iOS 8 was never compromised.

It further concludes that requiring smartphone makers to retain the ability to extract data will not increase users' risks of being hacked. It also concludes – and I am sorry for the spoilers – that doing nothing about this problem will perpetuate an untenable arms race between private industry and law enforcement, and that federal legislation is our only chance to lay these arms aside.

To fight crime effectively in the 21st century, we have to make smartphones answerable to search warrants – just as they were until 2014. Complying with judges' warrants for smartphones never involved a government backdoor. It never meant that the government held a key to anybody's phone. It never enabled access to real-time communications, and it never meant collecting bulk data on anyone.

But perhaps most relevant for purposes of today's symposium, warrant-proof encryption does nothing to protect us from the rising tide of cybercrime. Those large-scale, institutional, existential cyberattacks that I mentioned earlier? DNC, OPM, and Target? They were caused by phishing, malware, and improperly protected security systems.

Default device encryption does not defend against these kinds of cyberattacks, nor does it protect users from phishing attempts on their devices. What it does do, is thwart law enforcement's ability to identify the perpetrators, and take them out of the game. That is the great irony at the heart of this debate. In their purported attempt to provide more cybersecurity, Apple and Google have empowered cybercriminals to act with impunity.

My Office will continue working to set the record straight. Please pick up a copy of our Report today, or read it online at manhattanda.org.

This debate will rage on, and we'll explore it further throughout our program today. But for now, something we can all agree on – and that is how phenomenal it is to have Secretary of Homeland Security Jeh Johnson as our Keynote Speaker today.

Secretary Johnson and his staff of 229,000 work every day to protect Americans from cybercrime and terrorism. They secure our borders, our airports, and our infrastructure. They respond to disasters natural and manmade, they protect us from bad actors at home and abroad, they assist my Office in cases ranging from antiquities smuggling to credit card fraud, and they do a truly phenomenal job.

Before Secretary Johnson was appointed in 2013, he served as General Counsel at the Pentagon, a job my father held in the Kennedy administration at the start of my father's career in public service. In that role, Jeh helped pave the way for the repeal of Don't Ask, Don't Tell, and spearheaded countless other changes to strengthen our military.

Like many good people, Secretary Johnson is a native New Yorker. We're proud to welcome him back home today, and to recognize his years of tireless advocacy on behalf of our City – supporting our first responders on the front lines of local counterterrorism work, and ensuring that New York City has the resources we need to prevent the next attack.

He's been an extraordinary partner to the Manhattan District Attorney's Office, and we wish him the very best in his next endeavor. Please join me in welcoming the Secretary of Homeland Security, Jeh Johnson.

###