DA Vance Remarks on "Cybercrime: Crossing Borders and Sectors"
Bloomberg Big Law Business Summit
Remarks as Prepared for Delivery| June 9, 2016

Good morning. Thank you to Bloomberg Law for inviting me to be a part of your summit, and thank you Josh [Block] for that kind introduction. You've done a phenomenal job today bringing together the biggest in Big Law – managing partners, senior partners, and senior associates of some of the finest law firms on the planet; as well as Chief Legal Officers and general counsel of some of the world's most sought-after clients.

Much of today's summit is about innovation and the future of Big Law. It's a vital topic – for you as leaders in your profession, and for me leading a DA's office of 600 lawyers that handles more than 100,000 cases annually – more cases than the entire U.S. Department of Justice handles nationwide each year.

Nowhere is the need to innovate greater than in taking on the cyber threat today.

It's often said – and it's a phenomenal thing – that New York is now the safest big city in America. That is principally because we have done an amazing job reducing violent crimes like homicide, rape, and robbery. In the area of economic crime, however, New Yorkers remain very much at risk. Cybercrime is the case in point.

Despite all of the public safety gains we enjoy in contemporary New York, in my mind, cybercrime – second only to terrorism – is the greatest threat to our companies, our institutions, our residents, and our way of life. The crime scene of the 21st century is not a street corner cordoned off in yellow tape. It's the internet, and digital spaces all around us.

Nowhere is this more evident than Manhattan, where most major banks and financial institutions are headquartered or have a significant presence, and where those companies house the digital identities of millions of consumers, and of tens of thousands of businesses, large and small.

Because of Manhattan's nexus to money movement and customers' identities and accounts, my Office, since 2010, has invested unprecedented sums to develop the expertise, talent, and tools required to become a national leader in the prosecution of cybercrime. In this effort, we aren't operating by someone else's playbook; we are writing our own.

I could list the dozens of cyber conspiracies – local and international – that we have prosecuted successfully. But I have to tell you: systemically, these prosecutions alone will only get us so far. Given the sheer volume of cybercriminal attacks – and given the migration of folks moving over from street crime to cybercrime to join their ranks – prosecuting these cases, even the big ones, can sometimes feel like pushing sand up a hill.

One reason for that is, if the information about the cyberattack that we prosecuted isn't effectively shared, other institutions – indeed, perhaps whole industries – remain vulnerable to similar breaches.

The other reason why prosecuting cyber cases can feel so Sisyphean is the rapid evolution of cybercriminal methods. Cybercrime evolves, and when we catch up with it, it evolves yet again. In 2014 and 2015, it was large-scale breaches of sensitive customer data. Chinese hackers broke into the U.S. Office of Personnel Management and stole the data of up to 4 million federal employees and up to 18 million others, including my own. And in the private sector, it seemed like every month that we learned of another hack of massive amounts of data at major retailers, healthcare providers, and financial institutions, including Target, J.P. Morgan, Home Depot, and Staples – companies that touch the daily lives and personal information of tens of millions of Americans.

But just when it seemed like data breaches may be diminishing, new crimes filled the void. Business Email Compromise Schemes, or "BECS," are now familiar to many of you. This is where, for example, a Chief Financial Officer receives an email purportedly sent "from the CEO." The email, which looks legitimate, will say something like, "please wire 600,000 dollars to Account #1234 ASAP – highly confidential. Will discuss later." My office has handled many of these in recent years.

We will continue prosecuting cybercrime no matter how rapidly it evolves and no matter how many new entrants get in the game. But at the same time, I think these trends lay bare the limitations of our traditional courtroom approach.

First and foremost, cybercrime is international. Traditional borders and boundaries are irrelevant. I sat down with the Commissioner of the City of London Police some time ago. We talked about ways to collaborate and, in so doing, better protect our respective cities. To start, we formed a partnership to share intelligence, personnel, and training resources in order to combat transnational crimes affecting both New York and London residents. It was the first initiative of its kind I'm aware of between local prosecutors in the U.S. and foreign law enforcement.

Our partnership has enabled further joint investigations, including a multi-million dollar securities matter involving dozens of victims. It also enables the cross-pollination of strategies, which is why we offer secondments, or exchanges of personnel, between our Office and London. Participating Manhattan District Attorney staff become fully embedded members of the City of London Police, and vice versa.

It wasn't long until we figured out 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 crimefighting 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.

To really change the situation, to more effectively fight the international cybercriminals of the 21st century, we knew we had to engage in a level of cross-sector, cross-border cooperation that had not yet been achieved.

And so, last year, together with the City of London Police and the Center for Internet Security, my Office launched what we call the "Global Cyber Alliance," and pledged seed capital of up to $25 million in criminal forfeiture proceeds over five years to make our new organization a reality.

The Global Cyber Alliance, or GCA, is a transnational, non-profit, multi-sector effort focused not on prosecuting cyber crime, but preventing it – to neutralize and minimize cyber risks by sharing attack data across sectors and borders and developing new methods to protect our residents and institutions.

To date we have 64 member organizations, representing a dozen different areas of industry and practice, from finance to aviation to media. For the in-house counsel here today, I suspect that some of your institutions – including Aetna, Bloomberg, BNPP, Microsoft, Lockheed Martin and Citibank – are participating already, and we have 200 more in the process of joining.

Today I'm pleased to announce the newest member of the Global Cyber Alliance, and our first law firm to join. It's a small shop of about 900 attorneys called Simpson Thacher & Bartlett. We're excited to have them on board, and to incorporate their expertise and intelligence.

Our alliance is designed to be different from other cybersecurity entities. First, we are a non-profit organization. We are neither a government nor a commercial entity. And participation in GCA is entirely voluntary. As a prosecutor, I know that any effort to obtain information about internet communications will immediately be scrutinized for signs that we are attempting to lower the barriers of privacy. Our purpose instead is to develop the best technological solutions to counter cyber threats and share that information so that others in the Alliance can prevent them prospectively, or – based on information about nascent cyber attacks from other members – react intelligently, and share information in real time to mitigate the impact of an impending attack.

Another principle that guides GCA is confidentiality. Understandably, companies aren't enthusiastic about telling the world about a new data breach. We recognize that complete confidentiality is not always legally possible. Securities regulations, fiduciary obligations, and other laws sometimes require public disclosures of breaches. But wherever possible, GCA protects the identity of those reporting new attacks, in much the same way that the Centers for Disease Control and the World Health Organization can announce the

outbreak of a contagious disease, or the success of vaccination efforts, without revealing the identities of the patients.

Last month, we announced our plan to confront the top cyber risks threatening digital security today, which we've identified as:

- Phishing
- Vulnerability related to weak identity and authentication mechanisms
- Risks arising from compromised or unsecure websites, and
- Distributed Denial of Service, or DDoS, attacks.

Phishing is a relatively mundane, relatively old-school form of cyber attack. Yet it remains the number one cause of economic losses relating to data breaches today. So, GCA is working right now on a contemporary toolkit to minimize phishing, assembled by some of the leading cybersecurity experts in the world, including a team of specialists from Aetna. We'll share that kit among our members, ask them to apply it organization-wide, and then measure for success.

We want to give every collaborating member of GCA the ability to put the best, most current, and most aggressive protocols in place in order to reduce contemporary threats.

The truth is very clear to me: we cannot tackle a global threat like cybercrime without a concerted, collaborative, international response focused not on prosecution, but prevention. GCA's development of these toolkits – employing its in-house technical experts and experts from our GCA partners – is perhaps the only rational response to a cross-sector, global threat. It is a cross-sector and global strategy to defeat a cross-sector, global problem: energy talks to finance, who talks to health and hospitals, who talks to aerospace and transportation, who talks to municipalities like the City of New York – which is a GCA partner – and their work is shared across borders, not siloed within a country.

* * *

I'd like to close on an issue I believe is related. It relates to a new obstacle in our cybercrime investigations – and that is the provision of cloaking tools to cybercriminals by Apple and Google, two of the most powerful corporations in the world.

As recently as a year-and-a-half ago, when law enforcement officers seized a criminal suspect's iPhone or Android phone pursuant to a warrant, Apple and Google would comply with the judge's orders by extracting particularized evidence from the device as specified by the warrant, and sending the relevant evidence back to our prosecutors.

However, in September 2014, Apple and Google announced that they had reengineered their operating systems to be encrypted by default, and could no longer unlock their own products as a result.

Whether the motivating factor was concern for privacy or, as I suspect, to maintain market share in worldwide sales of smartphones, the effect is that iPhones – and certain phones running on Android – are now the first consumer products in history that are beyond the reach of judicial warrants. They are warrant-proof, and made to be warrant-proof.

The problem with that is: criminals, like all of us, now live their lives on smartphones. They communicate with each other, plan crimes with each other, and iMessage each other on their devices. Evidence that used to be stored in file cabinets, closets, and safes is now found on smartphones, including – just in our Office's cases – iMessages between sex traffickers and the victims they control, contact lists connecting criminal networks, and videos of shootings and homicides.

Right now, more than a thousand warrant-proof devices line the shelves of police and prosecutors' offices nationwide. In my Office alone, we now have 270 lawfully-seized iPhones running iOS 8 or 9 that are completely inaccessible. These devices represent hundreds of real crimes – committed right here in Manhattan – that cannot be fully investigated, including cases of homicide, child sex abuse, human trafficking, assault, robbery, and yes – cybercrime and identity theft.

One quarter of my Office's felony indictments now involve a cyber or ID theft element. The increasing prevalence of cybercrime is also reflected in our pile of lawfully-seized, inaccessible devices. Out of the 270 phones we have sitting in our Cyber Lab, 34 percent of them come from investigations *into* cybercrime, identity theft, and related larcenies and forgeries.

Talk about irony. In their purported effort to provide more cybersecurity to their customers, the companies have empowered cyber*criminals* to act with impunity.

I suspect that the federal San Bernardino case was the first time many of you learned about this issue. But the impact of smartphone encryption is felt most acutely in state and local prosecutors' offices, who handle 95% of criminal cases in the U.S. Until 2014, in case after case, we used smartphone evidence to hold criminals accountable and exonerate the innocent. Then Apple and Google adopted default device encryption in order to engineer themselves out of criminal investigations completely.

Now, many of you here today represent financial institutions, which are some of the most regulated companies in the U.S. As we learned more about how criminals were using banks to move money, Congress enacted laws to require them to file Currency Transaction Reports, to fight money laundering, and to better know their customers. Specifically,

Congress required banks to retain customers' data and make that data available to law enforcement when presented with a court order.

Over time, government and industry came together to work out compliance costs and procedures, and a broad consensus in favor of these rules emerged. The industry recognized that absolutism on customer privacy was not in its best interest. Banks and investment firms didn't want to be conduits for crime and terror.

A similar thing happened in the telecom space in 1994, when carriers were required to make access points available to law enforcement who had to execute a court-ordered wiretap. In nearly every other mature industry, you can find laws requiring and facilitating private companies' assistance with law enforcement investigations. But Apple and Google have engineered themselves out of these obligations; they have themselves decided where to draw the line between privacy and public safety. On a matter with such broad-reaching public safety consequences, I don't believe this public policy decision should be made by two giants who collectively operate more than 96% of smartphones worldwide. It should be made – as it has with other industries – by our elected representatives in the Capitol. Congress has got to step in.

Our office prosecutes more cybercrime and ID theft than most, so of course we understand the value of encryption. Put simply, people's smartphones can be as secure as are – quoting the Fourth Amendment – their "person, houses, papers and effects." That's the reasonableness standard that has guided our access to information since our country was founded. We can keep smartphones encrypted, but answerable to judges' warrants. And, using that time-tested standard, that's how it worked without any documented problems up through iOS 7, the last Apple operating system before they added this new level of encryption. At the time, Apple billed iOS 7 as offering the ultimate in privacy and security.

We've outlined all of this in our Report on Smartphone Encryption and Public Safety, which is available on our website at ManhattanDA.org. I encourage you to read the report, and then evaluate the dire warnings we hear from the other side. Silicon Valley says that what we want will jeopardize the security of millions of people around the world. But they never cite a single example of how complying with these court orders – which they did routinely until 2014 – ever resulted in anyone getting hacked, or resulted in the compromise of any smartphone.

In short, they haven't provided ample justification – backed up by data, not rhetoric – for why it is necessary to provide terrorists and criminals with unprecedented, evidence-free zones. I believe it is simply a matter of time before another case involving national security – or the path to justice for some vulnerable victim – is blocked unconscionably, and at that time we will understand that we have paid too high a price as a country for the purported security benefits we are told we receive from device default encryption.

Whether you agree with me or not, I urge you to lend your voice to this debate. Especially if you agree with me.

Thank you for the opportunity to speak today. I'm eager to take your questions.

###