American University Business Law Review

Volume 4 | Issue 1 Article 1

2014

United States Assistant Attorney General For National Security John P. Carlin Delivers Remarks At The American University Business Law Review 2014 Symposium

John P. Carlin
Harvard University

KEYNOTE

UNITED STATES ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY JOHN P. CARLIN DELIVERS REMARKS AT THE AMERICAN UNIVERSITY BUSINESS LAW REVIEW 2014 SYMPOSIUM

JOHN P. CARLIN*

Thank you for that kind introduction – and for inviting me here today. It's a pleasure to be back at AU, and a privilege to join so many experts, essential partners, and good friends in advancing one of the most important conversations currently facing government and private sector leaders across the country.

At the Justice Department's National Security Division, there is little we do that is more important than working on how the government can partner with private companies to protect our nation and its people better – from terrorism, from cyber-attacks, and from a range of other malicious activities.

This past December, I attended a ceremony marking the twenty-fifth anniversary of the bombing of Pan Am Flight 103 over Lockerbie, Scotland, which claimed the lives of 259 people on the plane and 11 on the ground. 189 were Americans. It was the deadliest act of terror against the United States prior to September 11th.

The families and friends of those who were lost came together that winter day at Arlington National Cemetery to recall the event that changed their lives forever. They spoke movingly of loved ones who had been on

*John P. Carlin, J.D., Harvard University 1999, is the United States Assistant Attorney General for National Security. Confirmed in April 2014, Mr. Carlin oversees nearly 350 federal employees responsible for protecting the United States against terrorism, cyber-threats, and other significant national security threats.

board that plane, many of whom were American college students flying home for the holidays.

On December 21, 1988, instead of reuniting with their companions and loved ones, they heard news reports of a catastrophic explosion and wreckage strewn over miles of the Scottish countryside. Shortly thereafter, they learned, as did the rest of the world, that terrorists were to blame.

There was a call for justice – to find the perpetrators and hold them responsible. And there was also a call for new security measures designed to stop another attack from happening.

At the ceremony last winter, former Secretary of Labor Ann McLaughlin Korologos spoke of her experience leading the seven-member Presidential Commission on Aviation Security and Terrorism that was formed a few months after the attack to investigate what went wrong. Eighteen months after Lockerbie, that Commission issued a report calling for national attention to our aviation security system, and identifying a host of specific proposals intended to harden our nation's airline security and keep all Americans safe – both at airports and in the skies.

Many of these measures did not become reality. Interest faded, attention waned – and so did political and social will. Twelve years later, the horror of 9/11 changed that. It reinvigorated the focus on aviation security – and the 9/11 Commission called for many of the same security measures called for in the wake of Lockerbie. This time, almost all of them were implemented.

Today, national leaders in both government and private industry must apply the lessons we learned from unspeakable tragedies like these, and from decades of effective counterterrorism policy, to business action in cyberspace. It is imperative that we take action promptly, without waiting for a galvanizing tragedy. We can work together to change norms now—not in the wake of an immensely damaging terrorist cyber-attack. In doing so, we will have a much better chance of preventing such an attack from ever taking place.

I grew up in New York City, a place where you can experience the anonymity now enjoyed by so many on the Internet. And when I was a kid, the NYPD sent an officer to our school who told us how to conduct ourselves on the streets of New York.

Our version of Officer Friendly told us to look both ways when we crossed the street. Of course, he told us not to make eye contact with people on the street—which was pretty standard advice back then.

As a kid, that seemed to make total sense. Decades later, New York City is now one of the safest major cities on the planet. And when we look back at that advice, it seems crazy that there was a consensus of blaming the victim for making eye contact. These days, on the internet, we tell our kids

to beware of chatting with individuals they don't know, to avoid certain websites or apps.

When a person's credit card gets stolen, or their credentials for accessing a social media site or their bank are hacked, we tell them, "You should have known better than to go to that website," or, "You shouldn't have used the same 18-character password more than once." Together, hopefully, we can look back in a few short years and think that that those warnings and the victim-blaming is also strange and that we've come a long way with regards to cyber security.

One of the things that's changed in New York over the years is its social norms – like making eye contact. We need to shape social norms in the cyber area, too. Just as it was in a chaotic urban environment, it's tricky to cultivate trust in cyberspace. There were streets in New York where the bad guys and the good guys passed each other shoulder to shoulder. The same thing is true in cyberspace. Legitimate businesses and innocent customers use the same Internet that hackers and terrorists use.

As my former boss at the FBI, Bob Mueller, explained, bad actors – specifically terrorists – are using cyberspace for at least three discrete aspects of terrorist activity: (1) to propagandize and recruit; (2) to plot and plan attacks in the physical world; and (3) to launch attacks in the virtual world itself. It's hard to cultivate trust online amidst such company and to restore a sense of security.□But like change in New York, change in cyberspace will be a community effort. When our Officer Friendly came to visit, he told us about Safe Havens – businesses that opened themselves up just a little bit, to be better members of the community, and to provide a place for people to go if they felt threatened. Back then, there were little yellow Safe Haven signs on the doors of stores in New York, and he told us, "If you're feeling uncomfortable or scared, or are being targeted, don't be afraid to go into one of these stores and seek help. Your safety should be your first priority."

Just as those Safe Havens existed as trusted businesses when I was kid, the government and the corporate community can come together to create safe havens in cyberspace.

We need to work together to prevent terrorists from using networks – using the very websites and apps we use every day – to plot attacks in the physical world. And we need to shore up our security so that devastating attacks cannot be launched in the virtual world. These tasks are not easy, and they are ones we need to undertake with care, to strike a proper balance between security and liberty.

Some businesses, especially those in the communications sectors, may be hesitant to build new partnerships with government – or are drawing back from their current partnerships – because of the national discussion

that has taken place over the last year.[]The President has committed to providing greater transparency about the government's lawful use of data collection authorities. However, as the President has noted, the nature of some unauthorized disclosures have shed more heat than light. And that heat has come onto companies as well, often unfairly. We take their concerns seriously, and we are dedicated to increasing transparency as well as protecting civil liberties. That is why many layers of checks and balances are built into the systems – without question some of the best protections provided by any country in the world. Our authorities are rigorously overseen by Congress, and often scrutinized by the courts and independent government watchdogs. And they are aimed at ensuring the safety of the nation and our allies.

Of course, the private sector should not be punished for complying with the law. We are concerned about this issue, and we are dedicated to working with companies to address misconceptions, correct misinformation, and help to rebuild the public's confidence that our partnerships are conducted under the law. We are working with industry to help them be more transparent about what kinds of information they are required to share with the government, and how very few of their customers are ever impacted by government actions.

Yesterday's announcement by the President of a way forward on the handling of telephony metadata indicates just how committed the Government is to ensuring that the public's concerns are addressed, without the Government sacrificing certain operational needs. As you might have heard, the President announced a proposal that will, with the passage of appropriate legislation, allow the government to end bulk collection of telephony metadata records under Section 215, while ensuring that the government has access to the information it needs to meet its national security requirements.

Getting our legal policies right is one thing. But make no mistake: It will lead to tragedy if the ultimate result of these disclosures is to cause businesses to shy away from working with the government to prevent terrorism. The undeniable truth is that our collaboration, and the protections we have put in place together, make us safer from those who would attempt to do us harm – from terrorists to hostile nation-states seeking to capitalize on our vulnerabilities.

One example that comes to mind is the case of Khalid Aldawsari, a college student from Saudi Arabia who took chemistry classes at Texas Tech in Lubbock, Texas. When he began placing large and unusual orders for chemicals online, the chemical company reported the order to the FBI, as did the shipping company. Ultimately, he was convicted in federal court and sentenced to life in prison for trying to use those chemicals to make a

bomb, potentially to attack a former President. And heading off that threat all began with two companies taking the right step of alerting the FBI to suspicious activity.

Whenever the public faces a threat, whether from terrorists, computer hackers, or pick-pockets on the Metro, people expect the government to protect them. But the government can't do it alone. And that is particularly true in the context of cyber threats, given just how much of our nation's most essential information is found online and, in particular, in the hands of private companies.

You know the threats we face. You've seen them firsthand. Although we often think of the government and our brave men and women serving abroad as a primary focus of terrorist attacks, we must keep in mind that the 9/11 attacks targeted this nation as a whole, and its impact was felt by all of us.

Since then, terrorism is now increasingly diverse and decentralized, from al Qaeda affiliates overseas to homegrown terrorists – such as the Boston Marathon bombers – who may live in the communities they intend to strike. But the cyber threat is growing rapidly, and down the road, may rival or even surpass the threat we face today.

Malicious cyber actors are an increasing risk to our security and prosperity. Last year, BP's CEO stated that his company sees approximately 50,000 attempted cyber intrusions each day. And he is not alone.

As you know, hackers – in many cases working for foreign states or organized criminal syndicates – break into private businesses' servers and steal the key intellectual property that gives us a competitive edge in the global marketplace. And malicious cyber actors sometimes target companies' infrastructure. In 2012, Saudi Arabia's state oil company, Aramco, suffered an attack that destroyed 30,000 of its computers – nearly 75% of its workstations, a devastating loss for any company.

Many of these same hackers exploit vulnerabilities in software, turning home computers or servers into launch pads for malicious denial-of-service attacks against banks, companies, and government agencies – shutting them down and disrupting their ability to do business. It does not take much imagination to see how these same tools could be used by terrorists, resulting in what has been referred to as a potential "cyber 9/11."

When these attacks happen, people ask the same two basic questions many asked after the Lockerbie bombing: "What more could have been done to protect me?" And, "are they going to get these guys?" To answer these questions, we need the private sector and the government to work together.

Intrusions by nation-states have gone on longer than acknowledged.

Why are so many companies waiting to come to the government for help? This situation is not unlike the way that organized crime was able to intimidate small businesses into paying for so-called "insurance" . For each mom and pop store, individually, it made more sense to pay the insurance rather than face retaliation for speaking up or going to the cops. And as a result, the criminal organizations made big profits. They only took a small amount from each business, but the money added up over the dozens or hundreds of businesses they intimidated. It wasn't until the cost of doing business with the mafia got too high – or someone was brave enough to stand up to the mob – that law enforcement was able to break up these organized crime rings.

The calculus that many businesses make today is similar to the decisions that the mom and pop stores had to make several decades ago: Does the cost of paying out – that is, failing to tell the authorities about cyber attacks – outweigh the costs of potential retaliation? When faced with the prospect of taking on a nation-state with all of its powers – not to mention the fear of not being able to do business in that's nation's marketplace – many companies have made the calculation of remaining silent.[ ]But the cost of that silence is increasing. As valuable assets, proprietary information, and research and development investments are repeatedly compromised by increasingly relentless attacks, businesses can no longer afford to stay silent victims. The calculus has changed. Companies are taking action.

Over the last year, we have seen a tipping point. As more and more companies come forward, more and more will feel emboldened. Eventually, these nation-state hackers – just like the mafia – will lose the ability to intimidate victims.[]Public-private partnerships are particularly important because of the key role that businesses play in our society. Unlike some countries, where government maintains control over the telecommunications and energy industries, nearly all critical infrastructure in the United States is owned and managed by private companies. The fiber-optic cables that our communications transit; the servers that direct our Internet traffic; the software that allows us to communicate; and the energy we use to power our daily lives – all of these things, and so many more, are created and operated by private companies.

We thrive as a nation because of private innovation, and the creativity that comes with the freedom to innovate. This has been true throughout our history. But these unique strengths also create opportunities for attacks. When attacked, companies are often in the best position to protect themselves and their customers from cyber aggressors. But they may not always be in the best position to know the precise threats they face, which is where we can help.

Take, for example, the Department's work on cyber threats. On a daily

basis, the FBI is working with companies that have been the victims of hacks – many of whom may not even know they have been victimized, or how to protect themselves. The Washington Post reported earlier this week that federal agents notified more than 2,000 U.S. companies last year that their computer systems were hacked – and, as the article explained, even that considerable figure represents only a fraction of the actual number of cyber intrusions into the private sector.

There are many efforts underway across the government to work with private corporations on strengthening public-private cyber cooperation. The Department of Homeland Security, the Department of Energy, and other departments and agencies routinely work closely with companies to protect critical infrastructure.

In driving this work forward, the FBI has long relied on its InfraGard program, which brings together individuals in law enforcement, government, the private sector, and academia to talk about how to protect our critical infrastructure. InfraGard has more than 85 chapters across the country, with more than 47,000 members.

These are all positive and important efforts, but we have to do more.

As we speak, the Department of Justice is working hard to be a more accessible partner to companies. Over the past two years, the National Security Division established a national program to focus on cyber threats to the national security – those posed by terrorist and nation state actors – and we are continuing to grow. We are still a very new Division, but we are evolving quickly to meet new and emerging threats.

The story of NSD's creation is an interesting one. Although not formally created until 2006, NSD's story begins, like so many others, with calls for reforms that were first spotted years ago. We trace our origin all the way back to 1978, with the passage of the Foreign Intelligence Surveillance Act. FISA was, in part, a response to public and congressional dissatisfaction with a series of intentional abuses of wiretaps and surveillance for political purposes. The Church Committee's report set out those problems and made a case for reform. The report emphasized that the Attorney General, as the nation's chief legal officer, plays an essential role in maintaining the lawfulness of actions by our country's intelligence agencies. NSD was created, and is proud, to execute that mission decades later on his behalf.

So as we tackle the cyber threat, we build upon our roots. We were created so that prosecutors and law enforcement officials could work smoothly and effectively with intelligence attorneys and the Intelligence Community, to ensure that we most effectively defend our nation's security while at the same time protecting our vital civil liberties. And I would be remiss in describing the vital work of our Division if I neglected to acknowledge this week's conviction of Sulaiman Abu Ghayth in New

York. Abu Ghayth, described as a senior spokesman for Osama bin Laden and al Qaeda, was convicted by a federal jury on all counts, including conspiring to kill Americans and other terrorism charges.

So, even as we defend our national security through successful counterterrorism prosecutions in federal court, we also defend our security while protecting our civil liberties in cyberspace. In 2012, we established the National Security Cyber Specialists' Network, with members from across all of our areas of expertise, federal prosecutors from each and every U.S. Attorney's Office, and partners from the Department's Computer Crime and Intellectual Property Section, who have had longstanding and continuing success against organized cyber criminals, hacktivists, criminal fraudsters and other bad actors.

Since then, we have hosted extensive training for these network members and for every member of the National Security Division, to ensure we have the skills we need to tackle the threat. Federal prosecutors across the country are reaching out to companies in their districts to let them know about the network and how we can help.

Here in our nation's capital, we work closely with the FBI's National Cyber Investigative Joint Task Force to assess cyber issues in real time as they arise. We've launched a 24/7 cyber response capacity. We are now a one-stop shop and resource for national security cyber matters across the country.

There are criminal cases to be brought against these actors, but that is just one tool. We are committed to using every tool at our disposal, law enforcement and others, to disrupt adversaries' activities and prevent damage to U.S. national interests – just as we do in other arenas of counterterrorism, counterespionage, and export control.

We are drawing from our expertise in those areas, and building new capabilities to ensure that we can use all available tools to meet a range of constantly-evolving threats.

Employing this comprehensive, "all-tools" approach means we need to be prepared not only to prosecute cyber intrusions, economic espionage, and export control violations, but also to work with our partners to enforce other civil and regulatory laws.

We cannot do this alone. This "all-tools" approach requires trusted collaboration, including with operational and legal experts in the private sector.

It's often said, there are only two types of companies: those that have been hacked and those that will be. Now, that's no longer the case. Today, there is only one category: those that have been hacked, and that will be hacked again.

Going forward, we want to work even more closely with our private

sector partners to be ready for whatever may happen in the near future. Of course, private companies will remain our first line of defense, and their legal teams must be prepared to face difficult questions and complex matters, including how to respond to cyber breaches; how to interpret and comply with the cyber Executive Order and the cybersecurity framework recently released by the Administration; and, how to stay on top of the evolving "standard of care" for cyber security.

All of us – including lawyers and operators in the public and private sectors – will need to cooperate closely to address these and associated threats. We all must act on the premise that success requires reporting from, and close relationships with, victims and potential victims who seek indicators of malicious activity.

My colleagues and I have already met with a number of private entities and received a positive response, and we will continue these meetings to keep the dialogue going.

And as we look toward the future, we must continue establishing channels that regularly communicate cyber threat information between the public and private sectors. Information must move in both directions. It is an approach that works in other contexts, and it will succeed here as well.

We have come a long way in our collective approach to counterterrorism. Together, we have improved airline safety, hardened critical infrastructure, developed new technology that can help first responders, and designed a wide range of protective measures. These measures, of course, don't eliminate the threat of to our national security, which remains very real and very dangerous. But we are safer than we used to be, and better prepared to cope with any potential attack.

We need to achieve this same success in the cyber realm. So the critical question is: What will it take?

We've certainly had plenty of attacks that caused real pain, exposed real weaknesses, and suggested real problems for the future. Yet, despite all of these warnings, we don't seem to have fully turned the corner in addressing this threat. And the reasons for that are understandable.

Confronting cyber threats incurs real economic cost. We appreciate that. But doing nothing will cost us all more in the long run, and may, for some businesses, prove devastating.

The writing is on the wall – our adversaries are getting bolder, more aggressive, and more skilled. They flex their muscle to show us what they can do, but it is only the tip of the iceberg. Without a concerted, collective effort to make the changes needed to protect ourselves in cyberspace, it is only a matter of time before we are really hit – hard. Far better to form partnerships and make the required investments before a large-scale attack takes place.

Indeed, perhaps even more than in the terrorism context, the private sector is critical to our success in the cyber context because of just how much vital information is now held "in corporate trust," so to speak.

While government holds and protects some of what cyber terrorists want to access, the private sector has much, much more. So, whether it's about ensuring that our electric grid is safe from attacks – whether physical or cyber – or making sure you can access your bank account information on your smartphone without getting hacked, we urgently need to form the type of public-private partnerships to keep those vital resources safe. These are the type of partnerships we've created for counterterrorism. We must build on those partnerships to combat cyber threats – not pull away from each other.

This is the challenge now before us – and this is the cause that everyone in this room, and many beyond it, must come together to confront. Each of us has a unique role to play, and distinct responsibilities to fulfill.

Leaders in government can articulate precisely what we have to offer the private sector. Leaders in the private sector can demonstrate what these partnerships have to offer to their customers. And leaders in academia can survey the legal authorities we have – and take stock of what legal authorities we don't have but need – to facilitate cooperative, productive cyber partnerships. We can build these partnerships while respecting civil liberties and do it in a transparent and productive way.

We are committed to meeting regularly with critical partners to get your feedback on how we are doing; to solicit suggestions on how we can do better; and to gain the benefit of your views on how the overall landscape is looking. Please reach out to us so that we can talk more about what NSD does, and how we can work together to keep you safer and our nation safer.

I want to close today by calling upon everyone here to continue the important open dialogue we're holding here at AU today. I urge you to serve as connectors – as bridges – to make private-public partnerships a reality.

We had warnings before 9/11. But we didn't act – at least not enough. The state of security of the Internet today is a rumbling storm in the distance. We need to be smart and work together, now, before a cyber-9/11 – before there's an attack or intrusion or exfiltration so big – and so devastating – we are forever changed. Thank you for participating in this important conversation, and thank you for having me here today.