Journal of Technology Law & Policy

Volume XIV – Spring 2014

ISSN 2164-800X (online)

DOI 10.5195/tlp.2014.144

http://tlp.law.pitt.edu

Creating a Model of Cyber Proficiency: Remodeling Law Enforcement Tactics in Pittsburgh to Address the Evolving Nature of Cybersecurity

An Interview with The Honorable David J. Hickton, United States Attorney for the Western District of Pennsylvania

Elizabeth Orton and Chris Schlag

Creating a Model of Cyber Proficiency: Remodeling Law Enforcement Tactics in Pittsburgh to Address the Evolving Nature of Cybersecurity

An Interview with The Honorable David J. Hickton, United States Attorney for the Western District of Pennsylvania

Elizabeth Orton[*] and Chris Schlag[†]

INTRODUCTION

David J. Hickton is the current U.S. Attorney for the Western District of Pennsylvania. He was sworn in as the 57th U.S. Attorney for the District on August 12, 2010 after being nominated for the position by President Barack Obama. Prior to his nomination, Mr. Hickton had been a co-founder of the Pittsburgh firm, Burns, White & Hickton LLC in 1987. He had also been an Associate Attorney at Dickie, McCamey & Chilcote from 1983 to 1987. Mr. Hickton began his legal career as a Law Clerk for the Honorable Judge Gustave Diamond after graduating from the University of Pittsburgh School of Law in 1981. Throughout his career, Mr. Hickton has taught as an Adjunct Professor of Law at the Duquesne University of Law and has participated as a Fellow in the American College of Trial Lawyers and Academy of Trial Lawyers of Allegheny County. In addition to his legal work, Mr. Hickton has been involved in a wide range of community activities and an active participant in organizations focusing on child services and performance arts. Since his appointment, Mr. Hickton has worked on restructuring the U.S. Attorney's Office through developing new sections within the Criminal Division to focus on Civil Rights and Exploitation and National Security and Cybercrime. The new National Security/Cybercrime section has allowed for improved efforts to enhance national security, better preparation for and response to cyber attacks upon critical infrastructure and cyber espionage, and investigation into and prosecution of sophisticated computer fraud schemes. Cybersecurity has been a persistent, primary focus of Mr. Hickton's while in office. This focus ultimately

[*] J.D. candidate, University of Pittsburgh School of Law, May 2014. She is also the Lead Articles Editor for the Pittsburgh Journal of Technology Law and Policy Academic Year 2013-2014.

[†] J.D. candidate, University of Pittsburgh School of Law, May 2014. She is also the current Editor in Chief for the Pittsburgh Journal of Technology Law and Policy Academic Year 2013-2014.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.144 ● http://tlp.law.pitt.edu

led to Mr. Hickton's creation of the Pittsburgh Cyber Security Initiative in 2013, which leverages the resources of both public and private entities to more adequately respond to cyber security threats.

Cybersecurity has quickly become a focal point in modern law enforcement. With recent and significant cyber attacks such as the backdoor theft of Target consumers' credit card information and the Heart Bleed Virus' collection of millions of users' online profiles and passwords, it is clear that one well executed cyber attack can result in a massive loss of consumer data, information corrosion, and financial theft. It is for this reason, that Mr. Hickton describes computers and computer servers as being relevant to all federal law enforcement and a centralizing factor in the evaluation of modern crime.

The Internet, which is essentially a cyber platform, has changed both business and personal communication around the world by allowing for increased speed and efficiency in communication transactions. The Internet has also allowed for the development of serious and harmful cyber crimes that are diverse and international in nature, ever evolving, and committed by sophisticated criminals. For example, with the combined development of the cyber platform and resulting exposure of criminals and predators to the internet, internet crimes involving child exploitation, identity theft, cyber theft, and cyber terror have become a much more frequent occurrence. Mr. Hickton describes the diversity of the resulting cyber threat as having "many spokes on the wheel," such that law enforcement must be extremely vigilant and aggressive in investigating cyber attacks and fully prosecuting cybercrimes.

Mr. Hickton has specifically reorganized the U.S. Attorney's Office for the Western District of Pennsylvania to fully address the changing nature of information systems and cybercrime. By establishing the National Security and Cyber Section, which prosecutes domestic and international terrorism and threats to our national security, the U.S. Attorney's Office now has a resource for investigating and prosecuting cyber attacks upon public and private entities, as well as critical infrastructure. His creation of a cyber task force and cyber terrorism task force within the National Security and Cyber Section has ensured that Pennsylvania has an effective team available to investigate and prosecute electronic crimes, large-scale fraud cases involving identity theft, and cyber terror. The National Security and Cyber Section has been instrumental in promoting awareness of cybercrime, the need for private and public sector cooperation to address the problem, and establishing best practices for law enforcement to investigate and prosecute cybercrime offenses.

Mr. Hickton believes that even with the establishment of a strong law enforcement team, law enforcement will continue to face significant challenges in the area of cybersecurity. The first and primary challenge faced in cybersecurity is

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.144 ● http://tlp.law.pitt.edu

the fact that the internet provides for a significant amount of anonymity. Uncovering and prosecuting a cyber criminal can therefore be significantly challenging and require modern and creative investigation tactics. The second challenge, Mr. Hickton explains, is in balancing the need to aggressively investigate and prosecute cybercrimes against an individual's reasonable right to privacy. The third challenge faced by law enforcement is the fact that cyber crime has no geographical borders and is often perpetrated by multinational actors. To illuminate this challenge through a real world application, Mr. Hickton pointed to the recent University of Pittsburgh hoax bomb threats, where it was determined that at least one of the individuals involved in the threats perpetrated the attack by email in Ireland. Finally, Mr. Hickton stated that because cyber criminals are very creative, can quickly change the method of a cyber attack, and are able to eliminate their cyber fingerprints; law enforcement needs talented, sophisticated, and knowledgeable personnel to be effective.

Mr. Hickton confirmed that cybersecurity implicates a significant number of legal issues. In addition to the constitutional concerns related to privacy that are implicated by law enforcement's investigation and prosecutorial efforts, there is also a significant concern over the rapid evolution of technology. Mr. Hickton specifically explained that this is because rapid changes in technology make it difficult for law enforcement to keep pace. He referenced the advancement of instant messaging and social media through such sites as Snapchat, Tumblr, and Instagram, which have in effect made Facebook largely less relevant, as an example of the fast paced changes in internet use. Mr. Hickton similarly noted that the individuals who use these web sites and overall knowledge of internet users have also changed overtime.

Mr. Hickton stated that one important legal issue implicated by cybersecurity is the need for reformation of the Mutual Legal Assistance Treaties. Mr. Hickton explained that Mutual Legal Assistance Treaties, which are essentially formal agreements between two or more countries for the purpose of gathering and exchanging evidence in an effort to enforce criminal laws, were largely developed in a pre-cyber era and may not meet current cybersecurity needs. Mr. Hickton stated that Mutual Legal Assistance Treaties specifically need to be amended to address the more fast-paced modern cyber landscape so that the international community could more effectively partner with law enforcement efforts.

Mr. Hickton said that even though cyber threats are significant and should not be discounted; there are a number of things that consumers can do to protect themselves against cyber attacks. First, consumers should establish a strong defense by installing and using a firewall with whatever cyber device they are using. Second, consumers should ensure that they have strong online passwords, that are changed frequently, and which are not shared or discernible by other people. Third,

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.144 ● http://tlp.law.pitt.edu

consumers should be extremely cautious with sharing financial information on the internet and should take steps to protect their cyber data. Finally, Mr. Hickton recommends that consumers and operating businesses, consider hiring a cybersecurity expert to clean up, diagnose, and fortify cyber defenses of their current system.

With the significant advancements made in cyber technologies, cyber use, and cybercrimes, cybersecurity has become a significant focal point for law enforcement, businesses, and consumers. Under Mr. Hickton's continued guidance, the U.S. Attorney's Office for the Western District of Pennsylvania has not only become but will continue to be a leader in cybersecurity expertise. His creation of the Pittsburgh Cyber Security Initiative will help the Pittsburgh region establish best practices for cybersecurity and act as a center for excellence in cybersecurity ingenuities. Furthermore, under Mr. Hickton's continued direction, Pittsburgh will establish cyber education at all levels and continue to recruit knowledgeable cyber professionals so that Pittsburgh will mature as a model of cyber proficiency in both overall cybersecurity efforts and prosecution of cybercrimes.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.144 ● http://tlp.law.pitt.edu