



SEARCH HIGH-TECH CRIME TRAINING SERVICES

State of the States Cyber Crime Consortium
—2014 Meeting Recap—

By Justin Fitzsimmons
Program Manager, High-Tech Crime Training Services
SEARCH

On May 1, 2014, the Office of the Massachusetts Attorney General, along with SEARCH, Microsoft, and the National White Collar Crime Center, hosted the 2014 State of the State's Cyber Crime Consortium meeting in Norwood, Massachusetts.[1] *The purpose of the meeting was to facilitate a roundtable on the current state of technology-facilitated cases around the country. The group discussed a variety of topics and viewed presentations by invited speakers.*

More devices = more data = more hours required for analysis

Discussion centered on the amount of data and number of devices commonly found at crime scenes. Participants said that it was common to encounter 6-12 different devices that are capable of storing data. Additionally, many participants described how it is common to seize multiple terabytes of information at crime scenes, dramatically up from 250-500 gigabytes of information commonly found just a year or two ago. The cheating scandal in the Atlanta school district was mentioned as one example of the overwhelming amount of data and the number of devices for one incident. In this case, over 50 hard drives were turned over to law enforcement at once. Participants agreed that is was not only the number of devices and size of the storage data that was concerning, but also the amount of hours required to analyze the large amount of data seized.

[1] Participants included representatives from Alaska, Arkansas, California, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Maine, Massachusetts, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Oregon, Pennsylvania, Rhode Island, South Carolina, Texas, Utah, Vermont, Virginia, Washington, Wisconsin, and Wyoming.

The need for collaboration and team building

Discussion turned to the need for command staff and elected prosecutors to understand the importance of team building among investigators, forensic examiners and prosecutors. This led to a discussion about the lack of resources for departments, and the type of specialized training needed to develop either a unit or an individual officer capable of investigating technology-based cases. Participants created a list of the types of sub-specialty training topics that would benefit law enforcement. Topics include computer forensics, cell phone extractions (including the advanced level of removing evidence from chip-offs), tablet device forensics, gaming device forensics, and network forensics. The group cited the lack of resources to provide continued training and the expense of necessary tools and licensing updates as significant burdens on agency budgets.

***Brady* and forensic images**

The data discussion led the group to consider what satisfies discovery requirements under *Brady* for prosecutors in court. One participant explained how he had spoken with many prosecutors on the topic as it related to whether the burden was met with access granted to the defense to review forensically imaged drives, or whether the discovery obligation was greater. They posed these questions: Does *Brady* require prosecutors to turn over a forensic image? Does it require prosecutors to point out potentially exculpatory evidence on the forensic image, or is access enough? Most agreed that access to the forensic image would satisfy any *Brady* obligation.

Law enforcement's role in network intrusion cases

Participants cited several examples of recent network intrusion cases, including an estimated $3.8 million breach at the Department of Revenue in South Carolina. Another example was a breach at the Florida Department of Children and Family Services, where the names and Social Security numbers of approximately 200,000 people were accessed and sold to third-party buyers. Participants discussed the role of law enforcement in responding to intrusion cases, with many indicating that their state lacked any law enforcement agency having the technological background, training, expertise, or resources to respond to such attacks. They discussed the role of federal law enforcement agencies versus private outside groups in responding to large data breaches. Participants indicated that it was not just the highlighted large breaches of major state agencies that was concerning. They pointed out that it's a challenge when small businesses approach local law enforcement about potential breaches and local law enforcement does not have the ability to adequately respond.

State court judges refuse to allow extraterritorial search warrants

The case of *State v. Mello*, 162 N.H. 11, 27 A.3d 771 (N.H. 2011), was used as an example of a State Supreme Court's restricting the use of search warrants to in-state entities. In that case, the State issued a search warrant for the subscriber data from the Comcast located in New Jersey. The trial court denied the defendant's motion to suppress the search. The Supreme Court of New Hampshire outlined two appropriate methods to obtain subscriber data, either through subpoena to the Keeper of Records to appear with the information, or written demand of the attorney general of the state where a belief that the subscriber information may be used for an unlawful purpose. The Court held that a New Hampshire Court has no authority to issue a search warrant outside the state. Participants discussed the ramifications of this opinion and indicated how states' long-arm jurisdiction statutes may be used to avoid this problem. Several participants discussed their individual statutes and the provisions that allow for out-of-state service of legal process.

Comcast X1 and wi-fi hotspots

The meeting included a presentation by a participant who had recently met with Comcast to discuss the company's new X1 Entertainment Operating System. According to the presentation, the X1 system creates, in effect, a single device capable of broadcasting two different wi-fi hotspots. One is the traditional wi-fi hotspot that a user creates. This hotspot has the option of encryption and is only accessible through password protection. However, the second wi-fi hotspot is public, and anyone with a Comcast account can access it simply by logging into his/her Comcast account. This second public hotspot accesses the web through NATing (Network Address Translation), and through NATing there can potentially be multiple users on the public side of the hotspot. The presenter explained that the recovery of information by law enforcement on the private, traditional hotspot does not change with X1 and it is separate from the data on the public side. However, on the public side, since multiple users can potentially be on one hotspot, law enforcement needs the port number from the ISP or webpage to determine which user is accessing the contraband material. The presenter indicated that this might be an issue, because it is uncertain whether the individual webpage owners, ISPs or web-based applications are keeping porting information.

Accessing cloud-based storage

(At the time of the meeting the U.S. Supreme Court had not rendered the opinion in the *Riley-Wurie* cases.) The issue was raised on what an on-scene officer should do when a device is on and running a program that is accessing a cloud-based application or storage. Participants discussed whether the officer could simply access the data or would need to get a warrant. Most agreed that a warrant would be necessary. Next, the group introduced hypotheticals that created exigent circumstances—they agreed these would allow law enforcement to access the cloud-based data. Law enforcement would first need to make a forensic copy and then seek a warrant to look at the copy. Participants pointed out that unless the data was accessed and copied at that point, it could potentially be lost and unrecoverable based on current encryption techniques. The search and seizure of cloud-based information led to a discussion about how long information could be retained and viewed by law enforcement. The group discussed several federal district court cases that limit the amount of time law enforcement can access data and the scope of the forensic examination. Participants universally agreed that it is almost impossible to try and explain the entire process of a computer forensic examination of a digital device in the affidavit for a search warrant, adding that each device and case requires a different analysis. Participants expressed a need for accepted standards and best practice documents and training materials regarding cloud-based storage, saying this would be beneficial for law enforcement and prosecutors.

This project was supported by Cooperative Agreement #2010-BE-BX-K022, awarded by the Bureau of Justice Assistance, U.S. Department of Justice. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the SMART Office, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice.