SEARCH HIGH-TECH CRIME TRAINING SERVICES

State of the States Cyber Crime Consortium —2015 Meeting Recap—

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

On April 30, 2015, the Office of the Massachusetts Attorney General, along with SEARCH, Microsoft, and the National White Collar Crime Center, hosted a gathering of law enforcement and prosecutor subject matter experts[1] for a State of the States Cyber Crime Consortium meeting. This meeting followed the 2015 National Cyber Crime Conference that was held in the preceding days in Norwood, Massachusetts. The purpose of the meeting was to have a roundtable on issues related to the investigation and prosecution of cases facilitated by the use of technology. This paper recaps that meeting and offers insight into the status of digital evidence challenges in law enforcement today.

Technology Issues Identified

During the course of participant introductions, each individual had the opportunity to describe any issues at a state or local level related to handling technology-facilitated crimes or issues dealing with any aspect of technology throughout an investigation or prosecution. Many of the participants agreed that issues raised were similar across state lines. Some of the issues discussed include:

- Encryption
- The amount or size of data seized in cases, and the resulting backlog of forensic examinations or data extractions

[1] Participants included representatives from Alaska, Arizona, Arkansas, California, Delaware, Florida, Georgia, Idaho, Illinois, Indiana, Maine, Massachusetts, Mississippi, Nebraska, New Jersey, New Hampshire, New Mexico, North Carolina, Rhode Island, South Carolina, Texas, Virginia, and Wisconsin.

- The evolution of technology, and the rapid pace of applications changing and offering new areas of potential evidence
- Revenge porn legislation
- Search and seizure, and the need to domesticate legal process across state lines
- Training of police officers, prosecutors and the judiciary
- Retaining well-trained officers
- Tiered forensics
- Responding to changing case law that finds a higher level of privacy for electronic devices and cell site location data
- Restitution issues for victims of child exploitation

The Snowden Effect

A common undercurrent to many of the difficulties facing state and local investigators and prosecutors is the continued fallout from the Edward Snowden disclosures. Many participants noted they were combatting this effect in court, with the judiciary adding ex ante conditions to search warrants. Others cited the difficulty of getting information from Internet Service Providers without providing notice to the target of the investigation. Several participants indicated that their state legislatures are currently considering amending the state equivalent of the federal Electronic Communications Privacy Act (ECPA). In most cases the legislatures are considering removing the lower threshold of subpoenas for subscriber information and court orders for transactional data. State legislatures are instead considering legislation that would require law enforcement to issue a search warrant for any and all information from Internet Service Providers.

Device Encryption

Participants discussed the implications of mobile device providers increasingly introducing operating systems that encrypt data. According to the providers, the encryption is unbreakable and there is no type of backdoor access to the information; once a device is locked, it is no longer accessible without the password. The arguments presented in the case of *Commonwealth v. Leon I. Gelfgatt* (468 Mass. 512) were discussed as a possible solution to some of the encryption issues. Participants talked about the basis of this brief that was successfully argued to the Massachusetts Supreme Court, and it was offered as a possible approach to combating the encryption of a device.

Warrants for Cloud-based Storage

Regarding cloud-based issues, participants discussed the role of exigent circumstances for seizing information from cloud-based storage for an open, running, and attached device.

This question was posed: Would a traditional warrant for any digital devices on the premises cover any cloud-based applications that were running and accessible at the suspect scene? Additional information was added to the hypothetical: Would the presence of the suspect at the scene matter? Participants agreed that if the suspect were present, the prudent action would be to secure a second search warrant for the intrusion into the device, while running to access and copy any contents from the cloud-based storage. However, that opinion changed with the addition of the suspect not being on scene. The group agreed that in that case, the most prudent course of action would be to access the cloud storage through the suspect device and make a copy of it. The next step would be to go back to a judge and ask for a second warrant to review the contents of the copy. Participants agreed that it would be important to explain the process of the exigency that necessitated the initial intrusion into the cloud storage. The group added that if the point of access were closed due to encryption, the ability to use legal process at a later time to access the account would only secure encrypted data that the police would not be able to access.

IACP Law Enforcement Cyber Center[2]

Participants discussed the new online portal managed by the International Association of Chiefs of Police that provides information and resources to a wide range of law enforcement officials, including chiefs, investigators, line officers, and prosecutors. The portal has dedicated resource pages for investigators and prosecutors. For investigators, there is detailed information on cyber crime investigations, training, and digital evidence. Prosecutors can get help with digital evidence, including Fourth Amendment interpretations, training, and resources for remaining current on case law decisions for digital evidence.

[2] The Center is funded by the Bureau of Justice Assistance (BJA) and the Program Manager for the Information Sharing Environment (PM-ISE), and was created through the joint efforts of the International Association of Chiefs of Police (IACP), RAND Corporation, and the Police Executive Research Forum (PERF). In addition, the Center represents a strategic partnership with a host of federal, state, and local law enforcement agencies (e.g., FBI, DHS, USSS, ICE, etc.) and professional organizations representing subject matter experts (e.g., NW3C, MS-ISAC, SEARCH, HTCIA, etc.). For more information, visit http://www.IACPCyberCenter.org.

The Need for Digital Evidence Training

The group discussed the need to develop something akin to a "digital evidence core competency skill set" for law enforcement in the 21st century. The discussion initially centered on what role technology plays in general crimes being committed today. Several prosecutors and law enforcement participants mentioned how technology was present in almost every case. Others echoed those sentiments, and added that there seemed to be a lack of training across the board on incorporating a digital element to every investigation. Participants then worked on developing training suggestions for the different levels of police officers and prosecutors, as outlined below. For law enforcement, the envisioned trainings would build on each level as foundational blocks as officers progressed through the ranks.

Patrol Officer

- Identification
- Seizure
- Preservation
- Referral-Resources
- Social Media-Tech Awareness
- Basic Legal
- Use of Technology by Criminals
- Officer Safety
- Exceptions to Search Warrants

Detective

- ECPA/SCA/State
- Search Warrants
- Securing Digital Crime Scene
- Resources
- Vertical Prosecution
- Mobile Devices

Cyber Detective

- Triage Training
- ESP/Mail Providers/ISP
- Network Investigations
- Cyber Intrusion
- Cloud Computing

Forensic Examiner

- Applications
- Mobile Devices
- Vehicles
- File System/Operating Systems

Prosecutor

- Computer Forensics 101
- Cell Phone Extractions 101
- Search and Seizure
- ECPA/SCA/PP
- Charging Decisions
- Discovery Issues
- Pre-Trial Motions: Motions to Suppress Motions in Limine
- Direct of Computer Forensic Examiner
- Cross of Defense Computer Forensic Examiner
- Authentication of Digital Evidence

Participants agreed that every patrol officer should take initial digital evidence training at the academy level and the training should continue through any field training officer period or probationary period that an officer goes through at the beginning of employment. In addition, participants agreed that digital evidence training should be required on a yearly basis. The group agreed that as technology advances, so too should the training officers receive. This would ensure they have a better understanding of what digital evidence devices are being used and what capabilities they may have.

Outcome

The group agreed that this had been an informative and beneficial meeting where much of the discussion applied to all jurisdictions. Several participants shared that they learned new techniques and information that they would apply to their investigations and prosecutions. In addition, several mentioned the possibility of working with their state legislatures to enact new laws that would assist an investigation based on the topics covered in the meeting.

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.