E24 Data Privacy

Ingrid A. Gill, JD, Law Office of the Cook County Public Defender, 69 West Washington, Suite 1500, Chicago, IL 60602*

After attending this presentation, attendees will understand the strategies of finding digital evidence while maintaining attorney client privilege digital communications when using third party providers. This presentation will impact the forensic community by changing current prac- tices in light of recent U.S. Supreme Court decisions governing data privacy and discovery.

The use of the internet, portable cell phones, PDA, and other wireless devices has increased reliance on electronic data in the forensic community. Law enforcement agencies, crime labs, prosecutors, defense attorneys, and court clerks are increasingly relying on communications via the internet maintained by ISPs or network administrators. The impact of two recent United States Supreme Court decisions dealing with information main- tained via third parties is discussed for its impact on the practices within the forensic community and the criminal justice system.

In *United States v. Miller*, the Supreme Court concluded that the Fourth Amendment did not apply to records maintained by a bank. Consequently, federal agents did not need a warrant to compel the production of defendant's bank records. The records sought were not secret since they were exposed to employees in the ordinary course of business. In *Smith v. Maryland*, the Supreme Court held that a warrant was not required where law enforcement sought the record of the numbers dialed by the defendant that had been captured by an electronic device, "the pen register". If infor- mation is not completely secret, it is not subject to protection under the right to privacy; thus, the government can use the power of the subpoena to acquire the records. At the same time, mistakes by court personal in emailing non-public crime lab reports concerning a high profile sexual assault can be argued by the defense to be waivers of secrecy requiring only the use of subpoenas rather than a court order by the defense to acquire the emergency room medical records of the sexual assault victim to prepare for trial.

For the defense, the major issue becomes how to challenge the relia- bility and accuracy of digital records maintained by the third party providers or the users of such digital evidence. The defense must motion for the discovery of all drafts and versions of digital documents to ade- quately challenge the accuracy of the records maintained by the custodian of digital records. How far back to the source document is the defense entitled to? Who decides what constitutes the "best evidence" to tender to the defense in discovery when it comes to digital discovery or imagining technology? Is a logical copy or a hash copy of a file sufficient for dis- covery? When does spoliation occur in the digital environment? Practical considerations will be given to the emerging field of computer forensics, imaging technology and the standards of admissibility for civil and criminal courts.

The presenter will discuss some of the federal statutes governing data privacy such as the Electronic Communications Privacy Act, the Pen Register Act, The Financial Privacy Act, The Cable Communications Act, and the Health Insurance Portability and Accountability Act of 1996. The impact of these statutes on those who practice in the criminal justice system will be discussed.

Data Privacy, Discovery, Digital Evidence

 ** Presenting Author*