WEEK NINE: NOVEMBER 10, 2005

Government Inquiries: Prosecution and Defense

HYPOTHETICAL FOR CLASS DISCUSSION

[This hypothetical, which involves investigations of computer hacking and online child pornography, subpoenas and search warrants, and related issues will form the foundation for this week's seminar discussion. Please read and consider the entire hypothetical. Focus particularly on the specific portions to which you have been individually assigned (you will receive an email with your assignment). You will be expected to discuss those portions during our seminar discussion. The hypothetical is based on, and requires careful review of, the readings for this week.]

An unknown individual was using his University I.D./Debit Card to buy high-priced textbooks at the University Bookstore. The charges, however, were actually debited to the accounts of other members of the campus community. The University Police initiated an investigation and determined that a junior computer science major, Kevin Mitnick, was the person who had "purchased" these books. On each occasion, he had presented what appeared to be his I.D. bearing his picture, but a different cardholder's account was debited for the charges. The police approached Mitnick in his room and observed a magnetic card coder in plain view. When the police asked Mitnick about the device, he explained that he had installed keystroke loggers on hundreds of PCs around campus by exploiting a known vulnerability in Windows 98. He then captured users' University network passwords, which he in turn used to access their debit account statements. Once he accessed those statements, he was able to tell what the code was on the back of the users' I.D.'s, re-code his own card, and charge books to them – books he later re-sold on E-bay.

With Mitnick's consent, the University Police began a forensic analysis of his computers. In one of the files recorded by a keystroke logger, police saw what appears to be an e-mail from a "Ferber@publicisp.com" custom ordering a movie of an eight year-old child being raped. The e-mail goes on to arrange for payment for the movie through a Paypal account. Police also found what appears to be a diary entry describing Ferber's desire to order such a video, his excitement upon receiving it, and his reactions to watching it. The diary entry and the e-mail are now over a year old. University Police turned this evidence over to the Office of the Attorney General (the "AGO").

The AGO used an administrative subpoena under M.G.L. c. 271, § 17B to obtain the subscriber information affiliated with "Ferber@publicisp.com". Ferber is a student who lived down the hall from Mitnick last year. The AGO then used a Grand Jury subpoena to obtain e-mails from Ferber's e-mail account that had already been marked as read, as well as multiple private diary entries that Ferber has stored on his shared network drive in an encrypted form. The e-mails and diary entries look much like those that the keystroke logger captured.

A short while later, the AGO was contacted by a State Trooper who is a member of the Internet Crimes Against Children Task Force. While posing as a thirteen year-old girl, she had been engaged in a series of I.R.C. chats and I.M.'s with an individual with a screen name – *1kzkdz* -- that investigators believed, based on the fruits of the keystroke logger, Ferber had used in the past. During his communications with the Trooper, *1kzkdz* sent the Trooper several .mpg files that, based on the Trooper's expert opinion, appear to involve actual prepubescent children engaged in sexual activity. During one of the chats, however, *1ikskdz* wrote about the attached video files: "These are so cool cuz they are computer generated images. They look real though."

The Trooper logged all of the chats and I.M.'s using I.R.C.'s and the I.M. program's built-in logging function. The Trooper captured the source I.P. address of all of these communications. Each of the I.P. addresses resolved to an overseas computer that was being used as a proxy server, thereby effectively making all communications routed through that server anonymous.

By then, Ferber was no longer on campus. The AGO contacted Paypal Security, and they volunteered that the user who purchased the child exploitation video some months ago had logged into his Paypal account ten times in the last week. On nine occasions, the I.P. address resolved to that same overseas proxy server Ferber had used in the past. On one occasion, it resolved to a nursing home that was across the street from an apartment building to which the State Police had followed Ferber at the end of each day and seen him exiting from in the early morning. Police did not know where in the four-unit dwelling Ferber was staying. Police investigation revealed that the nursing home was running an unsecured wireless access point that could be accessed from the street, and presumably, from the apartment where Ferber was staying

Citing the evidence obtained from the keystroke logger, the subpoenas to PublicISP and the undercover investigation, the police obtained a search warrant allowing a search of Ferber's residence for all computers and devices capable of storing any sort digital data. The Court further gave the police permission to take the computers and digital storage media off site and search them for evidence relating to the activities referenced in the logs from the keystroke logger, the subpoenaed evidence, and the communications with the undercover Trooper, as well as for other evidence relating to the creation, dissemination or possession of child pornography or dissemination of obscene material.

The police seized a terabyte server from the apartment Ferber was living in, created a forensic image within seven days and spent the next six months analyzing the data on the server.

Mitnick is charged with multiple violations of G.L. c. 272, § 99, among other crimes, for his operation of the keystroke loggers.

Ferber is charged with multiple violations of G.L. c. 272, §§ 29, 29A, 29B, and 29C based on the evidence gathered prior to the execution of the search warrant and evidence found on his server.

During class on Thursday, we will discuss the motions to suppress and/or dismiss that defense counsel are likely to bring and all of the issues that may be raised in those motions.