

Joint Advisory Committee on Computer Crimes
Tuesday, October 19, 2004, 9:30 a.m.
House Room D
General Assembly Building
Richmond, Virginia

The Joint Advisory Committee on Computer Crimes, charged with studying Virginia's Computer Crimes Act and related laws in light of current activities and technologies, recommending any necessary amendments, and evaluating the need for special laws on computer-related conduct, met for the third and final time on October 19, 2004 to discuss a draft of the Computer Crimes Act that incorporates all of the recommended amendments.

Recap and Review

Before discussing the amendments to the Computer Crimes Act, Mitchell Goldstein, JCOTS Director reviewed the meetings and actions taken prior to this final meeting of the Advisory Committee. The study was divided into two parts: the Joint Advisory Committee and the Joint Legislative Task Force. The Advisory Committee met on August 10 and September 21 to study the Computer Crimes Act. The Task Force met on August 18 and October 5; its final meeting will be October 26.

The study's objective was to examine the statutory basis for computer crimes and related laws in the Code of Virginia, including a determination of the appropriate definitions and elements constituting offenses; and recommend any necessary amendments in light of modern activities and technologies. The Committee decided to conduct its part of the study by identify threats, examining the Code of Virginia to determine if it addressed the threat and creating a new provision if the threat was not addressed. Its overriding focus was on the "bad actors" with a "bad motive" committing a "bad act." The Task Force not only reviewed the recommendations from the Committee, but also reviewed staff proposals that carried out further instructions to review the Act for other needed changes and updates.

At its first meeting, the Committee established a list of issues that it wanted to address and the Task Force added to the list. The final list of identified threats to address was: (i) phishing, spoofing and disguising one's identity (faking an identity to gather personal information); (ii) bots and zombies (programs implanted into a computer that allow third parties to use it); (iii) spyware and adware (a category of software that, when installed on a computer, may send pop-up ads, redirect the browser to certain websites, monitor the websites visited, or even log each key hit); (iv) viruses (programs or pieces of code that are loaded onto a computer without the user's knowledge and run against his wishes; some viruses can replicate themselves) and worms (programs that propagate themselves across a network, using resources on one machine to attack other machines) (a virus can insert itself into other programs, a worm cannot); (v) falsifying certifications, seals or other credentials; (vi) spam (unsolicited bulk electronic mail); (vii) identity theft; (viii) hacking and defacing websites, networks and databases; and (ix) denial of service (DoS) attacks (an attacker attempts to prevent legitimate users from accessing

information or services) and distributed denial-of-service (DDoS) attacks (an attacker uses others' computers to attack another computer).

The Advisory Committee began its review by discussing two specific proposals that the House Committee on Science and Technology (HCST) carried over and forwarded to JCOTS for review: HB 566 and SB 275. These bills attempted to address the spread of computer viruses. HB 566 (Patron – Albo) provided that adding or altering information without authority would be computer trespass and elevated the crime to a Class 6 felony if certain aggravating factors were present. SB 275 (Patron - Devolites) created a separate crime providing that knowingly and maliciously inserting a computer virus into a computer, computer program, computer software, or computer network of another without the knowledge and permission of the owner would be a Class 1 misdemeanor.

HCST was concerned that HB 566 would criminalize innocent acts such as sitting at the wrong computer and updating the software or merely hitting one key. In addition, a person could violate the statute without even knowing that he lacks the authority. SB 275 concerned HCST because it created a definition for computer virus that could criminalize the legitimate use of software that disables computers, but not the use of viruses that do not replicate themselves, worms, Trojan horses or other malicious code.

Staff drafted computer contaminant proposal to address the issues of bots, zombies, spyware, adware, viruses, worms and other malicious code. The Committee rejected the proposal, because it did not want to define the method, merely the underlying act.

Staff also drafted a computer invasion of privacy proposal to address identity theft, a crime that has a high risk of violation with low penalties and prosecutorial discretion whether to prosecute because it is a misdemeanor. The current law includes no definition for personal identification and no exemptions for network security, employers and law enforcement. It is important to note that employers and law enforcement are covered elsewhere in the Code and do not need specific exemptions.

The Computer Crimes Act - Revised

Next, Mr. Goldstein and Stewart Petoe, Virginia State Crime Commission Director of Legal Affairs, reviewed the proposals with the Committee. First, at the request of the Committee, they began with the definitions. To modernize the Code, Messrs. Goldstein and Petoe proposed definitions that mimic those found in the Uniform Computer Information Transactions Act (UCITA). Broader definitions will avoid some of the obsolescence problems that the law faces when trying to address technological issues. Also, some definitions have either been removed or combined with others. Under the revisions, a computer is a computer, property is property and computer information is computer information regardless of the type or form. Finally, for someone to be without authority, prosecutors must prove that he knew or had reason to know that he was without authority.

"Computer Fraud" and "Personal Trespass by Computer" would no longer require proof that the computer use was without authority. It does not matter if the person used a computer or network

without authority if he took the underlying action without authority and knowing that he had no authority to do it.

The crime of "Computer Trespass" would be expanded to address denial of service attacks, defacing websites. After the Committee proposed scrapping the computer contaminants bill, staff redrafted the statute to address malicious code and the earlier issues that were raised. Elements of the new statute were "using a computer or computer network, directly or indirectly" (addressing automated software and remote controls), "with the intent to maliciously" (addressing the issue of knowledge and bad intent) take the actions specified in subdivisions 1-6. In addition to the prohibited actions, the proposal added damaging, destroying, disabling or monitoring computer information to the prohibited actions. Because the Task Force had voted to remove the malicious requirement and some of the underlying actions could be benign, a new subsection B was added to require that altering, monitoring or installing computer software or computer information be malicious to be a crime. The remaining provisions require that the act be intentional and without authority. In addition, the presence of specified aggravating factors makes the crime a felony. The amount of damage also was reduced to \$1,000 to be consistent with other provisions in the Code.

The crime of "Computer Invasion of Privacy," which addresses identity theft, in part, was clarified and strengthened. The proposal replaces personal information with identifying information as defined in the identity theft statute (minus name and birth date) and increases the penalty for subsequent violations, selling or distributing the information, or using the information to commit another crime. In addition, the provision now offers an exemption for network security purposes. It would be a crime for someone to view information, which could be used to access financial information or create identification, without authority

To address phishing, spoofing, spyware, adware, bots, zombies, viruses and worms, falsifying seals and disguising identity or otherwise deceiving someone to gather information, the proposal contains a new crime: "Using a Computer to Gather Identifying Information." The original proposal to prohibit using computer contaminants (i.e., malicious code) to obtain information without authority was met with a request to not define something that could change rapidly, but, instead, to focus on the bad actor with a bad intent committing a bad act. The new provision would make it a criminal act to use a computer or computer network with the intent to deceive someone into providing information that no one has a legitimate reason for gathering by deception. The information is limited to identifying information as defined in the identity theft statute (minus name and birth date). The crime would be a Class 6 felony and would be elevated to a Class 5 felony if the perpetrator sold or distributed the information or used the information to commit another crime.

The Task Force talked about merging this section with the identity theft statute. However, if that were to happen, there would not be a separate crime in the Computer Crimes Act, and the crime of Identity Theft would have a greater penalty if the offense were accomplished through the use of a computer. The identity theft statute currently requires an additional intent to use the information, not just gather it. This crime only requires proof of the intent to gather it and offers a private right of action. The Committee determined that there exists no legitimate reason for engaging in these actions, people who do almost always use the information to commit identity

theft, and criminalizing the earlier actions would enable law enforcement and individuals to fight identity theft at an earlier stage.

To address bots, zombies, worms, viruses, cracking (also known as hacking), and other forms of invading computers and computer networks without authority, the proposal contains a second new crime: "Using a Computer to Gain Unauthorized Access." One subsection addresses prohibits using a computer or computer network with the intent of giving someone the ability to gain future access and another subsection prohibits using a computer or computer network with the intent of actually invading a system. The crime would be a Class 1 misdemeanor, elevated to a Class 6 felony for second and subsequent offenses, violating the provisions in the commission of another crime, or gaining access to three or more computers or one or more computer networks. The Committee decided to merge the provisions into the "Computer Trespass" statute.

Finally, the proposal would expand the definition of property for all larceny crimes. Currently, most intangible personal property, including computer information and services, is considered property only for purposes of the embezzlement statute. However, if it is considered property capable of embezzlement and embezzlement is deemed larceny, it naturally follows that it should be considered property for the larceny statutes as well.

Remaining Issues

In addition to reviewing the Committee's final proposed revisions, the Task Force will review whether the criminal procedure provisions should be relocated and consolidated with other provisions into the Criminal Procedure Code (Title 19.2) and whether any additional modifications are needed.