

2004 Computer Crimes Study

Final Report Talking Points

I. The Study

- In an effort to strengthen the 1 statute that Virginia has for dealing with cyber attacks (Computer Trespass), identical bills were introduced in the House and Senate during the 2004 General Session -- HB 566 (Albo) and SB 275 (Devolites). The House Committee on Science and Technology referred these bills to JCOTS.
- Believing that the entire Computer Crimes needed to be updated and amended to avoid criminalizing innocent conduct, to criminalize actions that use technological innovations to circumvent current laws, and to criminalize actions that were unheard of until recent years, JCOTS included a complete study in this year's work plan.
- In addition, the 2004 Appropriation Act directed the Virginia State Crime Commission to "examine the statutory basis for computer crimes in the Code of Virginia, including a determination of the appropriate definitions and elements constituting offenses in this area."
- The Commissions combined their studies and created a Joint Legislative Task Force and a Joint Advisory Committee.

II. Overview of the Computer Crimes Act

- Virginia's first computer crime statute, § 18.2-98.1, was written in 1978, in response to *Lund v. Commonwealth*, 217 Va. 688 (1977), to allow "computer time or services or ... information or data stored in connection therewith" to fall within Virginia's larceny laws.
- In 1984, the Commonwealth passed the Virginia Computer Crimes Act, which repealed § 18.2-98.1, and added Article 7.1 to Chapter 5 (Property Crimes) of Title 18.2. With few modifications, this Act is still Virginia's statutory scheme for handling computer crimes.
- Of the 17 statutes in the Act, only 8 are substantive criminal offenses. The Act also contains statutes covering civil liability, statute of limitations, venue and severability.
- Computer crimes can be considered as falling into one of three categories:
 - ✓ The computer used as a tool to carry out some substantive offense (forgery, copyright infringement, fraud);
 - ✓ The computer or its data as the direct objective of the crime (theft of data or hardware; theft of a hard drive); and
 - ✓ The computer as the subject of the crime (virus attacks, crashing computer systems).
- In the Virginia Computer Crimes Act:
 - ✓ The vast majority of offenses fall into the "computer as instrument" category: 5 statutes and 2 subsections of the "Computer Trespass" statute.
 - ✓ Three of the statutes are in the "computer as object" category.
 - ✓ Three subsections of 1 statute (computer trespass) are in the category of "computer as subject" category.

- There are additional “computer as an instrument” crimes found elsewhere in the Criminal Code. For example, use of a computer in connection with certain obscenity crimes and use of a communications system, including computers, to solicit minors or for the purposes of child pornography (§ 18.2-376.1).
- Offenses in the Computer Crimes Act afford both civil remedies to aggrieved parties and jurisdiction for the Attorney General's Office.

III. The Joint Legislative Task Force and Joint Advisory Committee

- Co-Chaired by Delegate May for JCOTS and Delegate Albo for the Crime Commission
- Advisory Committee - composed of 17 citizen members from the public and private sectors with technical and legal expertise in computers and computer crimes. Met 3 times: August 10, September 21 and October 19.
- Task Force - composed of representatives from JCOTS, Crime Commission, the House and Senate Courts of Justice Committees, the House and Senate at large, and the Advisory Committee. Met 3 times: August 18, October 5 and October 26.

IV. Meetings

- Both the Task Force and the Advisory Committee agreed to focus on the "bad actors" with a "bad motive" that do a "bad action," and to identify threats, look at the Code of Virginia to determine if it is addressed and then define the action, if necessary.
 - ✓ Concerned that defining the specific threats would lead to almost immediate obsolescence and would provide a road map to the bad actors.
- The list of identified threats are:
 - ✓ phishing, spoofing and disguising one's identity (faking an identity to gather personal information)
 - The behavior covered in these acts could be handled by modifying ...
 - ✓ bots and zombies (programs implanted into a computer that allow third parties to use it)
 - New provision
 - ✓ 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)
 - New provision
 - ✓ 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)
 -
 - ✓ falsifying certifications, seals or other credentials
 - This action currently falls under unfair and deceptive trade practice, trademark or copyright law, and fraud. To the extent that it is a method to deceive people out of personally identifiable

information, it falls under "phishing, spoofing and disguising one's identity."

- ✓ spam (unsolicited bulk electronic mail)
 - The Code of Virginia already addresses spam.
- ✓ identity theft
 - The Code of Virginia already addresses identity theft. That crime requires the intent to use the information.
- ✓ hacking and defacing websites, networks and databases
 - Computer Trespass already covers defacing websites, networks and databases. Hacking will become a new provision.
- ✓ 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 Task Force decided that the Computer Trespass statute already addresses this threat.

V. Proposed Bill

- Definitions
 - ✓ Condensed and Simplified. Some are based on UCITA definitions.
 - ✓ Computer includes general-purpose computers, but excludes dedicated-computer devices that contain microchips (e.g., washing machines, cars and pagers).
 - ✓ Computer Information replaces Computer Data.
 - ✓ Computer Network is deleted. Because using a computer network requires the use of a computer whether it is a client or server.
 - ✓ Computer Software incorporates Computer Program.
 - ✓ Person and Property are as broad as possible.
 - ✓ Without Authority requires that the person actually knew or should have known.
- Computer Fraud
 - ✓ Eliminates the requirement that the use of the computer be without authority.
- Spam is unchanged
- Computer Trespass
 - ✓ Added intent of "maliciousness."
 - ✓ To handle Bots and Zombies, it adds section 8 (maliciously installing software without authorization).
 - ✓ To cover viruses and worms that do not harm computers, but hinder their ability to operate peripheral devices (e.g., grocery scanners, security cameras, and environmental sensors), it adds subsection 9.
 - ✓ It also adds directly using a computer to obtain computer information without authority.
 - ✓ The task force reduced the amount of damage to be a felony from \$2,500 to \$1,000. However, the task force decided not to create any additional felonies in this statute.

- Computer Invasion of Privacy
 - ✓ Currently a crime for a person to examine, without authority, "employment, salary, credit or any other financial or personal information."
 - ✓ The bill substitutes "identifying information" from the identity theft statute for "personal information" so as not to criminalize the use of cookies and other legitimate business practices.
 - ✓ Increased penalty for subsequent violations, selling or distributing the information, or using the information to commit another crime.
 - ✓ Exemption for network security and determining authorized use.
- Using a Computer to Gather Identifying Information (Phishing, Spoofing, Spyware, Adware, Bots, Zombies, Viruses and Worms, Falsifying Seals and disguising identity or otherwise deceiving someone to gather information)
 - ✓ Makes it a crime to use a computer with the intent to fraudulently obtain, fraudulently access or fraudulently record identifying information. Class 6 Felony
 - ✓ Success is not necessary.
 - ✓ Increased penalty for selling the information or using it in another crime.
- Theft of Computer Services - no substantive change
 - ✓ Issue - Using an electronic device, not defined as a computer, to use computer services without authority is not a crime (e.g., using an X-Box to play online games for free).
- New Crime - Use of a computer to circumvent computer security measures. (Bots, Zombies, Worms, Viruses, and Cracking)
 - ✓ Class 1 Misdemeanor. Becomes a Class 6 felony for repeat convictions or violating section in the commission of a felony.
- Personal Trespass by Computer
 - ✓ Eliminates the requirement that the use of the computer be without authority.
- Harassment by Computer - no substantive change.
- Property Subject to Larceny and Embezzlement - clarified that all property can be stolen or embezzled.
- "Limitation of prosecution" and "Venue for prosecution" have been moved to Title 19.2 (Criminal Procedure).
- Computer as instrument of forgery - no substantive change
- The Task Force added a mandatory minimum fine of \$1,000 for any felony violation of the Act.
 - ✓ Note - this is the same penalty imposed for a 3rd violation in 10 years for driving while intoxicated.