

## Computer Crimes Act Issues

### I. Meetings

- A. **Advisory Committee** - Met on August 10 and September 21 to study the Computer Crimes Act.
- B. **Task Force** - Met on August 18 and October 5. The final meeting will be October 26.

### II. Grounds Rules and Procedures

- A. **Objective** - 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.
- B. **Conduct of Study** - Identify threats, look at the Code of Virginia to determine if it is addressed and then define the action, if necessary. Focus on the "bad actors" with a "bad motive" who do a "bad action."

Further instructions to review the Act for other needed changes and updates.

- C. **List of Issues** - At its first meeting, the Committee established a list of issues that it wanted to address and the Task Force added a couple. The final list of identified threats are: (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).

### III. Specific Proposals

#### A. Original Bills

##### **Problem to Solve** - Spread of Computer Viruses

HB 566 (Patron – Albo) provides that adding or altering information without authority is computer trespass and elevates the crime to a Class 6 felony if certain aggravating factors are present. SB 275 (Patron - Devolites) creates 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 is a Class 1 misdemeanor.

**Issues** - **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** 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.

#### B. Computer Contaminant

**Problem to Solve** - Bots, Zombies, Spyware, Adware, Viruses, Worms and other malicious code

**Issues** - Committee did not want to define the method, merely the underlying act.

#### C. Computer Invasion of Privacy

**Problem to Solve** - Identity Theft; High risk, low penalties and discretion in prosecuting misdemeanors

**Issues** - No definition for personal identification; no exemptions for network security, employers and law enforcement (NOTE: employers and law enforcement are covered elsewhere in the Code and do not need specific exemptions.)

### IV. New Proposals

#### A. Computer Fraud (page 4)

Does it really matter if the person used a computer or network without authority if he took the underlying action without authority and knowingly that he had no authority to do it?

**B. Computer Trespass (Denial of Service Attacks, Defacing websites) (page 4)**

**Background and update** - After the Committee proposed scrapping the computer contaminants bill, staff redraft the Computer Trespass 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" (addresses automated software), "with the intent to maliciously" (addresses the issue of knowledge and bad intent) take the actions specified in subdivisions 1-6. We added damaging, destroying, disabling or monitoring computer information to the prohibited actions.

The Task Force requested two alternatives. The first would address knowing and without authority. The second would address maliciously.

**Result** - A new subsection B that addresses altering, monitoring or installing and requires the act be intentional and malicious. The remaining provisions require an intentional act taken without authority.

**Additional** - Aggravating factors make the crime a felony. The amount of damage has been reduced to \$1,000 to be consistent with other provisions in the Code.

**C. Computer Invasion of Privacy (Identity Theft) (page 6)**

**Background and update** - Replaced personal information with identifying information as defined in the identity theft statute (minus name and birth date). Increased penalty for subsequent violations, selling or distributing the information, or using the information to commit another crime.

We added an optional new exemption for network security (subsection F).

**D. 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) (page 7)**

**Background and update** - Result of discussing the bill present at the last committee meeting.

Task Force talked about merging this section with the identity theft statute. If they decide to do this, there will not be a separate crime in the Computer Crimes Act; instead, the crime of Identity Theft will have a greater penalty if the offense is accomplished through the use of a computer.

The identity theft statute requires an additional intent to use the information, not just gather it. This crime only requires proof of the intent to gather it.

**E. Using a Computer to Gain Unauthorized Access (Bots, Zombies, Worms, Viruses, and Cracking) (page 7)**

**Background and update** - to address cracking and other forms of invading computers and computer networks. Subsection A covers giving the ability for future access; subsection B covers the action of cracking into a system. Increased penalties are provided.

**F. Personal Trespass by Computer (page 8)**

Does it really matter if the person used a computer or network without authority if he took the underlying action without authority and knowingly that he had no authority to do it? (Same issue as in IV.A).

**G. Property Subject to Larceny and Embezzlement (page 8)**

At the last meeting, we discussed alternative approaches to computer crimes. One was expanding when intangible personal property was considered property for traditional property crimes. Currently, it is considered so only for embezzlement. This section would expand that to larceny and receipt of stolen goods

**V. Issues for Task Force**

**A. Criminal Procedure Sections** - whether to relocate them

**B. Civil Penalties** - needed modifications