

Joint Advisory Committee on Computer Crimes
Tuesday, September 21, 2004, 1:00 p.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 second time on September 21, 2004.

Recap of the Issues raised at the August 10 meeting

At the August 10 meeting, the Advisory Committee identified a list of threats that the Computer Crimes Act needed to address. The Joint Legislative Task Force at its August 18 meeting added two more threats. The complete list of identified threats is (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).

Mitchell Goldstein, JCOTS Director, reviewed each threat and the statute that applies to it. Falsifying seals, certifications and other electronic authentication credentials is prohibited by laws pertaining to unfair and deceptive trade practices, such as the Virginia Consumer Protection Act; trademark and copyright laws; and fraud laws. A type of spam, known as unsolicited bulk electronic mail, is prohibited by section 18.2-152.3:1 of the Computer Crimes Act. Identity theft is prohibited under section 18.2-186.3, regardless of how the information was obtained. Phishing, spoofing, and disguising identity; bots and zombies; spyware and adware; and viruses and worms are partially addressed by fraud and identity theft laws. However, violations of those laws require someone to actually be injured, but by then, the harm is already done and the law is not much of a deterrent. The Committee believed that the attempt itself should be criminalized. To address those specific issues, staff drafted two legislative proposals.

Computer Invasion of Privacy Proposal

Current section 18.2-152.5 makes it a crime for any person to use a computer or computer network and intentionally examine without authority any employment, salary, credit or any other financial or personal information relating to any other person. Violations are punishable as a Class 1 misdemeanor. To strengthen this provision, it would be amended to replace "personal information" with "identifying information" as defined in the identity theft statute (subdivisions (iii) through (xiii) of section 18.2-186.3.C). This change was proposed to avoid criminalizing legitimate business practices while focusing those that involve gathering specific information that no legitimate business practice would involve gathering without authority. In addition, the penalty would increase to a Class 6 felony for repeat offenses and a Class 5 felony if the information is sold or used in another crime.

Because the Committee wanted to criminalize not only examining the information without authority, but also any attempt to gather it by deception, it discussed a proposed new statute that addressed the crimes of phishing, spoofing, and other deceptive means to gather information. Any person who used a computer or computer network with the intent to fraudulently obtain, record or access identifying information would be guilty of a Class 6 felony. Like violations of computer invasion of privacy, selling the information gathered in a violation of this section or using it another crime would be a Class 5 felony.

For the current statute, the Committee questioned whether an exemption for employers, law enforcement or network security was necessary. Chairman Albo apprised the Committee that while no other provision of the criminal code contains a specific law enforcement exemption, the common law and other general provisions of the criminal code address law enforcement. For employers, their authority to use and view information is governed by state and federal employment laws. To address issues of network security and verification of user license or authorization, staff agreed to draft an exemption for discussion.

For the new statute, it questioned whether the use of fraudulently in the intent would require proof of intent to take something physical from a person and. Convinced that the word fraudulently only required intent to deceive, it voted to keep the word.

Computer Contamination Proposal

The second proposal addressed viruses, worms, Trojan horses and other malicious code by defining these malicious codes and programs as computer contaminants and making their use a Class 1 misdemeanor. Second convictions or engaging in six defined acts considered dangerous raises the penalty to a Class 6 felony. The proposal defined a computer contaminant as any set of computer instructions that are designed to (1) alter, damage, destroy, or monitor information within a computer or network without the authorization of the owner of the information, or (2) degrade the performance of or disable a program, computer or network without the authorization of the owner, or (3) allow a person the ability to use or operate a computer or network, without the authorization of the owner.

The Committee was uncomfortable with defining a computer contaminant fearing that a definition would become obsolete. The task became to criminalize use of malicious code or malicious programs that replicate without defining the thing. The Committee opted for a more general provision that focused on a bad actor with a bad intent committing a bad act.