REPORT OF THE
VIRGINIA STATE CRIME COMMISSION

Computer Crimes Act

TO THE GOVERNOR AND
THE GENERAL ASSEMBLY OF VIRGINIA

REPORT DOCUMENT NO. 77

COMMONWEALTH OF VIRGINIA
RICHMOND
2005

MEMBERS OF THE VIRGINIA STATE CRIME COMMISSION

From the Senate of Virginia

Kenneth W. Stolle, Vice Chairman
Janet D. Howell
Thomas K. Norment, Jr.

From the Virginia House of Delegates

David B. Albo, Chairman
Robert B. Bell
Terry G. Kilgore
Robert F. McDonnell
Kenneth R. Melvin
Brian J. Moran

Gubernatorial Appointments

Glenn R. Croshaw
Col. W. Gerald Massengill
William G. Petty

Office of the Attorney General

Jerry W. Kilgore

Virginia State Crime Commission

Kimberly J. Hamilton, Executive Director
G. Stewart Petoe, Director of Legal Affairs
Christina M. Barnes, Legislative Policy Analyst
Stephen W. Bowman, Staff Attorney/Senior Policy Analyst
Thomas E. Cleator, Staff Attorney
Kristen J. Howard, Legislative Policy Analyst
Jaime H. Hoyle, Senior Staff Attorney
John B. Reaves, Legal Analyst
Sylvia Reid, Office Manager

TABLE OF CONTENTS

* Note: House Bill 2214 (Albo), House Bill 2215 (Albo) and House Bill 2631 (Bell) together contained all of the provisions in Senate Bill 1163 (Stolle).

I. Authority

The *Code of Virginia*, § 30-156, authorizes the Virginia State Crime Commission to study, report and make recommendations on all areas of public safety and protection. Additionally, the Commission is to study matters "including apprehension, trial and punishment of criminal offenders." Section 30-158(3) provides the Commission the power to "conduct studies and gather information and data in order to accomplish its purposes as set forth in § 30-156...and formulate its recommendations to the Governor and the General Assembly."

The Virginia State Crime Commission was directed, pursuant to Item 18 of the Appropriations Act of 2004, 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."[1]

II. Executive Summary

To ensure recently developed methods of computer crime are adequately defined and punished in the *Code of Virginia*, the Crime Commission recommended several modifications to the existing Computer Crimes Act. The current definitions found in *Virginia Code* § 18.2-152.2 should be modified to eliminate redundancies, promote clarity, and focus the scope of the Act. Many of the existing computer crimes should be rewritten, for the same reasons, and several new crimes should be inserted into the Act. These new crimes will make it easier for prosecutors to convict people who use the Internet to perpetrate fraud, engage in identity theft, or disseminate viruses or other types of malicious computer programs.

Thus, the Crime Commission made the following recommendations:

RECOMMENDATION 1 – Create a new crime making it a Class 6 felony to fraudulently obtain from any person their personal identifying information through the use of a computer; if the information is subsequently sold, distributed or used in the commission of another crime the penalty would be a Class 5 felony.

RECOMMENDATION 2 – Add, as one of the crimes listed in the Computer Trespass statute, that it shall be illegal to disable or disrupt the ability of a computer to transmit computer information to other computers or to related computer equipment, such as printers, scanners, or fax machines.

[1] *See* Attachment 1.

RECOMMENDATION 3 – Add, as one of the crimes listed in the Computer Trespass statute, that it shall be illegal to maliciously install a computer program on the computer of another without the authorization of the owner.

RECOMMENDATION 4 – Create a new crime, making it a Class 1 misdemeanor to circumvent a security measure (such as a password, firewall, or access code) that controls access to a computer; a second or subsequent violation, or a violation carried out in the commission of another felony, would be a Class 6 felony.

RECOMMENDATION 5 – The term "computer" should be defined as a device that accepts information in digital or similar form and manipulates it for a result based on a sequence of instructions. Such term (for purposes of the Computer Crimes Act) does not include a device whose predominate purpose is not the storage and manipulation of user-inputted computer information, such as automated typewriters, simple handheld calculators, digital cameras, faxes or pagers.

RECOMMENDATION 6 – The phrase "without authority," which is given a definition in § 18.2-152.2, should be amended to include a *mens rea* requirement of "know or reasonably should know."

RECOMMENDATION 7 – The definitions provided in § 18.2-152.2 should be extensively rewritten to promote brevity, eliminate awkward phrasings, and simplify the relevant concepts. When a term has already been defined elsewhere in the *Code of Virginia*, it should have, as far as possible, an identical meaning in the Computer Crimes Act.

RECOMMENDATION 8 – Amend § 18.2-152.7 and 18.2-152.3 to remove the phrase "without authority."

RECOMMENDATION 9 – Amend § 18.2-152.4 to require malice and lower the amount of resulting damage for a felony offense to $1,000.

RECOMMENDATION 10 – Amend § 18.2-152.5 to change the term "personal information" to "personal identifying information": those items of information that are "defined in subdivisions (iii) through (xiii) of subsection C of § 18.2-186.3."

RECOMMENDATION 11 – Amend § 18.2-152.8 to clarify that computer information is property that can be the subject of a larceny or a fraud; the existing statute only states that it can be the subject of an embezzlement.

RECOMMENDATION 12 – Rewrite §§ 18.2-152.3, 18.2-152.4, and 18.2-152.6, so that the emphasis is on the unlawful action, rather than the use of a computer.

RECOMMENDATION 13 – Relocate § 18.2-152.9 (dealing with the statute of limitations for misdemeanor computer crimes) and § 18.2-152.10 (dealing with venue) to Title 19.2.

III. Methodology

To accomplish its assignment, the Crime Commission, together with the Joint Commission on Technology and Science, formed a Joint Legislative Task Force on Computer Crimes, and an accompanying Advisory Committee.[2] The Legislative Task Force convened on August 18, October 5, October 26, and November 8, 2004 and the Advisory Committee met on August 10, September 21, and October 19, 2004. Together the Joint Legislative Task Force and the Advisory Committee provided information on the most common types of computer crimes that threaten individuals and businesses today. Representatives from law enforcement, the Attorney General's office and Commonwealth's Attorneys' offices contributed insight into what tools are and would be most effective in prosecuting criminals who engage in these sorts of computer crimes.

Using this information, the Crime Commission identified specific criminal behaviors, and then analyzed Virginia's existing criminal statutes to determine if such conduct was already prohibited. If the conduct was prohibited, the relevant statute was examined to see if any improvements could be made. However, if the conduct was not covered by any existing statutes, appropriate legislation was drafted to remedy this omission.

IV. Background

History of Virginia's Computer Crimes Act

Virginia's very first computer crime statute was passed in 1978. The original statute was passed in response to the case of Lund v. Commonwealth[3] which had been decided the previous year. In Lund, the Virginia Supreme Court, following the common law principle that services could not be the subject of a larceny, held that computer services were not something that could be embezzled or stolen. Thus, in 1978 the Virginia General Assembly passed a simple, one sentence statute to allow "[c]omputer time or services or data processing services or information or data stored in connection therewith" to be property that could be the subject of larceny, embezzlement, or false pretenses.[4]

One year later, in 1979, the General Assembly again dealt with the topic of computer crime by repealing *Virginia Code* § 18.2-98.1 and creating an entire Article[5] in Title 18.2 of the *Virginia Code* to cover a variety of computer crime offenses.[6] This new

[2] *See* Attachment 2.
[3] Lund v. Commonwealth, 217 Va. 688 (1977).
[4] VA. CODE § 18.2-98.1 (Repl. Vol. 1982) (repealed 1984).
[5] Article 7.1, in chapter 5 (Property Crimes) of Title 18.2. The entire Article is known as the "Virginia Computer Crimes Act."
[6] 1984 Va. Acts. ch. 751. For an extensive discussion of the origins of the Computer Crimes Act, and its original form, *see* Daniel R. Burk, *Virginia's Response to Computer Abuses: An Act in Five Crimes*, 19 U.

legislation was titled the "Virginia Computer Crimes Act,"[7] and, with very few modifications, remains the current statutory scheme for handling computer crimes. In its current form, the Act consists of seventeen statutes. However, only eight of those statutes are substantive offenses; the remaining nine statutes provide definitions,[8] pertain to civil lawsuits,[9] or are procedural in nature.[10]

Main Threats Facing Computer Users

The Advisory Committee identified nine current computer threats to businesses and individuals, including:

- phishing, spoofing and disguising one's identity;
- bots and zombies;
- spyware and adware;
- viruses and worms;
- falsifying certifications, seals, or other credentials;
- spam;
- identity theft;
- hacking and defacing websites, networks, and databases; and,
- denial of service attacks.

Each of these threats is discussed below.

Phishing - "Phishing" is a term that is used to describe how identity thieves send out false e-mails or set up false websites in order to trick victims into revealing sensitive information, such as Social Security numbers, bank account numbers, passwords, etc. "Spoofing" is a related term that generally means to impersonate another person, internet business, or web server without permission. In both phishing and spoofing, the criminal is disguising his identity as part of, or as a preliminary step to, committing some type of crime, such as identity theft or taking over another person's computer.

Bots and Zombies - The terms "bots" and "zombies," as used by the Advisory Committee, refer to computers that have been infected with computer programs that lie dormant, but allow a third party to take over or use the computer without authorization in the future. A "bot" is an infected computer; the term "zombie" is frequently used when referring to an entire network of computers that has been infected.

Spyware and Adware - Spyware is a computer program that allows a third party to secretly monitor or record the actions performed on a victim's computer. The information gathered may be fairly broad, or in the case of a keystroke logger, may include literally every action taken or instruction typed on the computer. Adware is an advertising program that generates pop-up ads on an infected computer. As with spam, it

---

RICH. L. REV., 85 (1984).

[7] VA. CODE § 18.2-152.1 (MICHIE 2004).

[8] VA. CODE § 18.2-152.2 (MICHIE 2004).

[9] VA. CODE § 18.2-152.12 (MICHIE 2004).

[10] VA. CODE § 18.2-152.9 (MICHIE 2004) (defining the statute of limitations for misdemeanor computer crimes); VA. CODE § 18.2-152.10 (MICHIE 2004) (setting forth venue for the prosecution of computer crimes).

becomes a problem when the volume of pop-up ads becomes so great that it significantly interferes with the normal operations of the computer.

Viruses and Worms - Viruses and worms refer to malicious computer programs that are designed to do such harmful things as delete computer data, or cause computers to malfunction or become inoperable. Some are self-replicating; others trick people into forwarding them onto friends through e-mail.

Falsifying - Falsifying certifications, seals, or other credentials is a special problem for internet businesses. Disreputable businesses, or sham companies, will pretend to be registered members of a trade group or business council, such as the Better Business Bureau, in order to lure victims into believing they are dealing with a legitimate business or company.

Spam - Spam is the commonly used term for unsolicited, e-mail advertisements. Frequently they are sent out in large volumes, to thousands of computers at one time. Besides general annoyance, spam can become a problem when the total number of e-mails sent becomes so great that it interferes with or shuts down individual computers, or even entire computer networks or internet providers.

Identity Theft - Identity theft involves the criminal obtaining an innocent person's identifying information, such as Social Security number, address, telephone number, credit card number, etc. They then use this information to impersonate the innocent third party, either stealing directly from him (emptying out a bank account), or from innocent merchants or banks (buying items with the stolen credit card number, or applying for a credit card using the name of the innocent third party).

Hacking - Hacking is the general term used to describe a computer user who interferes with other computers and websites, without authority, and does so through the Internet. Frequently hackers will attempt to steal guarded data, or as a "prank" will attempt to delete data or vandalize a website.

Denial of Service Attacks - Denial of service attacks occur when a person intentionally arranges for multiple computers, usually in the thousands, to all attempt to contact a single website at once or in a short period of time. This prevents legitimate computer users from being able to visit the website, and may cause the website to "crash," or become inoperable. The same technique may also be used against internet providers.

Virginia's Criminal Statutes

Of the nine threats identified by the Advisory Committee, all but bots and zombies and spyware were already covered by a limited degree in Virginia's current Computer Crimes Act or other criminal statutes. Phishing and spoofing, to the extent they are precursors to identity theft, are covered by Virginia's identity theft statute, § 18.2-186.3. Viruses and worms which delete data or cause a computer to malfunction could give rise to prosecution under Virginia's Computer Trespass statute, § 18.2-152.4.

Falsifying a certification, seal, or other credential is already covered by forgery, trademark laws, and laws dealing with fraud. Virginia has a specific statute, § 18.2-152.3:1, to criminalize spam to the extent allowed under federal law. As noted with phishing and spoofing, Virginia already has a comprehensive identity theft statute. Hacking is covered by the Computer Trespass statute, at least for those instances where the objective of the hacker was to steal or erase data, or vandalize or render inoperative a computer or website. Denial of service attacks are also covered by that statute.

The installation of a bot or zombie program on a computer is not adequately covered by existing statutes, however. Until the program is activated, it is not causing the computer to be used in an unauthorized way, nor is it harming the computer nor causing it to malfunction. Similarly, a hacker who gains unauthorized entry into another person's computer, but does so simply as a challenge and not to steal, read or destroy computer data or services, has not committed any crime. The same problem exists with spyware; as long as the information is not gathered for purposes of committing a crime, arguably no violation of a criminal statute has occurred.[11]

V. Summary

Legislative remedies for offenses

The fundamental goal of all criminal legislation is to ensure that harmful actions are criminalized as appropriate, yet also ensure that the criminal statutes are not written in a manner so overly broad as to criminalize innocuous conduct or lead to constitutional challenges. These twin ideals are especially relevant when it comes to updating Virginia's Computer Crimes Act. In addition, the goals of drafting criminal statutes in this area should be to ensure that the definitions and substantive offenses are described in terms of broad concepts—any attempts to use overly specific definitions or particularized offenses will result in statutes of minimal usefulness. With the rapid changes in technology, they would likely be outdated in a few years, or even worse, would be so specific that criminals would have little trouble in planning their behavior to avoid the "letter of the law." Therefore, it is also important to define terms and crimes in a manner flexible enough to handle the inevitable advancements that will occur with computer technology.

Most of the threats identified by the Advisory Committee are already covered by existing statutes in the Computer Crimes Act. However, the Crime Commission identified the following broad crimes as ones that should be covered by additional legislation: (1) phishing, spoofing, and identity theft; (2) viruses and worms; (3) bots,

[11] Although the Computer Invasion of Privacy statute, § 18.2-152.5, makes it a crime to examine without authority the "personal information" of another, it is not clear if this would cover spyware, as the criminal is not examining data on someone else's computer, but is receiving data sent directly to his own computer as it is generated by a third party on an infected computer. Even if spyware would be covered, it is at most a Class 1 misdemeanor.

zombies, and spyware; and, (4) hacking. In addition, the Crime Commission determined definitions should be clarified and incongruities eliminated throughout the Act.

Phishing and Spoofing

Phishing and spoofing are, by nature, attempted identity theft crimes.[12] Virginia already criminalizes identity theft under § 18.2-186.3, however this *Code* section requires the prosecution show that the personal identifying information be obtained for the purposes of defrauding someone,[13] or selling or distributing the information to another.[14] While there are valid policy reasons for requiring an additional element beyond simply obtaining such information before a person can be guilty of identity theft,[15] identity theft carried out via the Internet presents far more of a threat to society, and faces unique challenges in prosecution. Because of the ease with which a criminal can send out thousands of misleading e-mails, or the number of victims he can con by setting up a fraudulent website, a computer should be viewed as a "dangerous instrumentality" when it is used by an identity thief. Also, there have been cases of computer hackers who have attempted to gain thousands of Social Security numbers, passwords, and the like, not for reasons of personal gain, but simply as a challenge to see if it could be accomplished. Their rationale, if believed by prosecutors or triers of fact, would prevent any convictions for identity theft, regardless of the amount of economic damage they caused. In order to prohibit such a defense, and to proportionately punish the extreme danger caused by phishing and spoofing, it is the recommendation of the Crime Commission that a new crime be created, making it illegal to trick or fraudulently obtain from any person their personal identifying information, through the use of a computer.[16] Under this crime, no additional motives or elements would need to be shown.[17] The penalty would be increased if the information were sold or distributed, or were used in the commission of another crime.[18]

Viruses and Worms

Viruses and worms are already covered in the Computer Crimes Act, under Computer Trespass, § 18.2-152.4, to the extent that they cause damage to a computer or its data. The only omission in the existing act would be a computer program that does

[12] At least in the context identified by the Advisory Committee.
[13] VA. CODE § 18.2-186.3(A) (MICHIE 2004).
[14] VA. CODE § 18.2-186.3(B) (MICHIE 2004).
[15] Among the types of information that are covered under Va. Code § 18.2-186.3 are a person's name, date of birth, and social security number. Law enforcement and private investigators routinely attempt to locate and identify fugitives and missing persons, and occasionally attempt to locate bank accounts, all in the course of their normal duties, and for legitimate purposes. That is why obtaining such information only becomes a crime when the defendant does so for a nefarious reason, such as fraud.
[16] The personal identifying information that is listed in Va. Code § 18.2-186.3, the identity theft statute, includes a person's name and date of birth. Because these types of information are relatively innocuous, they have not been included in the new statute.
[17] *See* Attachment 3, pg. 3, proposed statute § 18.2-152.5:1.
[18] *Id.*

not affect a computer directly, but instead attacks peripheral devices, such as printers. This can be remedied by adding a paragraph to *Virginia Code* § 18.2-152.4.[19]

Bots, Zombies and Adware

Bots, zombies and spyware pose a different problem, in that none of them necessarily cause any harm to a computer or its data. Instead, they create potential harm. In the case of bots and zombies, while they may lie dormant for months or years, they have at any time the potential to allow a third party to make unauthorized use of it.[20] Spyware, while performing an insidious function, may not necessarily affect the operation of a computer, nor, depending on what it transmits, fall within the restrictions of identity theft or § 18.2-152.5, Computer Invasion of Privacy. To ensure these types of computer programs are criminalized, a simple paragraph can be added to the Computer Trespass statute.[21]

Hacking

Hacking creates a similar problem when the actions taken to "invade" another computer or restricted website do not cause any harm, and the hacker is not stealing nor examining data. To prevent this type of undesirable conduct, a short statute can be created that criminalizes unauthorized attempts to bypass or evade computer security measures.[22]

Definitions

To eliminate some of the incongruities that exist in the current Computer Crimes Act, the Crime Commission recommends modifying the definition of a computer in § 18.2-152.2 (the definitional section of the Computer Crimes Act).[23] The current definition is substantially different from the more recent definition of computer that was adopted by the General Assembly in 2000.[24] In order to slightly restrict the applicability of the Act, though, the broad definition of a computer should be limited in scope to those items that are commonly thought of, by the general public, as computers.[25]

---

[19] *See* Attachment 3, pg. 2, proposed subsection 9, lines 136 -138.

[20] The same problem occurs with viruses and worms that lie dormant for a period of time before they actively cause damage. In this instance, the legislative remedy for one type of problem will also handle the other.

[21] *See* Attachment 3, pg. 3, proposed subsection 8, line 135.

[22] *See* Attachment 3, pg. 4, proposed statute § 18.2-152.6:1.

[23] VA. CODE § 18.2-152.2 (MICHIE 2004).

[24] The recently enacted Uniform Computer Information Transactions Act, Va. Code § 59.1-501.1 *et seq.*, defines a computer as "an electronic device that accepts information in digital or similar form and manipulates it for a result based on a sequence of instructions." Va. Code § 59.1-501.2. This definition is shorter and easier to understand than the definition in the Computer Crimes Act.

[25] Common household items and electronic goods are increasingly outfitted these days with microchips and small micro-processors. With the day fast approaching on the horizon when almost every item will have such components, care must be taken to ensure that merely using someone's coffee maker, or digital camera, without permission is not a crime. *See, eg.* Va. Code § 18.2-152.6, which essentially criminalizes the use of another's computer without permission.

The phrase "without authority," as used in the Act, is defined as merely using a computer when the person has "no right or permission of the owner" to do so.[26] There is no *mens rea* requirement in this definition; someone would be guilty of various crimes in the Act if they used a computer by mistake, or if they used a computer, thinking they had permission, when they did not. It is the recommendation of the Crime Commission to insert a *mens rea* requirement into this definition—a person should not be guilty of a crime for merely installing software on the wrong computer.

In addition, it is the recommendation of the Crime Commission that the following definitions be amended:[27]

The term "computer data" should be replaced with "computer information." The new term should have a short, broad definition—"information in any form that is obtained from or through the use of a computer or that is in a form capable of being processed by a computer."

The phrase "computer network" should be eliminated as unnecessary and duplicative. If a "computer network" is nothing more than two or more computers joined together, then any crime involving a computer network must, of necessity, involve a computer. There are no advantages to having the additional phrase "or a computer network" used repeatedly throughout the Computer Crimes Act.

The definition of "computer operation" should be simplified—"an operation that a computer is designed and built to perform."

The definitions of "computer program," and "computer software" should be replaced with one, simple definition for both terms—"a set of statements or instructions to be used directly or indirectly in a computer to bring about a certain result."

The current definitions of "computer services" and "owner" are almost circular, due to awkward phrasing—"'computer services' means computer time or services…;" "'owner' means an owner or lessee…." They should be rewritten to avoid that result.

The definition of "financial instrument" should include financial assets, as defined in § 8.8A-102.

The definition of "person" should be changed to that provided for by § 1-13.19.

The definition of "property" should be shortened, simplified, and made as broad as possible, imitating the language currently found in the Money Laundering Act—"'Property'" means anything of value, and includes any interest therein, including any benefit, privilege, claim or right with respect to anything of value, whether real or personal, tangible or intangible."

---

[26] VA. CODE § 18.2-152.2 (MICHIE 2004).
[27] *See* Attachment 3, pg. 1-2, for all proposed changes to Va. Code § 18.2-152.2.

The definition of "using a computer" should be eliminated as unnecessary. Even worse, it includes in its terms ideas which are more properly expressed as elements of substantive criminal offenses.

Eliminating "Without Authority"

For the current crimes of Computer Fraud, § 18.2-152.3 and Personal Trespass by Computer, § 18.2-152.7, the phrase "without authority" should be eliminated. In instances where a criminal uses a computer to either commit a fraud on another, or injure another, it should not be a possible defense that he had the permission of the owner of the computer to engage in illegal activities.

Mens Rea

The current Computer Trespass statute, § 18.2-152.4, does not have a *mens rea* requirement. In order to prevent criminalizing innocent mistakes, such as accidentally erasing the wrong data on someone else's computer, or on the wrong computer,[28] a requirement of malice should be added to the statute. The amount of resulting damage that is required to raise an offense under this statute to a felony is currently $2,500.[29] It is the recommendation of the Crime Commission to lower this amount to $1,000, which is consistent with the felony threshold amount for the destruction of property in general.[30]

Personal Identifying Information

The existing Computer Invasion of Privacy statute, § 18.2-152.5, criminalizes the intentional examination of any "personal information relating to any other person" when the defendant knows, or should know, that he is without authority to examine that information. Due to concerns raised by the Advisory Committee that standard business practices in the computer industry normally allow merchants and Internet providers to observe and obtain information about their patrons and potential customers, the scope of this statute should be restricted to "personal identifying information," as that phrase is used in the identity theft statute.[31]

Property Subject to Larceny or False Pretenses

While the Computer Crimes Act states that computer data is property that can be the subject of an embezzlement, it does not specifically state that it can also be the subject of a larceny or false pretenses.[32] This technical oversight should be corrected by amending § 18.2-152.8.

---

[28] *See, e.g.*, Subsection (A)(3) of Computer Trespass, Va. Code § 18.2-152.4: "Alter or erase any computer data, computer programs, or computer software."
[29] VA. CODE § 18.2-152.2(B) (MICHIE 2004).
[30] VA. CODE § 18.2-137 (MICHIE 2004).
[31] VA. CODE § 18.2-186.3(C) (MICHIE 2004).
[32] VA. CODE § 18.2-152.8 (MICHIE 2004).

Rewriting the Statutes for Computer Fraud, Computer Trespass, and Theft of Computer Services

Throughout the Computer Crimes Act, many of the substantive offenses are written in an awkward form: Any person who uses a computer with the intent to…shall be guilty of a crime.[33] Typically the criminal statutes in Title 18.2 are written more directly: Any person who does…is guilty of a crime. Rather than making the use of a computer with bad intent a crime, these statutes should be rewritten so that the offense is the carrying out of the bad action, through the use of a computer.

Procedural Statutes

Finally, there are two criminal procedure statutes in the Computer Crimes Act, § 18.2-152.9 (dealing with the statute of limitations for misdemeanor computer crimes) and § 18.2-152.10 (dealing with venue) that would be more appropriately placed in Title 19.2. It is the recommendation of the Crime Commission that these statutes be transferred to that Title.

VI. Recommendations

The Virginia State Crime Commission recommends that the following changes be made to the Computer Crimes Act and legislation to accomplish this be introduced.[34]

RECOMMENDATION 1 – Create a new crime making it a Class 6 felony to fraudulently obtain from any person their personal identifying information through the use of a computer; if the information is subsequently sold, distributed or used in the commission of another crime the penalty would be a Class 5 felony.

RECOMMENDATION 2 – Add, as one of the crimes listed in the Computer Trespass statute, that it shall be illegal to disable or disrupt the ability of a computer to transmit computer information to other computers or to related computer equipment, such as printers, scanners, or fax machines.

RECOMMENDATION 3 – Add, as one of the crimes listed in the Computer Trespass statute, that it shall be illegal to maliciously install a computer program on the computer of another without the authorization of the owner.

RECOMMENDATION 4 – Create a new crime, making it a Class 1 misdemeanor to circumvent a security measure (such as a password, firewall, or access code) that controls access to a computer; a second or subsequent violation, or a violation carried out in the commission of another felony, would be a Class 6 felony.

[33] *See, eg.* Va. Code § 18.2-152.3 (Computer Fraud); § 18.2-152.4 (Computer Trespass); § 18.2-152.6 (Theft of Computer Services).
[34] *See* Attachment 3.

RECOMMENDATION 5 – The term "computer" should be defined as a device that accepts information in digital or similar form and manipulates it for a result based on a sequence of instructions. Such term (for purposes of the Computer Crimes Act) does not include a device whose predominate purpose is not the storage and manipulation of user-inputted computer information, such as automated typewriters, simple handheld calculators, digital cameras, faxes or pagers.

RECOMMENDATION 6 – The phrase "without authority," which is given a definition in § 18.2-152.2, should be amended to include a *mens rea* requirement of "know or reasonably should know."

RECOMMENDATION 7 – The definitions provided in § 18.2-152.2 should be extensively rewritten to promote brevity, eliminate awkward phrasings, and simplify the relevant concepts. When a term has already been defined elsewhere in the *Code of Virginia*, it should have, as far as possible, an identical meaning in the Computer Crimes Act.

RECOMMENDATION 8 – Amend § 18.2-152.7 and 18.2-152.3 to remove the phrase "without authority."

RECOMMENDATION 9 – Amend § 18.2-152.4 to require malice and lower the amount of resulting damage for a felony offense to $1,000.

RECOMMENDATION 10 – Amend § 18.2-152.5 to change the term "personal information" to "personal identifying information": those items of information that are "defined in subdivisions (iii) through (xiii) of subsection C of § 18.2-186.3."

RECOMMENDATION 11 – Amend § 18.2-152.8 to clarify that computer information is property that can be the subject of a larceny or a fraud; the existing statute only states that it can be the subject of an embezzlement.

RECOMMENDATION 12 – Rewrite §§ 18.2-152.3, 18.2-152.4, and 18.2-152.6, so that the emphasis is on the unlawful action, rather than the use of a computer.

RECOMMENDATION 13 – Relocate § 18.2-152.9 (dealing with the statute of limitations for misdemeanor computer crimes) and § 18.2-152.10 (dealing with venue) to Title 19.2.

VII. Acknowledgements

The Virginia State Crime Commission extends its appreciation to the following individuals for their assistance and cooperation on this study:

Joint Legislative Task Force on Computer Crimes
Delegate Ward L. Armstrong
Steve Benjamin
Robert M. Blue, Office of the Governor
Richard Campbell, Office of the Attorney General
Charles D. Curran, AOL Corporation
Senator Jeannemarie Devolites Davis
Delegate Robert Hurt
Delegate Joe T. May
Delegate Ryan T. McDougle
Senator William C. Mims
Senator Stephen D. Newman
Delegate Samuel A. Nixon, Jr.
Jim E. Plowman
Delegate Thomas D. Rust

Computer Crimes Advisory Committee
Michael Aisenberg
William B. Baker
Steve Benjamin
Charles D. Curran
Steve DelBianco
Cynthia H. de Lorenzi
Magnolia Mansourkia
Thomas W. Mastaglio
Russell E. McGuire
Gregory C. Mullen
Brian H. Murray
Jeffrey H. Nelson
Jim E. Plowman
Greg Redfern
Terry E. Riley
William Wiita

Citizens
Matt Benedetti
Todd Flournoy, Motion Picture Association of America
Lisa Hicks-Thomas, Office of the Attorney General
Michael J. Huppe, Recording Industry of America
Josh Levi, Northern VA Technology Council
Gary Rolling, Albers & Company
Gregory Thomas, Symantec Corporation

Attachment 1

House Appropriations Act, Item 18

ITEM 18.		Item Details($) First Year FY2005	Item Details($) Second Year FY2006	Appropriations($) First Year FY2005	Appropriations($) Second Year FY2006
	Virginia Crime Commission (142)				
18.	Criminal Justice Research, Planning, and Coordination (30500)			$569,899	$500,436
	Criminal Justice Research (30503)	$569,899	$500,436		
	Fund Sources: General	$465,133	$395,670		
	Federal Trust	$104,766	$104,766		

Authority: Title 30, Chapter 16, Code of Virginia.

A. Included within this appropriation is $69,463 the first year from the general fund to replace a federal grant that has expired. Should the Crime Commission obtain additional federal funds during fiscal year 2005, an equal amount of these general funds, not to exceed $69,463, shall revert to the general fund.

B. The Virginia Crime Commission shall 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.

Attachment 2

Joint Legislative Task Force and Joint Advisory Committee on Computer Crimes Memberships

VIRGINIA STATE CRIME COMMISSION
JOINT COMMISSION ON TECHNOLOGY AND SCIENCE
JOINT LEGISLATIVE TASK FORCE ON COMPUTER CRIMES
2004 MEMBERSHIP

Delegate David B. Albo, Co-Chairman
Delegate Joe T. May, Co-Chairman

Delegate David B. Albo
P.O. Box 6405
Springfield, VA 22150
(703) 451-3555 & (703) 455-0046 (law office)
(703) 455-0043 (fax)

Delegate Ward L. Armstrong
P.O. Box 1431
Martinsville, VA 24114
(276) 632-7022 ext. 4
(276)632-2935 (fax)

Delegate Robert B. Bell
2 Boar's Head Place; Suite 100
Charlottesville, VA 22903
(434) 245-8900
(434) 245-8903 (fax)

Mr. Stephen Benjamin
11 South 12th Street, Suite 302
Richmond, Virginia 23219
(804) 788-4444
(804) 644-4512 (fax)

Mr. Robert M. Blue
Counselor to the Governor
Office of the Governor, State Capitol
Richmond, VA 23219
(804) 786-2211 ext. 2342
(804) 371-2655 (fax)

Mr. Richard Campbell
Deputy Attorney
Office of the Attorney General
900 East Main Street
Richmond, VA 23219
(804) 786-3847

Mr. Charles D. Curran
America Online, Inc.
22000 AOL Way
Dulles, VA 20166-9323
(703) 265-3153
(703) 265-1239 (fax)

Senator Jeannemarie Devolites Davis
P.O. Box 936
Vienna, VA 22183
(703) 938-7972
(703) 938-1706 (fax)

Senator Janet D. Howell
P.O. Box 2608
Reston, VA 20195
(703) 709-8283
(703) 435-1995 (fax)

Delegate Robert Hurt
P.O. Box 2
Chatham, VA 24531
(434) 432-4600
(434)432-4162 (fax)

Delegate Joe T. May
P.O. Box 4104
Leesburg, VA 20177
(703) 777-1191
(703) 777-6059 (fax)

Delegate Ryan T. McDougle
P.O. Box 187
Mechanicsville, VA 23111
(804) 730-1026
(804)730-1051 (fax)

Senator William C. Mims
P.O. Box 741
Leesburg, VA 20178
(703) 779-1888
(703) 777-4001 (fax)

Delegate Brian J. Moran
4154 Duke Street
Alexandria, VA 22304
(703) 370-4154 & (703) 684-5755 (law office)
(703) 370-4011 (fax)

Senator Stephen D. Newman
P.O. Box 2209
Lynchburg, VA 24501
(434) 385-1065
(434) 385-1021 (fax)

Delegate Samuel A. Nixon, Jr.
P.O. Box 34908
Richmond, VA 23234
(804) 745-4335
(804)745-4432 (fax)

The Honorable Jim E. Plowman
Commonwealth's Attorney
Loudoun County
20 East Market Street
Leesburg, VA 20176
(703) 777-0242
(703) 777-0160 (fax)

Delegate Thomas D. Rust
730 Elden Street
Herndon, VA 20170
(703) 437-9400
(703)435-6655 (fax)

Senator Kenneth W. Stolle
700 Pavilion Center, Box 626
Virginia Beach, VA 23451
(757) 486-5700
(757) 486-8020 (fax)

Revised 08/12/04

Joint Advisory Committee on Computer Crimes

NAME	ADDRESS	PHONE & FAX	E-MAIL
Michael Aisenberg	VeriSign, Inc. 21345 Ridgetop Circle Dulles, VA 20166	P - 202-973-6600 F - 202-466-9103	maisenberg@verisign.com
William B. Baker	Wiley Rein & Fielding LLP 1776 K Street, NW Washington, DC 20006	P - 202-719-7255 F - 202-719-7049	wbaker@wrf.com
Steven D. Benjamin	11 South 12th Street, Suite 302 Richmond, Virginia 23219	P - 804-788-4444 F - 804-644-4512	sdbenjamin@aol.com
Charles D. Curran	America Online, Inc. 22000 AOL Way Dulles, VA 20166-9323	P - 703-265-3153 F - 703-265-1239	cdcurran@aol.com
Steve DelBianco	Association for Competitive Technology 9123 Horner Court Fairfax, VA 22031	P - 703-615-6206 F - 703-783-0322	sdelbianco@actonline.org
Cynthia H. de Lorenzi	PatriotNet, Inc. 4031 University Drive, 2nd Floor Fairfax, VA 22030	P - 703-797-1888 Ext. 211 F - 703-273-9236	cdelorenzi@patriot.net
Magnolia Mansourkia	MCI Network Services, Inc 1133 19th Street, NW Washington, DC 20036	P - 202-736-6448 F - 202-736-6460	m_mansourkia@yahoo.com
Thomas W. Mastaglio	MYMIC LLC 200 High Street, Suite 308 Portsmouth, VA 23704	P - 757-391-9200 F - 757-391-9098	tom.mastaglio@mymic.net
Russell E. McGuire	Office of the Attorney General 900 East Main Street Richmond, VA 23219	P – 804-786-0086 F – 804-786-1991	rmcguire@oag.state.va.us
Gregory C. Mullen	Deputy Chief Virginia Beach Police Department 2509 Princess Anne Road Municipal Center Bldg. 11 Virginia Beach, VA 23456	P – 757-427-4141 F – 757-427-9163	gmullen@vbgov.com
Brian H. Murray	Cyveillance, Inc. 1555 Wilson Boulevard, Suite 404 Arlington, VA 22209-2405	P - 703-312-1252 F - 703-312-0536	bmurray@cyveillance.com
Jeffrey H. Nelson	Nixon & Vanderhye P.C. 1100 N. Glebe Road Arlington, VA 22201	P - 703-816-4023 F - 703-816-4100	jhn@nixonvan.com
Jim Plowman	Commonwealth's Attorney Loudoun County 20 E. Market Street Leesburg, VA 20176	P - 703-777-0242 F -	oca@loudoun.gov
Greg Redfern	Computer Sciences Corporation (CSC) 3160 Fairview Park Drive M/C 263 Falls Church, VA 22042	P - 703-876-1452 F - 703-205-0133	gredfern@csc.com
Terry E. Riley	Executive Director Hampton Roads Technology Council Southside Office 420 North Center Drive Building 11, Suite 221 Norfolk, VA 23502	P – 757-233-0875 F – 757-233-0876	riley@hrtc.org
William Wiita	Bedford County Sheriff's Office 1345 Falling Creek Road Bedford, VA 24523	P - 434-534-0661 F - 434-534-0663	rwiita@bedfordsheriff.org

Attachment 3

*Crime Commission Recommendations, Introduced Legislation**

* Note: House Bill 2214 (Albo), House Bill 2215 (Albo) and House Bill 2631 (Bell) together contained all of the provisions in Senate Bill 1163 (Stolle).

057935134

SENATE BILL NO. 1163

Offered January 12, 2005

Prefiled January 12, 2005

A BILL to amend and reenact §§ 18.2-152.2 through 18.2-152.8, 18.2-152.12, 18.2-152.14, and 19.2-8 of the Code of Virginia; to amend the Code of Virginia by adding sections numbered 18.2-152.5:1 and 18.2-152.6:1, in Article 7.1 of Chapter 5 of Title 18.2 a section numbered 18.2-152.17, and a section numbered 19.2-249.2; and to repeal §§18.2-152.9 and 18.2-152.10 of the Code of Virginia, relating to redefinition and modernization of terms and streamlining the laws governing computer crimes; penalties.

Patrons—Stolle, Howell and Norment; Delegates: Albo, Kilgore, McDonnell and Moran

Referred to Committee for Courts of Justice

Be it enacted by the General Assembly of Virginia:

1. That §§ 18.2-152.2 through 18.2-152.8, 18.2-152.12, 18.2-152.14 and 19.2-8 of the Code of Virginia are amended and reenacted and that the Code of Virginia is amended by adding sections numbered 18.2-152.5:1 and 18.2-152.6:1, in Article 7.1 of Chapter 5 of Title 18.2 a section numbered 18.2-152.17, and a section numbered 19.2-249.2 as follows:

§ 18.2-152.2. Definitions.

For purposes of this article:

"Computer" means ~~an electronic, magnetic, optical, hydraulic or organic device or group of devices which, pursuant to a computer program, to human instruction, or to permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person. The term "computer" includes any connected or directly related device, equipment, or facility which enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device~~ *a device that accepts information in digital or similar form and manipulates it for a result based on a sequence of instructions. Such term does not include a device whose predominate purpose is not the storage and manipulation of user-inputted computer information, such as automated typewriters, simple handheld calculators, digital cameras, facsimile machines or pagers.*

~~"Computer data" means any representation of information, knowledge, facts, concepts, or instructions which is being prepared or has been prepared and is intended to be processed, is being processed, or has been processed in a computer or computer network. "Computer data" may be in any form, whether readable only by a computer or only by a human or by either, including, but not limited to, computer printouts, magnetic storage media, punched cards, or stored internally in the memory of the computer.~~

"Computer information" means information in any form that is obtained from or through the use of a computer or that is in a form capable of being processed by a computer.

~~"Computer network" means two or more computers connected by a network.~~

"Computer operation" means ~~arithmetic, logical, monitoring, storage or retrieval functions and any combination thereof, and includes, but is not limited to, communication with, storage of data to, or retrieval of data from any device or human hand manipulation of electronic or magnetic impulses. A "computer operation" for a particular computer may also be any function for which that computer was generally designed~~ *an operation that a computer is designed and built to perform.*

~~"Computer program" means an ordered set of data representing coded instructions or statements that, when executed by a computer, causes the computer to perform one or more computer operations.~~

"Computer services" means ~~computer time or services~~ *the use of a computer,* including *but not limited to, computer time,* data processing services, Internet services, electronic mail services, electronic message services, or information or data stored in connection therewith.

"Computer software" *or "computer program"* means a set of ~~computer programs, procedures and associated documentation concerned with computer data or with the operation of a computer, computer program, or computer network~~ *statements or instructions to be used directly or indirectly in a computer to bring about a certain result.*

"Electronic mail service provider" (EMSP) means any person who (i) is an intermediary in sending or receiving electronic mail and (ii) provides to end-users of electronic mail services the ability to send or receive electronic mail.

"Financial instrument" includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization

mechanism, marketable security, *financial asset as that term is defined in § 8.8A-102,* or any computerized representation thereof.

~~"Network" means any combination of digital transmission facilities and packet switches, routers, and similar equipment interconnected to enable the exchange of computer data.~~

~~"Owner" means~~ *The term "owner" includes* an owner or lessee of a computer ~~or a computer network~~ or an owner, lessee, or licensee of computer ~~data~~ *information,* computer ~~programs~~ *services,* or computer software.

~~"Person"~~ *The term "person"* shall ~~include any individual, partnership, association, corporation or joint venture~~ *have the same meaning as set forth in § 1-13.19.*

"Property" ~~shall include:~~

~~1. Real property;~~

~~2. Computers and computer networks;~~

~~3. Financial instruments, computer data, computer programs, computer software and all other personal property regardless of whether they are:~~

~~a. Tangible or intangible;~~

~~b. In a format readable by humans or by a computer;~~

~~c. In transit between computers or within a computer network or between any devices which comprise a computer; or~~

~~d. Located on any paper or in any device on which it is stored by a computer or by a human; and~~

~~4. Computer~~ *means anything of value, and includes any interest therein, including any benefit, privilege, claim, or right with respect to anything of value, whether real or personal, tangible or intangible. "Property" includes, but is not limited to, computers, financial instruments, computer information, computer software, and computer* services.

~~A person "uses" a computer or computer network when he attempts to cause or causes:~~

~~1. A computer or computer network to perform or to stop performing computer operations;~~

~~2. The withholding or denial of the use of a computer, computer network, computer program, computer data or computer software to another user; or~~

~~3. A person to put false information into a computer.~~

A person is "without authority" when *he knows or reasonably should know that* he has no right or permission ~~of the owner to use a computer or computer network or he uses a computer or computer network~~ *or acts* in a manner exceeding such right or permission.

§ 18.2-152.3. Computer fraud; penalty.

Any person who*, through the use of a computer* ~~uses a computer or computer network without authority and with the intent to~~:

1. ~~Obtain~~ *Obtains* property or services by false pretenses;

2. ~~Embezzle~~ *Embezzles* or ~~commit~~ *commits* larceny; or

3. ~~Convert~~ *Converts* the property of another

is guilty of the crime of computer fraud.

If the value of the property or services obtained is $200 or more, the crime of computer fraud shall be punishable as a Class 5 felony. Where the value of the property or services obtained is less than $200, the crime of computer fraud shall be punishable as a Class 1 misdemeanor.

§ 18.2-152.3:1. Transmission of unsolicited bulk electronic mail (spam); penalty.

A. Any person who:

1. Uses a computer ~~or computer network~~ with the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers; or

2. Knowingly sells, gives, or otherwise distributes or possesses with the intent to sell, give, or distribute software that (i) is primarily designed or produced for the purpose of facilitating or enabling the falsification of electronic mail transmission information or other routing information; (ii) has only limited commercially significant purpose or use other than to facilitate or enable the falsification of electronic mail transmission information or other routing information; or (iii) is marketed by that person acting alone or with another for use in facilitating or enabling the falsification of electronic mail transmission information or other routing information is guilty of a Class 1 misdemeanor.

B. A person is guilty of a Class 6 felony if he commits a violation of subsection A and:

1. The volume of UBE transmitted exceeded 10,000 attempted recipients in any 24-hour period, 100,000 attempted recipients in any 30-day time period, or one million attempted recipients in any one-year time period; or

2. The revenue generated from a specific UBE transmission exceeded $1,000 or the total revenue generated from all UBE transmitted to any EMSP exceeded $50,000.

C. A person is guilty of a Class 6 felony if he knowingly hires, employs, uses, or permits any minor to assist in the transmission of UBE in violation of subdivision B 1 or subdivision B 2.

§ 18.2-152.4. Computer trespass; penalty.

A. It shall be unlawful for any person ~~to use a computer or computer network without authority and~~, with ~~the~~ *malicious* intent, to:

1. Temporarily or permanently remove, halt, or otherwise disable any computer ~~data, computer programs,~~ *information* or computer software from a computer ~~or computer network~~;

2. Cause a computer to malfunction, regardless of how long the malfunction persists;

3. Alter, *damage, destroy, disable,* or erase any computer ~~data, computer programs,~~ *information* or computer software;

4. Effect the creation or alteration of a financial instrument or of an electronic transfer of funds;

5. Cause physical injury to the property of another; ~~or~~

6. Make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer ~~data, computer programs~~ *information,* or computer software residing in, communicated by, or produced by a computer ~~or computer network~~*;*

7. [Repealed].

8. Install computer software on the computer of another, without the authorization of the owner; or

9. Disable or disrupt the ability of a computer to share or transmit its computer information to other computers or to any related computer equipment or devices, including, but not limited to, printers, scanners, or fax machines, through the direct or indirect use of a computer.

B. *It shall be unlawful for any person to maliciously obtain any computer information, without authority, through the direct use of a computer.*

C. Any person who violates this section shall be guilty of computer trespass, which offense shall be punishable as a Class 1 misdemeanor. If there is damage to the property of another valued at ~~$2,500~~ *$1,000* or more caused by such person's ~~malicious~~ act in violation of this section, the offense shall be punishable as a Class 6 felony.

~~C~~*D.* Nothing in this section shall be construed to interfere with or prohibit terms or conditions in a contract or license related to computers, computer ~~data, computer networks~~ *information,* computer operations, ~~computer programs,~~ computer services, or computer software or to create any liability by reason of terms or conditions adopted by, or technical measures implemented by, a Virginia-based electronic mail service provider to prevent the transmission of unsolicited electronic mail in violation of this article. Nothing in this section shall be construed to prohibit the monitoring of computer usage of, the otherwise lawful copying of data of, or the denial of computer or Internet access to a minor by a parent or legal guardian of the minor.

§ 18.2-152.5. Computer invasion of privacy; penalties.

A. A person is guilty of the crime of computer invasion of privacy when he uses a computer ~~or computer network~~ and intentionally examines without authority any employment, salary, credit ~~or any other~~, financial or ~~personal~~ *identifying* information, *as defined in clauses (iii) through (xiii) of subsection C of § 18.2-186.3,* relating to any other person. "Examination" under this section requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed.

B. The crime of computer invasion of privacy shall be punishable as a Class 1 misdemeanor.

C. Any person who violates this section after having been previously convicted of a violation of this section or any substantially similar laws of any other state or of the United States is guilty of a Class 6 felony.

D. Any person who violates this section and sells or distributes such information to another is guilty of a Class 6 felony.

E. Any person who violates this section and uses such information in the commission of another crime is guilty of a Class 6 felony.

F. This section shall not apply to any person collecting information that is reasonably needed to (i) protect the security of a computer, computer service, or computer business, or to facilitate diagnostics or repair in connection with such computer, computer service, or computer business or (ii) determine whether the computer user is licensed or authorized to use specific computer software or a specific computer service.

§ 18.2-152.5:1. Using a computer to gather identifying information; penalties.

A. It is unlawful for any person, other than a law-enforcement officer, as defined in § 9.1-101, and acting in the performance of his official duties, to use a computer to fraudulently obtain, fraudulently access, or fraudulently record identifying information, as defined in clauses (iii) through (xiii) of subsection C of § 18.2-186.3. Any person who violates this section is guilty of a Class 6 felony.

B. Any person who violates this section and sells or distributes such information to another is guilty of a Class 5 felony.

C. Any person who violates this section and uses such information in the commission of another crime is guilty of a Class 5 felony.

§ 18.2-152.6. Theft of computer services; penalties.

Any person who willfully ~~uses a computer or computer network, with intent to obtain~~ *obtains* computer services without authority~~, shall be~~ *is* guilty of the crime of theft of computer services, ~~which shall be~~ punishable as a Class 1 misdemeanor. If the theft of computer services is valued at $2,500 or more, he is guilty of a Class 6 felony.

§ 18.2-152.6:1. Use of a computer to circumvent computer security measures; penalties.

A. Any person who uses a computer to circumvent a security measure that controls access to a computer, including but not limited to passwords, firewalls, or access codes, and does so without the authorization of the owner of such computer, is guilty of a Class 1 misdemeanor.

B. Any person who violates this section after having been previously convicted of a violation of this section or any substantially similar laws of any other state or of the United States is guilty of a Class 6 felony.

C. Any person who violates this section in the commission of a felony is guilty of a Class 6 felony.

§ 18.2-152.7. Personal trespass by computer; penalty.

A. A person is guilty of the crime of personal trespass by computer when he uses a computer ~~or computer network without authority and with the intent~~ to cause physical injury to an individual.

B. If committed maliciously, the crime of personal trespass by computer shall be punishable as a Class 3 felony. If such act is done unlawfully but not maliciously, the crime of personal trespass by computer shall be punishable as a Class 6 felony.

§ 18.2-152.7:1. Harassment by computer; penalty.

If any person, with the intent to coerce, intimidate, or harass any person, shall use a computer ~~or computer network~~ to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or make any suggestion or proposal of an obscene nature, or threaten any illegal or immoral act, he shall be guilty of a Class 1 misdemeanor.

§ 18.2-152.8. Property capable of embezzlement.

For purposes of § 18.2-111, personal property subject to embezzlement shall include:

1. Computers ~~and computer networks~~;

2. Financial instruments, computer ~~data~~ *information*, computer programs, computer software and all other personal property regardless of whether they are:

a. Tangible or intangible;

b. In a format readable by humans or by a computer;

c. In transit between computers or within a computer network or between any devices which comprise a computer; or

d. Located on any paper or in any device on which it is stored by a computer or by a human; and

3. Computer services.

§ 18.2-152.12. Civil relief; damages.

A. Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, "damages" shall include loss of profits.

B. If the injury under this article arises from the transmission of unsolicited bulk electronic mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider where the defendant has knowledge of the authority or policies of the EMSP or where the authority or policies of the EMSP are available on the electronic mail service provider's website, the injured person, other than an electronic mail service provider, may also recover attorneys' fees and costs, and may elect, in lieu of actual damages, to recover the lesser of $10 for each and every unsolicited bulk electronic mail message transmitted in violation of this article, or $25,000 per day. The injured person shall not have a cause of action against the electronic mail service provider that merely transmits the unsolicited bulk electronic mail ~~over its computer network~~. Transmission of electronic mail from an organization to its members shall not be deemed to be unsolicited bulk electronic mail.

C. If the injury under this article arises from the transmission of unsolicited bulk electronic mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider where the defendant has knowledge of the authority or policies of the EMSP or where the authority or policies of the EMSP are available on the electronic mail service provider's website, an injured electronic mail service provider may also recover attorneys' fees and costs, and may elect, in lieu of actual damages, to recover $1 for each and every intended recipient of an unsolicited bulk electronic mail message where the intended recipient is an end user of the EMSP or $25,000 for each day an attempt is made to transmit an unsolicited bulk electronic mail message to an end user of the EMSP. In calculating the statutory damages under this provision, the court may adjust the amount awarded as necessary, but in doing so shall take into account the number of complaints to the EMSP generated by the defendant's messages, the defendant's degree of culpability, the defendant's prior history of such conduct, and the extent of economic gain resulting from the conduct. Transmission of electronic mail from an organization to its members shall not be deemed to be unsolicited bulk electronic mail.

D. At the request of any party to an action brought pursuant to this section, the court may, in its discretion, conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, ~~computer network,~~ computer ~~data,~~ ~~computer program~~ *information*, and computer software involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party and in such a way as to protect the privacy of nonparties who complain about violations of this section.

E. The provisions of this article shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

F. A civil action under this section must be commenced before expiration of the time period prescribed in § 8.01-40.1. In actions alleging injury arising from the transmission of unsolicited bulk electronic mail, personal jurisdiction may be exercised pursuant to § 8.01-328.1.

§ 18.2-152.14. Computer as instrument of forgery.

The creation, alteration, or deletion of any computer ~~data~~ *information* contained in any computer ~~or computer network~~, which, if done on a tangible document or instrument, would constitute forgery under Article 1 (§ 18.2-168 et seq.) of Chapter 6 of this ~~Title~~ *title,* will also be deemed to be forgery. The absence of a tangible writing directly created or altered by the offender shall not be a defense to any crime set forth in Article 1 (§ 18.2-168 et seq.) of Chapter 6 of this ~~Title~~ *title* if a creation, alteration, or deletion of computer ~~data~~ *information* was involved in lieu of a tangible document or instrument.

§ 18.2-152.17. Additional penalties.

In addition to any other penalties specified by statute, the punishment of any person convicted of a felony under this article shall include a mandatory minimum fine of $1,000.

§ 19.2-8. Limitation of prosecutions.

A prosecution for a misdemeanor, or any pecuniary fine, forfeiture, penalty or amercement, shall be commenced within one year next after there was cause therefor, except that a prosecution for petit larceny may be commenced within five years, and for an attempt to produce abortion, within two years after commission of the offense.

A prosecution for violation of laws governing the placement of children for adoption without a license pursuant to § 63.2-1701 shall be commenced within one year from the date of the filing of the petition for adoption.

A prosecution for making a false statement or representation of a material fact knowing it to be false or knowingly failing to disclose a material fact, to obtain or increase any benefit or other payment under the Virginia Unemployment Compensation Act (§ 60.2-100 et seq.) shall be commenced within three years next after the commission of the offense.

A prosecution for any violation of §§ 10.1-1320, 62.1-44.32 (b), 62.1-194.1, or Article 11 (§ 62.1-44.34:14 et seq.) of Chapter 3.1 of Title 62.1 ~~which~~ *that* involves the discharge, dumping or emission of any toxic substance as defined in § 32.1-239 shall be commenced within three years next after the commission of the offense.

Prosecution of Building Code violations under § 36-106 shall commence within one year of discovery of the offense by the owner or by the building official; provided that such discovery occurs within two years of the date of initial occupancy or use after construction of the building or structure, or the issuance of a certificate of use and occupancy for the building or structure, whichever is later. However, prosecutions under § 36-106 relating to the maintenance of existing buildings or structures as contained in the Uniform Statewide Building Code shall commence within one year of the discovery of the offense.

Prosecution of nonfelonious offenses which constitute malfeasance in office shall commence within two years next after the commission of the offense.

Prosecution of any violation of ~~§~~§ 55-79.87, 55-79.88, 55-79.89, 55-79.90, 55-79.93, 55-79.94, 55-79.95, 55-79.103, or any rule adopted under or order issued pursuant to § 55-79.98, shall commence within three years next after the commission of the offense.

Prosecution of illegal sales or purchases of wild birds, wild animals and freshwater fish under § 29.1-553 shall commence within three years after commission of the offense.

Prosecution of violations under Title 58.1 for offenses involving false or fraudulent statements, documents or returns, or for the offense of willfully attempting in any manner to evade or defeat any tax or the payment thereof, or for the offense of willfully failing to pay any tax, or willfully failing to make any return at the time or times required by law or regulations shall commence within three years next after the commission of the offense, unless a longer period is otherwise prescribed.

Prosecution of violations of subsection A or B of § 3.1-796.122 shall commence within five years of the commission of the offense, except violations regarding agricultural animals shall commence within one year of the commission of the offense.

A prosecution for a violation of § 18.2-386.1 shall be commenced within five years of the commission of the offense.

A prosecution for any violation of the Campaign Finance Disclosure Act (§ 24.2-900 et seq.) shall commence within one year of the discovery of the offense but in no case more than three years after the date of the commission of the offense.

A prosecution of a crime that is punishable as a misdemeanor pursuant to the Virginia Computer Crimes Act (§ 18.2-152.1 et seq.) shall be commenced before the earlier of (i) five years after the commission of the last act in the course of conduct constituting a violation of the article or (ii) one year after the existence of the illegal act and the identity of the offender are discovered by the Commonwealth, by the owner, or by anyone else who is damaged by such violation.

Nothing in this section shall be construed to apply to any person fleeing from justice or concealing himself within or without this Commonwealth to avoid arrest or be construed to limit the time within which any prosecution may be commenced for desertion of a spouse or child or for neglect or refusal or failure to provide for the support and maintenance of a spouse or child.

§ 19.2-249.2. Venue for prosecution of computer crimes.

For the purpose of venue under the Virginia Computer Crimes Act (§ 18.2-152.1 et seq.), any violation of the article shall be considered to have been committed in any county or city:

1. In which any act was performed in furtherance of any course of conduct that violated this article;

2. In which the owner has his principal place of business in the Commonwealth;

3. In which any offender had control or possession of any proceeds of the violation or of any books, records, documents, property, financial instrument, computer software, computer program, computer data, or other material or objects that were used in furtherance of the violation;

4. From which, to which, or through which any access to a computer or computer network was made whether by wires, electromagnetic waves, microwaves, or any other means of communication;

5. In which the offender resides; or

6. In which any computer that is an object or an instrument of the violation is located at the time of the alleged offense.

2. That §§ 18.2-152.9 and 18.2-152.10 of the Code of Virginia are repealed.

3. That the provisions of this act may result in a net increase in periods of imprisonment or commitment. Pursuant to § 30-19.1:4, the estimated amount of the necessary appropriation cannot be determined for periods of imprisonment in state adult correctional facilities and is $0 for periods of commitment to the custody of the Department of Juvenile Justice.