

BRIEF SUMMARY OF VIRGINIA TRADE SECRET LAW

I. VIRGINIA TRADE SECRET LAW

Virginia has adopted the Virginia Uniform Trade Secrets Act (Va. Code §§ 59.1-336 to 59.1-343), often referred to as VUTSA to distinguish it from the model Uniform Trade Secrets Act (UTSA).

II. SIGNIFICANT DIFFERENCES BETWEEN VUTSA AND MODEL UTSA

VUTSA differs from the model UTSA because it:

- Expands the definition of improper means to also include the unauthorized use of a computer or computer network (Va. Code Ann. § 59.1-336).
- Restricts a punitive damages award to either of the following, whichever is less:
 - 1) two times the monetary damages; or
 - 2) \$350,000.

(Va. Code § 59.1-338(8)).

- Excludes a motion to terminate an injunction made or resisted in bad faith as a basis for an award of attorneys' fees (Va. Code Ann. § 59.1-338).
- Excludes a severability provision.

III. DEFINITION OF A TRADE SECRETE

The Virginia Uniform Trade Secrets Act (VUTSA) defines a trade secret as information that meets all of the following criteria:

- Includes at least one of the following: formula; pattern; compilation; program; device; method; technique; or process.
- Derives actual or potential independent economic value because it is:
 - i. generally unknown; and
 - ii. not readily ascertainable by proper means and by another person who can obtain economic value from its disclosure or use.
- Is the subject of reasonable efforts under the circumstances to maintain its secrecy.

Va. Code Ann. § 59.1-336

IV. EXAMPLES OF TRADE SECRETS

Virginia courts have found the following types of information to be trade secrets:

- Customer lists, pricing information, marketing and sales techniques and product information (MicroStrategy, Inc. v. Bus. Objects, S.A., 331 F. Supp. 2d 396 (E.D. Va. 2004)).
- Source code or object code where copyright ownership is not at issue (Avtec Sys Inc. v. Peiffer. 21 F.3d 568 (4th Cir. 1994)).
- Software components (MicroStrategy Inc. v. Li, 601S.E.2d580 (Va. 2004)).
- A document containing a competitive strategy against the defendant that was only provided to the employer's field sales staff (MicroStrategy, Inc. v. Bus. Objects, S.A., 331 F. Supp. 2d 396 (E.D. Va. 2004)).
- A computer database of customer and product information (One Stop Deli, Inc. v. Franco's, Inc., No. 93-090-H, 1993 WL 513298 (W.D. Va. Dec. 7, 1993)).
- Manufacturing process for compressed foam for use in the inner packaging industry (Dionne v. Se. Foam Converting & Packaging, Inc .. 397 S.E.2d 110 (Va. 1990)).
- Schedule of customer discounts (MicroStrategy, Inc. v. Bus. Objects, S.A, 331 F. Supp. 2d 396 (E.D. Va. 2004)).
- Compilation of public facts where the compilation itself is confidential (Comprehensive Techs. Int'l, Inc. v. Software Artisans, Inc., 3 F.3d 730 (4th Cir. 1993)).

V. NOT TRADE SECRETS

The following types of information have been found not to be trade secrets:

- Patented subject matter (*MicroStrategy, Inc. v. Bus. Objects, S.A.*, 331 F. Supp. 2d 396 (E.D. Va. 2004)).
- Passwords that were not based on a special formula or algorithm (*State Analysis, Inc. v. Am. Fin. Servs. Ass'n*, 621 F. Supp. 2d 309 (E.D. Va. 2009)).
- Church documents contained in an open court file and posted on the internet (*Religious Tech. Ctr. v. Lerma*, 897 F. Supp. 260 (E.D. Va. 1995)).
- An outdated contacts list that was readily ascertained through proper means, such as a phone directory or phone operator (*Tryco, Inc. v. U.S. Med. Source, LLC*, 80 Va. Cir. 619 (Va. Cir. Ct. 2010)).
- Employment negotiations (*Rohrbaugh v. Kreidler*, 71 Va. Cir. 298 (Va. Cir. Ct. 2006)).

VI. REASONABLE EFFORTS TO MAINTAIN SECRECY

A trade secret owner is not required to maintain absolute secrecy of the trade secret. Information is only required to be kept secret by reasonable efforts under the circumstances (*MicroStrategy Inc. v. Bus. Objects, S.A.* 331 F. Supp. 2d 396 (E.D. Va. 2004)).

For example, a trade secret owner may disclose his trade secret to a licensee, employee or third party in express or implied confidence, and still maintain its secrecy (*Dionne v. Se. Foam Converting & Packaging, Inc.*, 397 S.E.2d 110 (Va. 1990)).

Reasonable efforts to maintain secrecy include:

- Restricting access to information.
- Using confidentiality agreements.
- Using physical or software-related barriers to restrict access to the information.
- Disclosing sealed information during a trial.
- Disclosing unsealed information during a trial that has no evidence of further publication.

MicroStrategy, Inc. v. Bus. Objects, S.A., 331 F. Supp. 2d 396 (E.D. Va. 2004)

VII. MISAPPROPRIATION

Misappropriation is defined in three different ways:

- Acquisition.
- Disclosure.
- Use.

Va. Code Ann. § 59.1-336

VIII. ACQUISITION AS MISUSE

A trade secret can be misappropriated if the acquirer knew or had reason to know that the trade secret was acquired by improper means

Va. Code Ann. § 59.1- 336

IX. DISCLOSURE OR USE OF TRADE SECRET AS MISUSE

Disclosure or use of a trade secret of another without express or implied consent can constitute misappropriation where the person does either of the following:

- Uses improper means to acquire knowledge of the trade secret.
- At the time of disclosure or use, knew or had reason to know that the trade secret was:
 - i. derived from another who used improper means to acquire it;
 - ii. acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use;
 - iii. derived from or through another who owed a duty to maintain its secrecy or limit its use; or
 - iv. acquired by accident or mistake.

Va. Code § 59.1-336

X. DEFINITION OF IMPROPER MEANS

Improper means includes:

- Theft.
- Bribery.
- Misrepresentation.
- Unauthorized use of a computer or computer network.
- Breach of a duty or inducement of a breach of duty to maintain secrecy.
- Espionage through electronic or other means.

Va. Code § 59.1-336

Espionage is the use of a spy to obtain confidential information about a competing company (MicroStrategy, Inc. v. Bus. Objects, S.A., 331 F. Supp. 2d 396 (E.D. Va. 2004)).

XI. STATUTE OF LIMITATIONS

The Virginia Uniform Trade Secrets Act (VU TSA) imposes a three-year statute of limitations. Specifically, the three-year period begins to run when either:

- The misappropriation is discovered.
 - The misappropriation should have been discovered by exercising reasonable diligence.
- Va. Code § 59.1-340

A continuing misappropriation constitutes a single claim. Va. Code § 59.1-340

XII. REMEDIES

A plaintiff may recover damages for misappropriation, unless monetary recovery is inequitable because the acquirer made a material and prejudicial change of position before acquiring knowledge of the misappropriation.

Va. Code Ann. § 59.1- 338(A)

Under the Virginia Uniform Trade Secrets Act (VUTSA) relief may include:

- *Monetary damages.* Monetary damages can include actual loss and unjust enrichment caused by the misappropriation (Va. Code § 59.1-338(A)).
- *A reasonable royalty.* Instead of awarding monetary damages, courts may award a reasonable royalty for the unauthorized disclosure or use of a trade secret. Courts may use the actual market value of the trade secret to determine the royalty amount (Am. Sales Corp. v. Adventure Travel, Inc .. 867 F. Supp. 378 (E.D. Va. 1994)).
- *Punitive damages.* Courts may award punitive damages if willful and malicious misappropriation exists. The damage amount may equal either of the following, whichever is less:

- two times the monetary damages or reasonable royalty; or
- \$350,000.

Va. Code § 59.1 -338(A)

- *Reasonable attorneys' fees.* Courts may award reasonable attorneys' fees if:
 - the misappropriation claims was made in bad faith; or
 - willful and malicious misappropriation exists.

Va. Code § 59.1-338.1

MicroStrategy, Inc. v. Bus. Objects. S.A., 331 F. Supp. 2d 396 (E.D. Va. 2004).)

- *Affirmative acts.* A court may issue an order compelling affirmative acts to protect the trade secret (Va. Code § 59. 1-337(C)).
- *Injunctive relief.* A court may issue an injunction for actual or threatened misappropriation to prevent future misappropriation. Va. Code § 59. 1-337(A)

Virginia Computer Crimes Act

§ 18.2-152.1

Specific offenses prohibited

1. Computer Fraud
2. Spam
3. Computer Trespass
4. Computer Invasion of Privacy
5. Gathering Identifying Information
6. Theft of Computer Services
7. Personal Trespass by Computer
8. Harassment by Computer

1. Computer Fraud §18.2-152.3

- ▶ Using a computer or network without authority to embezzle, steal or obtain property by false pretenses
- ▶ Felony if the property or services obtained is \$200 or more
- ▶ Misdemeanor if the property or service obtained is less than \$200

2. Spam §18.2-152.3:1

- ▶ Using a computer or network with the intent to falsify or forge electronic information
 - ▶ Generally, a violation is a misdemeanor unless the volume of spam
 - ▶ exceeds 10,000 attempted recipients in a 24-hour period, or
 - ▶ exceeds 100,000 attempted recipients in a 30-day time period, or
 - ▶ exceeds 1,000,000 attempted recipients within a year,
- Then it is a Class 6 felony
- ▶ If the revenue generated from a specific transmission is >\$1,000 or total revenue from all spam transmitted to any EMSP exceeds \$50,000 then it is a Class 6 felony
 - ▶ Any person who hires or permits a minor to assist in the transmission is guilty of a Class 6 felony

3. Computer Trespass

§18.2-152.4

- ▶ Includes disabling, removing, halting, or causing a malfunction to an unauthorized computer network
- ▶ Any person who violates this section is guilty of a misdemeanor
- ▶ However, if the individual trespasses on more than one person's computer or installs software that records a majority of keystrokes, that person is guilty of a Class 6 felony

4. Computer Invasion of Privacy §18.2-152.5

- ▶ Using a computer or network to intentionally examine confidential information without authority
- ▶ Violation is a Class 1 misdemeanor
- ▶ A second violation is a Class 6 felony
- ▶ Any person who violates this and sells or distributes the information is guilty of Class 6 felony
- ▶ Any person who violates this and uses the information in the commission of another crime is guilty of a Class 6 felony

5. Gathering Identifying

Information §18.2-152.5.1

- ▶ Using a computer to obtain, access, or record through trickery or deception any personally identifying information
- ▶ Violation of this section is a Class 6 felony
- ▶ Any person who violates this and sells or distributes the information is guilty of a Class 5 felony
- ▶ Any person who violates this to use the gathered information in the commission of another crime is guilty of a Class 5 felony

6. Theft of Computer

Services §18.2-152.6

- ▶ Willfully obtaining computer services without authority
- ▶ Violation is a Class 1 misdemeanor unless the theft is value at \$2,500 or more, then the violation is Class 6 felony

7. Personal Trespass §18.2-152.7

- ▶ Using a computer or network to cause physical injury to an individual
- ▶ If done maliciously, the violation is a Class 6 felony
- ▶ If not done maliciously, then the violation is a Class 3 felony

8. Harassment by

Computer §18.2-152.7:1

- ▶ The act of coercing, intimidating, or otherwise harassing someone through a computer or network
- ▶ Violation is a Class 1 misdemeanor

Civil Relief §18.2-152.12

- ▶ A violation of this Act does not require malicious intent in a Civil suit
- ▶ The injured person does not have a cause of action against the electronic mail service provider
- ▶ Transmission of electronic mail from an organization to its members is *not* spam
- ▶ Statute of limitations, pursuant to §8.01-40.1, is (i) five years after the last act in the course of conduct constituting a violation of the Computer Crimes Act or (ii) two years after the P discovers or reasonably should have discovered the last act in the course of conduct constituting a violation of the Computer Crimes Act, whichever is first.

Fact Pattern Trade Secrets

The Soup Fascist serves the best soup in Northern Virginia. People line up around the corner to get a taste of his delicious soups. His recipes are kept a secret, even from his employees. The Soup Fascist gives his friend Kramer an armoire that has been sitting in the Fascist's basement for years after Kramer tells him a story about two tough guys robbing him on the street. Kramer gives the armoire to his friend Elaine, who has been banned from the Soup Fascist's restaurant due to her improper ordering technique. Elaine opens the bottom drawer of the armoire and is delighted to discover a dozen of the Soup Fascist's coveted soup recipes were inadvertently left in the piece of furniture.

Question 1:

Can Elaine use the recipes in a competing business without exposing herself to potential liability under the Uniform Trade Secrets Act?

Answer Question 1:

No. Even though the recipes were obtained by accident, her use of the recipes constitute a misappropriation under Va. Code sec. 59.1-336(2)(b)(4), which includes the following as a definition of misappropriation: "Disclosure or use a trade secret of another without express or implied consent by a person who...At the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was...Acquired by accident or mistake."

Question 2:

What if Elaine doesn't sell the soup, but instead only uses the recipes for family gatherings. Does that change your answer?

Answer Question 2:

No. In *Collelo v. Geographic Services*, 283 Va. 56 (2012), the Supreme Court of Virginia held “the Trade Secrets Act does not require that one who is accused of misappropriating a trade secret use the allegedly misappropriated trade secret to compete with the holder of the trade secret.”

Question 3:

What if Elaine does nothing with the recipes? If the Soup Fascist finds out that she has them, could he successfully sue under the Uniform Trade Secret Act?

Answer Question 3:

Not likely. If Elaine doesn't "disclose" or "use" the trade secret, she hasn't misappropriated the trade secret under Va. Code sec. 59.1-336(2). However, an injunction under Va. Code sec. 59.1-337 could be an option for the Soup Fascist. That section provides that actual or threatened misappropriation may be enjoined.

Changing the facts—let's say Kramer and Elaine were both banned from the Soup Fascist's restaurant. Kramer and the Soup Fascist are not friends at all. Kramer steals the recipes from the Soup Fascist. Knowing Elaine wants to get back at the Soup Fascist, Kramer gives the recipes to Elaine and tells her to have fun with them. By now, Elaine has gotten over the incident, so she simply files the recipes away in a drawer never to be seen again.

Question:

Under these facts, has Elaine misappropriated the Soup Fascist's trade secrets?

Answer:

Yes.

Mere acquisition of a trade secret by person who knows (or has reason to know) that it was acquired by improper means constitutes misappropriation under Va. Code sec. 59.1-336(1). Elaine knows (or has reason to know) that Kramer used improper means (theft) to get the recipes. Even though she doesn't use or disclose the trade secret, her acquisition is enough to meet the statutory definition under these facts.



Virginia Computer Crimes

Act

HYPOS



Computer Crimes- Fact Pattern 1

(Page 1)

- ▶ Brian Thomas began to work for Tryco in 2005 as a customer sales representative. His two main accounts were Lackland Air Force Base ("Lackland") and Air Force Medical Logistics Office ("AMFLO").
- ▶ Went to work for a competitor, USMS, in April 2008.
- ▶ Was asked to tie up some loose ends and to prepare instructions for the person who was going to be taking over his accounts. He cleaned out his desk and cleared his desktop computer of his personal files by transferring them to a flash drive.
- ▶ He also created, at Tryco's instruction a document called "How to Quote Lackland" to pass on to his successor. The document included the names of buyers he worked with, their phone numbers, and information on how to mark-up sales.

Computer Crimes- Fact Pattern 1

(Page 2)

- ▶ After transferring the files onto the flash drive, Thomas deleted all files including the "Lackland Contacts" list
- ▶ When he examined the flash drive, he found two documents that he asserted had been mistakenly copied:
 - ▶ the "Lackland Contacts" list was among them
 - ▶ He promptly returned the entire flash drive to Tryco.
 - ▶ Asserted that he never used the flash drive at USMS

Computer Crimes- Fact Pattern 1

(Page 3)

▶ Cause of action for violation of the Computer Crimes Act?

▶ YES OR NO

Computer Crimes- Fact Pattern 1

(Page 4)

- ▶ Tryco sued Brian Thomas for a civil violation of the Computer Trespass Act
- ▶ Under the Computer Trespass Act, it is "unlawful for any person, with malicious intent, to ... erase any computer data, computer programs or computer software ... or ... make or cause to be made an unauthorized copy ... or computer data, computer programs or computer software residing in ... a computer or computer network[.]" Va.Code Ann. § 18.2-152.4.
- ▶ In a civil suit, a violation of the Computer Trespass Act does not require a finding of malice. It is enough under the statute that the defendant is shown to have purposefully committed the acts that deprived his employer of computer files or records. Va.Code Ann. § 18.2-152.12.

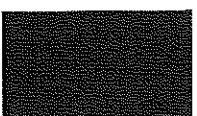
Computer Crimes- Fact Pattern 1

(Page 5)

- ▶ No violation of the Act because no damages could be shown -
 - ▶ Tyco, Inc. v. U.S. Med. Source, L.L.C., 80 Va. Cir. 619 (2010) (Fairfax County)
 - ▶ Document was outdated
 - ▶ Tyco already had the information
- ▶ What if Tyco had been damaged?
 - ▶ Violation?

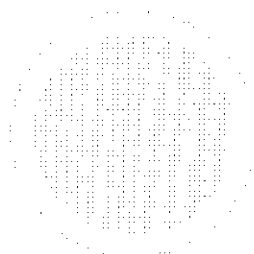
Computer Crimes- Fact Pattern 1

(Page 5)



▶ If Tyco had been damaged would there have been a violation?

▶ Likely



Computer Crimes - Fact Pattern 2(Page 1)

- LOVELEN PYLES EMPLOYED BY TECH SYSTEMS INC. (TSI)
 - HR Manager
 - April 1, 2012 – TSI's IT department discovered that the server was down
 - Investigation determined that:
 - Someone broke into the secure server room
 - Disconnected the components
 - Accessed the financed service and change the start-up sequence so the server would fail to load
 - TSI concluded it was Ms. Pyles

Computer Crimes- Fact Pattern

2(Page 2)

- ▶ Ms. Pyles was terminated
- ▶ She then forwarded emails to employees, vendors, and customers before she returned her Blackberry to TSI
- ▶ She deleted the forwarded emails – to cover up the incriminating emails
- ▶ TSI sued Pyles for a violation of the Virginia Computer Crimes Act
- ▶ Sufficient cause of action?

YES/NO

Computer Crimes- Fact Pattern

2(Page 3)

- ▶ Cause of action existed for violation of the VCCA
- ▶ It shall be unlawful for any person, with malicious intent, to:
 - ▶ 1. Temporarily or permanently remove, halt, or otherwise disable any computer data, computer programs or computer software from a computer or computer network;
 - ▶ 2. Cause a computer to malfunction, regardless of how long the malfunction persists; [or]
 - ▶ 3. Alter, disable, or erase any computer data, computer programs or computer software.

Computer Crimes- Fact Pattern

2(Page 4)

- ▶ A reasonable jury found Ms. Pyles liable for sabotaging and disabling TSI's computer server which caused the server to malfunction. Tech Systems, Inc. v. Pyles, 2013 WL 4033650, Slip Copy (E.D. Va. 2013)
- ▶ \$300,000 jury verdict
- ▶ Was TSI entitled to attorneys fees?

YES/NO

Computer Crimes- Fact Pattern

2(Page 4)

- ▶ Yes
- ▶ "Tech Systems is entitled to reasonable attorney's fees and the costs of litigation pursuant to the VCCA."
- ▶ Why?

Amount of damage done to TSI, or

Statutory right (automatically entitled to attorneys fees), or

Malicious intent

Computer Crimes- Fact Pattern

2(Page 5)

- ▶ The Court holds that the jury's award demonstrates the jury found malicious intent.
- ▶ The jury was instructed that liability on this claim required TSI demonstrate that Ms. Pyles committed any of the prohibited acts [in the VCCA] with malicious intent. Therefore, TSI is entitled to recover the costs of not only attorneys' fees but also the cost of litigation.

Hypo:

Plaintiff husband filed for divorce on the grounds that defendant wife had constructively deserted the marriage. Wife filed a cross-complaint seeking a divorce on the grounds that the husband had committed acts of sodomy and/or buggery. Wife filed a motion for examination of the husband's password protected files on computers.

The wife claimed the husband viewed child pornography on family computers and had sex with a child. After separation, she took three computers to a computer company. It examined files on the hard drives, some of which were photos the wife claimed depicted her husband having sex with men. He denied that he was the man depicted engaging in sodomy.

Pursuant to Va. Code Ann. § 18.2-152.5, the wife sought court authority for the company to access password protected files and view the husband's e-mail messages to determine if he was the man in those pictures and if he had possessed child pornography.

Can the Court grant authority for wife to access password protected files and husband's e-mail?

Court's Reasoning

- A person is without authority to intentionally examine information protected by § 18.2-152.5 if she "knows or reasonable should know that [s]he has no right or permission or knowingly acts in a manner exceeding such right or permission." § 18.2-152.2.
- The statute does not state that the circuit courts have power to grant authority. The former § 18.2-152.2 stated that a person was "without authority" when she "has no right of permission of the owner to use a computer or computer network." Va. Code § 18.2-152.2(2004) (emphasis added).
- The deletion of the limiting phrase "of the owner" in the current statute is evidence that a person/entity, in addition to the owner, can grant authority.
- Law enforcement officers acting pursuant to a valid search warrant have authority to view these documents. *Rosa v. Commonwealth*, 48 Va. App. 93, 96, 628 S.E.2d 92 (2006).
- The courts, therefore, have the power to grant authority to examine information protected by § 18.2-152.5.

- Under Rule 4:9, the court has the power to require Plaintiff to produce his actual hard drives so Defendant can "inspect and copy" the writings, photographs, or data compilations stored therein.
- Because the court is vested with the greater authority to force a party to produce documents, photographs, information, and data compilation which would otherwise be protected by § 18.2-152.5, the court is vested with the constituent power to grant "authority" to a party to access said documents, photographs, information, and data compilation already in the requesting party's possession or control.
- **Holding:** The circuit courts may, pursuant to the powers governing discovery, grant "authority" for parties to access information otherwise protected by Va. Code § 18.2-152.5.

Albertson v. Albertson, 73 Va. Cir. 94, 97 (Cir. Ct. 2007)

Albertson v. Albertson

Circuit Court of Fairfax County, Virginia

March 15, 2007, Decided

CL-2006-9521

Reporter

73 Va. Cir. 94; 2007 Va. Cir. LEXIS 132

Paul D. Albertson v. Shelia E. Albertson

Core Terms

files, documents, imaged, discovery, hard drive, password, e-mail, inspect, party's, child pornography, adultery, buggery, papers, sodomy, incriminating, compulsion, circuit court, court order, self-incrimination, Amendment's, photographs, responsive, computers, pictures, writings, sexual

Case Summary

Procedural Posture

Plaintiff husband filed for divorce on the grounds that defendant wife had constructively deserted the marriage by entering into a lesbian relationship. The wife filed a cross-complaint seeking a divorce on the grounds that the husband had committed acts of sodomy and/or buggery. She filed a motion for examination of the husband's password protected files on computers. He claimed granting the motion would violate his Fifth Amendment rights.

Overview

The wife claimed the husband viewed child pornography on family computers and had sex with a child. After separation, she took three computers to a computer company. It examined files on the hard drives, some of which were photos the wife claimed depicted her husband having sex with men. He denied that he was the man depicted engaging in sodomy. Pursuant to Va. Code Ann. § 18.2-152.5, the wife sought court authority for the company to access password protected files and view the husband's e-mail messages to determine if he was the man in those pictures and if he had possessed child pornography. The court noted that the e-mail correspondence sought could not only prove the wife's claim for divorce on fault grounds, but could impact equitable distribution and custody. Under Va. Sup. Ct.

R. 4:9, the court could grant "authority" for the wife to access information otherwise protected by Va. Code Ann. § 18.2-152.5. As such an order did not require the husband to perform a testimonial act, it was not barred by the Fifth Amendment. However, Va. Sup. Ct. R. 4:9 limited inspection and copying to "designated" documents; it did not allow the wife to access the computer files *carte blanche*.

Outcome

The wife was entitled to inspect (A) e-mail messages regarding (1) whether the husband was the man in the already obtained photos performing sexual acts on other men, (2) the identity of the other individual in the pictures, (3) whether the husband committed adultery, sodomy and/or buggery; and (B) any other photos of the husband engaged in adultery, sodomy and/or buggery.

LexisNexis® Headnotes

Computer & Internet Law > Criminal Offenses > Data Crimes & Fraud

HN1 Under Virginia's computer trespass law, 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 identifying information, as defined in Va. Code Ann. § 18.2-186.3(C)(iii)-(xiii), relating to any other person. Va. Code Ann. § 18.2-152.5. "Passwords" are protected personal information identified by Va. Code Ann. § 18.2-186.3(C)(xii). A person is guilty of violating Va. Code Ann. § 18.2-152.5 unless he or she acted "with authority." § 18.2-152.5.

Constitutional Law > ... > Fundamental Rights > Procedural Due Process > Self-Incrimination Privilege

HN2 The Virginia self-incrimination privilege is construed identically to its federal counterpart in the Fifth Amendment.

Computer & Internet Law > Criminal Offenses > Data Crimes & Fraud

Computer & Internet Law > Procedural Matters > Search & Seizure

HN3 A person is without authority to intentionally examine information protected by Va. Code Ann. § 18.2-152.5 if she knows or reasonably should know that she has no right or permission or knowingly acts in a manner exceeding such right or permission. § 18.2-152.2. A person/entity, in addition to the owner, can grant authority. Law enforcement officers acting pursuant to a valid search warrant have authority to view these documents. The courts, therefore, have the power to grant authority to examine information protected by § 18.2-152.5.

Civil Procedure > Discovery & Disclosure > Disclosure > General Overview

Civil Procedure > ... > Discovery > Methods of Discovery > General Overview

Civil Procedure > ... > Discovery > Methods of Discovery > Inspection & Production Requests

HN4 The Rules of the Supreme Court of Virginia grant great discretion to the circuit courts in their task of overseeing discovery. Specifically, under Va. Sup. Ct. R. 4:9 the court may permit access to land, property, and information when such acts would otherwise be tortious and criminal. Pursuant to Rule 4:9 the court may require a party to allow another party to inspect and copy any designated documents, including writings, photographs, and other data compilations from which information can be obtained, or to inspect and copy, test, or sample any tangible things in the possession, custody, or control of the party upon whom the request is served. Rule 4:9(a).

Civil Procedure > Discovery & Disclosure > Disclosure > General Overview

Civil Procedure > ... > Discovery > Methods of Discovery > Inspection & Production Requests

Computer & Internet Law > Criminal Offenses > Data Crimes & Fraud

HN5 Under Va. Sup. Ct. R. 4:9, the court has the power to require a party to produce his actual computer hard drives so the other party can inspect and copy the writings, photographs, or data compilations stored therein. Because the court is vested with the greater authority to force a party to produce documents,

photographs, information, and data compilation which would otherwise be protected by Va. Code Ann. § 18.2-152.5, the court is vested with the constituent power to grant "authority" to a party to access said documents, photographs, information, and data compilation already in the requesting party's possession or control. Virginia circuit courts may, pursuant to the powers governing discovery, grant "authority" for parties to access information otherwise protected by § 18.2-152.5. Va. Sup. Ct. R. 4:9 limits inspection and copying to "designated" documents. Accordingly, Rule 4:9 does not allow a party to access computer files carte blanche.

Civil Procedure > ... > Discovery > Methods of Discovery > Inspection & Production Requests

Constitutional Law > ... > Fundamental Rights > Procedural Due Process > Self-Incrimination Privilege

HN6 Personal documents are not protected by the Fifth Amendment simply because they are personal in nature and the individual asserts a general privacy interest in keeping their contents private. The Fifth Amendment can not be cut completely loose from the moorings of its language, and made to serve as a general protector of privacy--a word not mentioned in its text and a concept directly addressed in the Fourth Amendment. The Fifth Amendment protects against compelled self-incrimination, not the disclosure of private information. Thus, an individual's Fifth Amendment protection from self-incrimination is not implicated when private papers, writings, documents, and books are prepared without compulsion and are later used to incriminate the individual. Compulsion sufficient to trigger protection by the Fifth Amendment must be governmental compulsion because the protection is a limitation on the federal government's power and Commonwealth of Virginia's power by virtue of the Fourteenth Amendment.

Computer & Internet Law > Privacy & Security > General Overview

Constitutional Law > ... > Fundamental Rights > Procedural Due Process > Self-Incrimination Privilege

HN7 The voluntary writing or receiving of e-mail messages, and the voluntary viewing of any image--either as an e-mail attachment or as an image on an internet web page containing pornographic images of children--is not "compelled" as this terms relates to the Fifth Amendment's privilege against self-incrimination.

Civil Procedure > Discovery & Disclosure > Disclosure > General Overview

HN8 See Va. Sup. Ct. R. 4:1(b)(1).

Civil Procedure > Discovery & Disclosure > Discovery > Protective Orders

HN9 The court may restrict discovery if the court determines that the request is unduly burdensome. Va. Sup. Ct. R. 4:1(b)(1). The court must balance a party's right under the discovery rules to obtain the information against the other party's privacy interests.

Headnotes/Syllabus

Headnotes

The courts have the power to grant authority to examine electronic computer information protected by Va. Code § 18.2-152.5.

The privilege from self-incrimination is not implicated when private papers, writings, documents, and books are prepared without compulsion and are later used to incriminate the individual.

Counsel: **[**1]** William L. Schmidt, Esquire, Fairfax, Virginia.

Grant T. Moher, Esquire, Fairfax, Virginia.

Judges: Kathleen H. MacKay.

Opinion by: Kathleen H. MacKay

Opinion

[*94] OPINION LETTER

Defendant filed a *Motion for Examination and Analysis of Computers* on September 15, 2006. Plaintiff filed a

response on September 21, 2006. The court heard initial arguments on September 29, 2006. At that time the court took the matter under advisement and asked the parties to provide supplemental briefs addressing the procedural, legal, and constitutional issues raised by Defendant's motion and Plaintiff's assertion of a Fifth Amendment privilege. The court heard oral arguments upon the supplemental briefs on November 22, 2006. After a review of the record, and in light of the parties' thorough written submissions and oral presentations, the court is prepared to rule.

Part I – Background

Plaintiff Mr. Albertson filed for divorce on July 28, 2006 on the grounds that Mrs. Albertson had constructively deserted the marriage by entering into a loving and affectionate lesbian relationship. Plaintiff alleged the couple separated and that he left the marital residence on May 29, 2006. Defendant Mrs. Albertson filed an Answer & Cross-Complaint on August **[**2]** **[*95]** 21, 2006. Defendant's Cross-Complaint sought a divorce on the grounds that Plaintiff had committed acts of sodomy and/or buggery in early 2005. Defendant confirmed that Plaintiff left the marital residence on May 29, 2006, but Defendant claimed Plaintiff's departure was precipitated by her finding a pornographic DVD entitled "Couples Love She-Males" ¹ in Plaintiff's possession. In a subsequent pleading, Defendant alleged that immediately before separation, Defendant learned from two friends that Mr. Albertson had an adulterous liaison, involving sexual contact, with both an underage girl and the girl's mother. Defendant further alleged that Mr. Albertson had viewed child pornography on a computer in the past.

Shortly after separation, Defendant took three computers from the marital residence to Sensei Enterprises, Inc., a Computer Forensics/Legal IT corporation ("Sensei"). Sensei "imaged," or made **[**3]** an exact copy, of each computer's hard drive. ² Defendant and Sensei then opened and examined files contained on the "imaged" hard drives. Among these

¹ Defendant alleged that the DVD's packaging depicted various "she-males," a crude slang term for individuals with both male and female genitalia (hermaphrodites), engaged in various sexual activities. The DVD packaging also had the slogan "Couple Who Love R**k H**d C**k on Girls and Boys."

² The parties presented evidence as to the ownership, use, and control of the three computers. The court finds that the blue Dell laptop was purchased from joint funds and though it was initially and primarily used by Plaintiff, Defendant had permission to use the blue Dell laptop and it was often kept **[**4]** in the family room. The court finds that the black Dell laptop was used by Plaintiff as a work computer in the past, but as of the date of separation was kept in the family room and could be used by any member of the family. The court additionally finds that the family computer ("tower hard rive") could be used by any member of

files Defendant found an extensive library of homosexual and hermaphroditic pornography and pictures she contends depict her husband, dressed in women's clothing, engaged in sexual acts with other men. Defendant was unable to open files on the "imaged" hard drive that were password protected. Files are password protected if the computer user must enter a specific password/code before the computer will permit access to open the protected files. Among the password protected files which Defendant could not open were Plaintiff's web-based e-mail accounts.³ [*96] Despite the technological ability to override the password protections, Sensei refused to open the password protected files without a court order expressly granting Sensei such authority.

Defendant now seeks court authority for Sensei and Defendant to access password protected files and view Plaintiff's e-mail messages which may, or may not, reveal whether Plaintiff is the individual engaged in homosexual relations in the pictures. Defendant's inspection of Plaintiff's e-mail correspondences stored on the "imaged" drives could collaterally provide evidence of Plaintiff's (a) other acts of adultery; (b) other non-pictured acts of sodomy or buggery; (c) possession, distribution, or production of child pornography; (d) other illegal acts; and (e) other embarrassing [*5] information.

The relevancy of Defendant's request can not be understated. Plaintiff denies that he has engaged in acts of adultery, sodomy, or buggery. Plaintiff further denies that he is the person performing homosexual acts in the pictures already recovered from non-password protected files. The e-mail correspondences sought could not only prove Defendant's claim for divorce upon fault grounds, but could critically impact the pending Equitable Distribution and future custody arrangements.

HN1 Under Virginia's computer trespass law, "[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 identifying information, as defined in clauses (iii) through (xiii) of subsection C of § 18.2-186.3, relating to

any other person." Va. Code § 18.2-152.5. "Passwords" are protected personal information identified by § 18.2-186.3(C)(xii). A person would be guilty of violating § 18.2-152.5 unless they acted "with authority." Id. Defendant and Sensei now ask the court for authority to violate § 18.2-152.5. Thus, the court must first determine if the court [*6] is vested with the power to grant Sensei and Defendant "authority," as described in § 18.2-152.5.

Plaintiff contends the court may not grant Sensei or any other party "authority" to view his password protected files because it would violate his constitutional rights under the Fifth Amendment to the United States Constitution and Article 1, section 8 of the Virginia Constitution. U.S. CONST. Amend V; CONST. Art. 1, § 8.⁴ The court notes that in Plaintiff's Answer to Defendant's Cross-Complaint, Plaintiff denied having committed acts of adultery, sodomy, or buggery. The Fairfax County Circuit Court, per Judge F. [*97] Bruce Bach held in Leitner v. Leitner, 11 Va. Cir. 281, 282 (1988), that a party's "den[ial of an] allegation of adultery in [an] answer rather than invoking his Fifth Amendment right at that time," in addition to the party's "allegation of faithfulness" waived a subsequent assertion of a Fifth Amendment privilege. However, in Helmes v. Helmes, 41 Va. Cir. 277, 279 (1997), the Fairfax County Circuit Court, per Judge Leslie M. Alden, held that a party's "assertion of lack of knowledge or denial of the allegation does not constitute of waiver of the [Fifth Amendment] privilege." [*7] The court need not reconcile these decisions because Plaintiff stipulated that he waived any Fifth Amendment protection regarding adultery, sodomy, or buggery by failing to invoke the amendment's protection before denying the same. Despite allegations that Plaintiff has viewed child pornography in the past, he has neither admitted nor denied these allegations. Plaintiff now asserts his Fifth Amendment rights and contends that a court order authorizing inspection of his hard drive files could lead to the discovery of incriminating evidence. Whether this court may grant Defendant and Sensei "authority" to violate § 18.2-152.5 and whether Plaintiff's invocation of the Fifth Amendment bars the court from granting said authority are matters of first impression for this court. We consider them in turn.

the family. Accordingly, the court finds that Defendant was entitled to use each computer and no computer, or its hard drive's files, were guarded by means other than password protection.

³ America Online (AOL), Yahoo Mail, Hotmail, and Google G-Mail are examples of web based e-mail accounts.

⁴ **HN2** The Virginia privilege is construed identically to its federal counterpart, Flanary v. Commonwealth, 113 Va. 775, 779, 75 S.E. 289 (1912), thus reference to the Fifth Amendment is shorthand for both constitutional protections.

Part II - Granting "Authority" Under Va. Code § 18.2-152.5

HN3 A person is without authority to intentionally examine information protected by § 18.2-152.5 if she "knows or reasonable [****8**] should know that [s]he has no right or permission or knowingly acts in a manner exceeding such right or permission." § 18.2-152.2. The statute does not state that the circuit courts have power to grant authority. The former § 18.2-152.2 stated that a person was "without authority" when she "has no right of permission of the owner to use a computer or computer network." Va. Code § 18.2-152.2(2004) (emphasis added). The deletion of the limiting phrase "of the owner" in the current statute is evidence that a person/entity, in addition to the owner, can grant authority. Law enforcement officers acting pursuant to a valid search warrant have authority to view these documents. *Rosa v. Commonwealth*, 48 Va. App. 93, 96, 628 S.E.2d 92 (2006). The courts, therefore, have the power to grant authority to examine information protected by § 18.2-152.5.

HN4 The Rules of the Supreme Court of Virginia grant great discretion to the circuit courts in their task of overseeing discovery. Specifically, under *Rule 4:9* the court may permit access to land, property, and information when such [****98**] acts would otherwise be tortious and criminal.⁵ Pursuant to *Rule 4:9* the court may require a party to allow another party to "inspect and [****9**] copy, any designated documents (including writings, . . . photographs, . . . and other data compilations from which information can be obtained, . . . or to inspect and copy, test, or sample any tangible things . . . in the possession, custody, or control of the party upon whom the request is served." *Rule 4:9(a)*. Thus **HN5** under *Rule 4:9*, the court has the power to require Plaintiff to produce his actual hard drives so Defendant can "inspect and copy" the writings, photographs, or data compilations stored therein. Because the court is vested with the greater authority to force a party to produce documents, photographs, information, and data compilation which would

otherwise be protected by § 18.2-152.5, the court is vested with the constituent power to grant "authority" to a party to access said documents, photographs, information, and data compilation already in the requesting party's possession or control. The circuit courts may, pursuant to the powers governing discovery, grant "authority" for parties to access information otherwise protected by Va. Code § 18.2-152.5.⁶

Part III - Fifth Amendment Protection of Personal Computer Files

The United States Supreme Court in *Boyd v. United States*, 116 U.S. 616, 633, 6 S. Ct. 524, 29 L. Ed. 746 (1886), was "unable to perceive [how] the seizure of a man's private books and papers to be used in evidence against him is substantially different from compelling him to be a witness against himself." *Id.* Though dicta,⁷ this pronouncement of the *Fifth Amendment's* content-based protection of personal papers, writings, documents, and books precluded the use in evidence of personally prepared materials for nearly a century. In 1976 the Court limited *Boyd's* sweeping protection of personal papers from use against an individual in *Fisher v. United States*, 425 U.S. 391, 96 S. Ct. 1569, 48 L. Ed. 2d 39 (1976), holding that when "the preparation of all the papers sought . . . was wholly voluntary, . . . the [preparation] cannot be said to contain compelled testimonial evidence." 425 [****99**] U.S. at 409-10.⁸ The *Fisher* Court held, the "proposition that [****11**] the *Fifth Amendment* protects private information obtained without compelling self-incriminating testimony is contrary to the clear statements of this Court that under appropriate safeguards private incriminating statements of an accused may be overheard and used in evidence, if they are not compelled at the time they were uttered." *Fisher*, 425 U.S. at 400. Under the United States Supreme Court's present *Fifth Amendment* jurisprudence, **HN6** personal documents are not protected by the *Fifth Amendment* simply because they are personal in nature and the individual asserts a general privacy interest in keeping their contents private. *Fisher*, 425 U.S. at 401. "We cannot cut the *Fifth*

⁵ *Rule 4:10* even allows the court to grant civil litigants access to another party's blood and bodily fluids, the extraction [****10**] of which would be tortious and criminal otherwise.

⁶ The court notes that *Rule 4:9* limits inspection and copying to "designated" documents. Accordingly, *Rule 4:9* does not allow a party to access computer files *carte blanche*. See, Part IV, *supra*.

⁷ The writings and papers obtained in *Boyd* were import invoices required to be kept by federal law, not personal letters, diaries, or correspondences.

⁸ See also, 35 Geo.L.J. Ann. Rev. Crim. Proc. 465, 591-98 (2006).

Amendment completely loose from the moorings of its language, and make it serve as a general protector of privacy - a word not mentioned in its text and a concept directly addressed in the Fourth Amendment. We adhere to the view that the Fifth Amendment protects against 'compelled self-incrimination, not the disclosure of private information.'" Fisher, 425 U.S. at 401 (citing United States v. Nobles, 422 U.S. 225, 233 n.7, 95 S. Ct. 2160, 45 L. Ed. 2d 141 (1975)). Thus, an individual's Fifth Amendment protection from self-incrimination is not implicated [**12] when private papers, writings, documents, and books are prepared without compulsion and are later used to incriminate the individual. Fisher, 425 U.S. at 400-01, 409-10.⁹ This court is also guided by the Virginia Court of Appeals' analysis of Fifth Amendment jurisprudence contained in Moyer v. Commonwealth, 33 Va. App. 8, 531 S.E.2d 580 (2000).

Compulsion sufficient to trigger protection by the Fifth Amendment must be governmental compulsion because the protection is a limitation on the federal government's power and Commonwealth's power by virtue of the Fourteenth Amendment, Malloy v. Hogan, 378 U.S. 1, 6, 84 S. Ct. 1489, 12 L. Ed. 2d 653 (1968)("We hold today that the Fifth Amendment's exception from compulsory self-incrimination is also protected by the Fourteenth Amendment against abridgment by the States.")

[**100] Plaintiff was not compelled to write or send e-mail messages regarding the possession, distribution, or production of child pornography. Nor was Plaintiff under a governmental compulsion to voluntarily view pornographic images of children on his computer. No compulsion is present regardless of whether Plaintiff voluntarily viewed such images as an attachment to a

"received" e-mail or if he voluntarily viewed such images on an internet web page.¹⁰ Accordingly, **HN7** the voluntary writing or receiving of e-mail messages, and the voluntary viewing of any image--either as an e-mail attachment or as an image on an internet web page containing pornographic images of children--is not "compelled" as this terms relates to the [**14] Fifth Amendment's privilege against self-incrimination.

As [**15] noted above, Fifth Amendment "compulsion" can be present when the *production* of requested documents "compels the holder of the document to perform an act that may have testimonial aspects and an incriminating effect." United States v. Doe, 465 U.S. 605, 610, 104 S. Ct. 1237, 79 L. Ed. 2d 552 (1984). Defendant seeks a court order allowing a third party to open files already in Defendant's custody and possession. None of Sensei's applications will require Plaintiff to produce any document, nor perform any act. Accordingly, the issuance of a court order granting Defendant and Sensei "authority" to access Plaintiff's password protected files does not require Plaintiff to perform a testimonial act and thus is not barred by Plaintiff's assertion of a Fifth Amendment right.

Part IV -- Scope

Plaintiff argues, and the court acknowledges, that unfettered access to Plaintiff's computer files would be improper. Rule 4:1(b)(1) states that [**101] **HN8** "[p]arties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action, whether it relates to the claim or defense of the party seeking discovery or to the claim or defense of any other party." Though the Fifth Amendment does not [**16] provide a bar to Defendant's

⁹ The Fisher Court noted, 425 U.S. at 410 n.11, and the Court in United States v. Doe, 465 U.S. 605, 613, 104 S. Ct. 1237, 79 L. Ed. 2d 552 (1984), held that "the act of producing the document may be" privileged under the Fifth Amendment. The Fifth Amendment is implication if a "government subpoena compels the holder of the document to perform an act that may have testimonial aspects and an incriminating effect. As we noted in Fisher: 'Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena.'" Doe, 465 U.S. at 610 [**13] (citing Fisher, 425 U.S. at 410 n.11).

¹⁰ The court notes that pornographic images of children can be saved to a computers hard drive without the user's knowledge. See, Kromer v. Commonwealth, 45 Va. App. 812, 817, 613 S.E.2d 871 (2005). This issue is pertinent in the Commonwealth's prosecution under Va. Code § 18.2-374.1:1, which prohibits the "knowing[] possess[ion of] sexually explicit visual material utilizing or having as a subject a person less than 18 years." In Kromer, the Court of Appeals held that the defendant must knowingly, not constructively, possess the prohibited materials. Kromer, 45 Va. App. at 816. The court stated that possession was voluntary where an individual "intentionally sought out and viewed child pornography knowing that the images would be saved on his computer, and . . . continued to view child pornography knowing that the pornography was being saved, if only temporarily, on his computer . . . [because] he knew his browser cached the image files each time he intentionally sought out and viewed child pornography with his Web browser." Kromer, 45 Va. App. at 816-17 (citing United States v. Tucker, 305 F.3d 1193, 1205 (10th Cir. 2002)(punctuation omitted)).

discovery of personal e-mail correspondence, documents, and images contained on a copy of Plaintiff's hard drives, *HN9* the court may restrict discovery if the court determines that the request "is unduly burdensome." Rule 4:1(b)(1). The court finds that any order granting Defendant "authority" under Va. Code § 18.2-152.5 entails a high probability that immensely personal information will be discovered because of the breadth of information stored on the "imaged" hard drives. Accordingly, the court must balance Defendant's right under the discovery rules to obtain the information against Plaintiff's privacy interests.

On the facts in this case, Defendant should be able to obtain e-mail messages regarding (1) whether Plaintiff is the individual in the already obtained pictures performing sexual acts on other men; (2) the identity of the other individual in the pictures; (3) whether Plaintiff has committed adultery, sodomy and/or buggery. This third category includes the discovery of additional photographs stored on the "imaged" hard drive, other than those already discovered by Defendant, of Plaintiff engaged in adultery, sodomy and/or buggery. As discussed in *[**17]* Part III above, Plaintiff does not have a Fifth Amendment right to bar a court order granting the discovery of information pertaining to these categories simply because the inspection of the "imaged" hard drives could reveal incriminating evidence of Plaintiff's possessing child pornography. Nor can the discovery be barred by Plaintiff's assertion of a Fifth Amendment privilege regarding the potential

discovery of evidence incriminating Plaintiff of adultery, sodomy, and/or buggery because such protection has been waived.

Part V -- Conclusion

The court grants authority for Defendant and Sensei Enterprises, Inc. to access the full contents of the "imaged" hard drives currently in Defendant's possession. Sensei is instructed to replicate all password protected e-mail files on the "imaged" hard drives and deliver the copies to Plaintiff's counsel. Sensei shall only make copies of such files and shall not inspect or review the files. Sensei shall have twenty-one (21) days from the date of this order to copy the files. Defendant bears Sensei's costs of copying the files and providing them to Plaintiff's counsel. Upon Sensei's tendering the files, Plaintiff shall review and mark all files *[**18]* which are responsive to the three categories stated in Part *[*102]* IV. Plaintiff shall identify responsive documents and provide Defendant with an opportunity to inspect and copy the responsive documents, pursuant to Rule 4:9, within thirty (30) days after Plaintiff receives the files from Sensei. Plaintiff's identification of responsive documents/files and Defendant review of such documents/files shall proceed as if Defendant's discovery request was made pursuant to a request for the production of documents under Rule 4:1(a).¹¹

Kathleen H. MacKay

¹¹ Plaintiff should not mark as responsive files or documents which are protected by the attorney client privilege or other applicable privilege.

Computer Crime and Trade Secrets

WHEN COMPUTER CRIME IS INVOLVED IN THE THEFT OF TRADE SECRETS

Computer Crime and Trade Secrets

Example One

- Acme Company fires product demonstrator Wile E. Coyote for alleged safety violations
- Wile E. Coyote gains new employment with Beta Company
- Wile E. Coyote uses a computer program to remotely access his old work computer at Acme Company through the internet, and downloads secret Acme Client lists and other trade secrets
- Wile E. Coyote shares these trade secrets with his new employer Beta Company

Computer Crimes and Trade Secrets Example

- ▶ Acme Sues Wile E. Coyote and Beta Company under Virginia Computer Crime Act
- ▶ Computer Crime act allows for private cause of action for civil damages
- ▶ Acme alleges that Wile E. Coyote AND Beta Company, with malicious intent, used a computer to make unauthorized copies of data on Acme's Computer network
- ▶ Acme also alleges violation of Uniform Trade Secrets Act, for unjustly enriching themselves by improperly obtaining and disclosing Acme trade secrets

Computer Crime and Trade Secrets Example

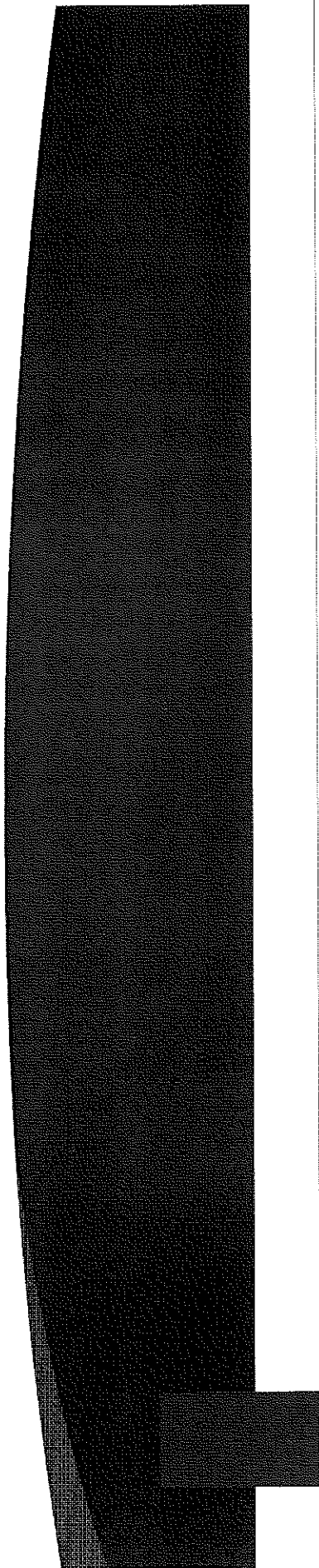
- ▶ Atlantic Marine Construction, Inc. v. McGrath and C&C Contractors, LLC
- ▶ Filed in United States District Court, Eastern District of Virginia
- ▶ Filed in Norfolk, November 2015
- ▶ Alleges violations of State and Federal Computer Crimes and Trade Secrets Statutes
- ▶ Alleges defendant used Google remote office program installed on his old work computer to access files without permission and share trade secrets with new employer.

Computer Crime and Trade Secrets Hypothetical One

- ▶ Beta Corporation gains a client's password for Acme Company and uses the password to enter Acme's computer system and copies work manuals, software, information and data
- ▶ Acme Discovers this and files a lawsuit in Virginia State Court, alleging violations of the Computer Crime Act and the Uniform Trade Secrets Act
- ▶ Beta files to remove to Federal Court and argues that all of this information that they allegedly copied is copyright protectable material and therefore Acme's Computer Crime Act claim is pre-empted by federal copyright law
- ▶ Acme Claims that the Computer Crime Act requires a trespass that is separate from federal copyright claims

Computer Crime and Trade Secrets Hypothetical

- ▶ MAXIENT, LLC v. Symplicity Corp., 63 F. Supp. 3d 592 - Dist. Court, ED Virginia 2014
- ▶ Symplicity discovered their former clients were using the same passcode they had with Symplicity to log on to MAXIENT web site, broke in and copied Maxient Data and programs
- ▶ Symplicity claimed this was a copyright violation, not a computer crime violation
- ▶ Court used a "... two-prong inquiry to determine when a state law claim is preempted: first, the work must be within the scope of the `subject-matter of copyright` as specified in 17 U.S.C. §§ 102, 103, and second, the rights granted under state law must be equivalent to any exclusive rights within the scope of federal copyright as set out in 17 U.S.C. § 106."

- 
- ▶ Court holds that Computer Crime Act Claim for copying software with “malicious intent” was within the exclusive rights of federal copyright law and preempted
 - ▶ BUT claims under Computer Crime Act that BETA acted “with False Pretenses” and “used encryption” to gain data not part of federal copyright law and those claims would be remanded back to state court to be heard with violation of trade secrets claim