State Bar of Michigan

Michigan IT Lawyer

A Publication of the State Bar of Michigan Information Technology Law Section

http://www.michbar.org/it

Table of Contents

May 2013 ▪ Vol. 30, Issue 3

Michigan IT Lawyer is published every other month. Previously published issues of the *Michigan IT Lawyer*, and its predecessor the *Michigan Computer Lawyer*, are available at http://www.michbar.org/it/newsletters.cfm. If you have an article you would like considered for publication, send a copy to:

Michael Gallo
2700 Renshaw Drive
Troy, Michigan 48085
e-mail: michael@gallo.us.com

Bits and Bytes from the Section

By Karl A. Hochkammer, *Honigman Miller Schwartz & Cohn LLP*

I would like to provide a summary of the upcoming events for the IT Law Section, and information about the recently established Privacy Law Committee.

One of the Section's main goals for this year is to increase the level of engagement with Section members. We are increasing the use of the LinkedIn group '*IT Law Section of State Bar of Michigan*', http://www.linkedin.com/groups?home=&gid=2993995&trk=anet_ug_hm, providing event information, news, and a forum for Section members to communicate with each other. Susanna Brennan graciously agreed to help make this resource of greater interest and use to members. For those who are not yet members of the Section's LinkedIn group, please join and use this resource to share articles of legal interest, notice of educational or networking events and career opportunities, or to communicate with other Section members.

The IT Law Section is proud to announce the formation of the *Privacy Law Committee*. The *Privacy Law Committee* is a forum for discussing this new and developing area of the law, which affects a broad range of practices at the state, national and international levels. The committee will work to educate State Bar members about the privacy and security obligations of their organizations, and those of their clients.

Whether you are in-house counsel, a member of a firm, or a solo practitioner, if you are interested in any of the following areas, you may benefit from becoming a member of *the Privacy Law Committee*:

- Advertising and Marketing Law
- Corporate Governance
- Employment Law
- Financial Services Law

Continued on next page

Bits and Bytes . . .

Continued from page 1

- Healthcare Law
- IT Law
- International Litigation
- Mergers & Acquisitions (Domestic or International)

Membership in the Privacy Law Committee is free, and is open to all members of the SBM IT Law Section. If interested in learning more, please email one of the Co-Chairs listed. An 'I want to join' message is sufficient.

- Bob Rothman, Co-Chair, Privacy Law Committee (rrothman@privassoc.com)
- Keith Cheresko, Co-Chair, Privacy Law Committee (kcheresko@privassoc.com)

This is a great opportunity to become involved in what is quickly developing into the next new legal specialty!

The Council is always seeking people who would like to increase their involvement with the Section – we welcome those who would like to assist with event planning, the annual IT law seminar, the newsletter, and the *Edward F Langs Writing Award*. If interested in volunteering, please contact any Council member, who will be happy to put you in touch with the correct person.

Our last Section meeting occurred on Thursday, January 31, 2012 at Sweet Lorraine's in Berkley. Brian Wassom, a partner at Honigman, presented on the legal issues relating to augmented reality – digital data superimposed on the physical world. This is an interesting and quickly evolving area in which traditional legal concepts are being applied in unique ways. Brian regularly blogs about these issues (and issues relating to social media) at http://www.wassom.com.

The Section is tentatively planning to hold a meeting in early June and, of course, the annual meeting and IT Law Seminar at St. John's in Plymouth in late September. Please watch for email messages from the Section for further details. If you have suggestions for meeting locations, or are willing to present on a topic of interest, please let a Council member know.

I look forward to seeing all of you at a meeting soon. As always, feel free to contact me with any questions that you may have regarding the IT Law Section.

Karl A. Hochkammer

2012-2013 Section Chair

The *Michigan IT Lawyer* is pleased to present "Wanderlust—The 'Curious Exploration' Partial-Access Problems in Campus Local Area Networks" by Matthias J. Kaseorg, a winner of the 2012 Edward F. Langs Writing Award competition, and a Juris Doctor candidate at Washington and Lee University School of Law.

The statements made and opinions expressed in this essay are strictly those of the author, and not the State Bar of Michigan or the Information Technology Law Section. Comments regarding this article can be forwarded to the *Michigan IT Lawyer,* care of *michael@gallo.us.com*. Enjoy!

Wanderlust - The "Curious Exploration" Partial-Access Problems in Campus Local Area Networks

By Matthias J. Kaseorg [1]

"The man who trades freedom for security does not deserve nor will he ever receive either."

—Benjamin Franklin

Matthias J. Kaseorg

I. Introduction

Online campus networking is an essential tool for institutions of higher learning. Most institutions offer students the ability to access both the Internet and a campus local area network (LAN).[2] A standard campus LAN essentially operates as a series of nodes. Users connect their laptops and other electronic devices to access points such as wireless routers or switches. The access point then routes the network traffic to a central server or series of servers, which host network resources and also permit users' electronic devices to access the Internet. A LAN therefore allows students to access both the Internet and campus-wide resources such as personal storage, class handouts, and shared folders. LANs are integral tools for students, but pose a number of security challenges as well.

A. LAN Security Issues

The first security challenge comes with initial student access to the LAN as a whole. Most institutions will issue unique usernames and passwords to students, and require students to install identify-verification software on their computers in order to access the LAN. Thus, if an individual is authorized to access the network, she will have a unique user ID, a password, and will have enabled verification software. Most institutions will not fail to "lock their front door," so to speak. An unauthorized individual will, therefore, only be able to access the network by somehow obtaining and using an authorized student's identification credentials. It is entirely implausible to suggest that this type of unauthorized access could occur incidentally or accidentally. Thus, any initial network access by an unauthorized individual can be considered fraudulent—as if the individual had broken down the front door of a building to get in. The proscribable conduct is the initial access itself, rather than any subsequent information gathering.

This Paper focuses on the second security challenge: subsequent student access to specific resources. Once a student has legitimately accessed the LAN through her own credentials, she will purportedly have access to a specific subset of LAN resources. A student should have access to her private folder, but not to other students' private folders. A student should have access to her class's resources, but not other classes' resources. A student should have access to student resources, but not to the same resources that a professor or faculty member may have.

A network administrator may partition access availability in two different ways. First, the network administrator could leave all public, private, and group folders universally accessible but password protected. Then, teachers or group leaders could disseminate the group folder's password to group members. Group access would thus be contingent on having a password. This is technologically the simplest solution, but it requires students to write down or memorize a multitude of different passwords for each subgroup, and can make LAN navigation very cumbersome.

The second, and more common, solution is for the network administrator to partition student access server-side by creating code to block or allow access to different folders based upon the student's username. This way, each student is (ideally) only allowed to see and access folders that the network administrator has authorized for that particular student's username.

However, as with many technological solutions, the computer code used to achieve server-side folder resource partitioning can fail or be improperly executed. The code-based "walls" may not operate as planned and clever students may be able to access folders that they were not supposed to access. If the network administrator did not password protect folders as a failsafe, then these clever students would be able to access non-authorized folders in the same way that they can access their authorized folders. Thus, the legal implications of a student will probably focus on "exceeding authorized access."

B. Scenario and Thesis

This Paper posits the following scenario: Virginia Private University's (hereinafter "V.P.U.") campus LAN has a user-based authorization system, but fails to properly password protect certain campus resources. Thus, Jane Student is able to access her own folders, but can also navigate to other class folders, other student folders, professor materials, and other internal resources that V.P.U. did not intend to authorize student access to. Furthermore, V.P.U. has outlined a typical network use policy that forbids, among other things, accessing other user's data.[3] This Paper asks the question: at what point does Ms. Student's curious exploration of the network become illegal under Federal law and Virginia law? This Paper suggests that Ms. Student will probably be criminally liable under both jurisdictions. This Paper then analyzes whether the current standard is justified, and what can be done to improve it.

II. Current Jurisprudence

A. Computer Fraud and Abuse Act § 1030(a)(2)(C)

Congress passed the Computer Fraud and Abuse Act (CFAA)[4] in 1984 to combat a newly-developing genre of harmful activity—computer crime. Congress most recently amended the CFAA in 2008 by passing the Identify Theft Enforcement and Restitution Act.[5]

The CFAA proscribes a broad range of various computer crimes, from unauthorized access of financial institution computers[6] to installation of damaging computer programs.[7] Only one CFAA section, however, is particularly relevant to this scenario. § 1030(a)(2)(C) of the CFAA forbids intentional access to any computer if (1) the user lacks or exceeds her authorization, and (2) the user obtains information (3) from a "protected computer."[8]

1. Lacks or Exceeds Authorization

The CFAA explicitly states that a user "exceeds authorization" when she (1) has proper authorization but (2) uses that authorization to "obtain or alter" computer information that she was not entitled to.[9] The main debate over "authorization" centers on whether a network owner may define authorization by contract, or whether the defendant must take some objectively "unauthorized" action against the network such as breaking through a code-based restriction.[10] There is currently a circuit split on this issue between the Ninth Circuit and the rest of the circuit courts.

In *United States v. Rodriguez*, the Eleventh Circuit held a Social Security Administration worker criminally liable under § 1030(a)(2)(C) for using his work access during work hours to run background checks on women from his church group.[11] The court found that Mr. Rodriguez was "exceed[ing] authorization" because he used his work access in violation of his workplace's computer use policy.[12] Mr. Rodriguez is not the most sympathetic defendant. He used information and addresses that he obtained from unauthorized background checks to mail flowers, send letters, and even show up unannounced at one woman's house.[13] Mr. Rodriguez should probably face a bevy of stalking charges and court-ordered restraining orders. But I am not convinced that Mr. Rodriguez should be considered a criminal computer hacker simply because he defied his boss's orders. After all, Mr. Rodriguez could have probably obtained the same information through other perfectly legitimate methods: by hiring a private investigator, using background check software such as Intelius,[14] or doing an in-depth Google search.

Similarly, in *United States v. Teague*, the Eighth Circuit held a debt-collection worker criminally liable under § 1030(a)(2)(C) for looking up Barrack Obama's student loan information via her Department of Education network access.[15] The government's computer-use policy only permitted Ms. Teague to look up student loan information pursuant to work-related purposes.[16]

On the other hand, the Ninth Circuit recently held in *United States v. Nosal* that an individual cannot "exceed authorization" merely by using a computer in violation of a contractual computer-use policy.[17] The Ninth Circuit stopped short of reserving liability for offenders who break code-based restrictions, although Judge Kozinski suggested that

the CFAA was intended to prevent "the circumvention of technological access barriers—not misappropriation of trade secrets."[18] The court instead held that the defendant, to be liable under the CFAA, must violate a policy restricting access to a specific subset of information, rather than a policy merely restricting how the accessed information is used.[19]

Other circuits may adopt the Ninth Circuit's test in the future. For now, however, the majority view is that contract-based restrictions, via computer use policies, can define when a defendant lacks or exceeds her authorization.[20]

2. "Obtains Information"

The CFAA merely requires that an individual obtain "information" in order to be liable, and does not specify the nature of that information. As we saw in *Rodriguez* and *Teague*, basic information such as names, addresses, birth dates, or financial information will certainly suffice, even if the information is commercially available.[21]

3. Obtains Information from a "Protected Computer"

The CFAA also explicitly, albeit broadly, defines the term "protected computer" as including any computer affecting interstate or foreign commerce.[22] Campus computers will likely meet this prong for several reasons. First, the servers used to host LAN resources are often also used to host the university's web site, which is accessible from many different states and will often offer a variety of goods, services, and information. Second, the campus LAN allows an outbound connection from campus computers to the global Internet. Third, through use of a virtual private network or proxy access, students from many different states can access the internal campus LAN from their homes or elsewhere.

4. Mens Rea

Courts imposed a relatively low mens rea requirement for criminal liability under the CFAA. The defendant need only intend to obtain unauthorized access of a protected computer to be liable under § 1030(a)(2)(C).[23] Furthermore, to be liable, the defendant need not intend to use the obtained information for any particular purpose.[24]

B. Virginia Statute: Virginia Computer Crimes Act and Associated Jurisprudence

Federal law may be applicable in Ms. Student's case. However, the primary battleground for computer access crimes is within state computer crime statutes. Virginia has a broad range of specific computer crimes on the books—namely within the Virginia Computer Crimes Act (VCCA). A select few statutory sections may be realistically applicable in Ms. Student's case.

Virginia lumps both "without authorization" and "exceeds authorization" into one category—"without authority." A user is without authority when she knows or should know that she is either acting without permission or exceeding the bounds of permitted conduct.[25] There are two potential ways by which courts judge a user to be "without authority." The first method would be to identify when the user subverts some form of code-based restriction—the electronic version of breaking-and-entering. The second method would be to identify when the user breaks some sort of contractual terms-of-use policy set by the network owner. Virginia courts suggest that the latter standard is sufficient,[26] and have further outlined that the bounds of "permitted conduct" is usually defined by the owner, but can also be granted by court order in some scenarios.[27]

Virginia creates a civil cause of action as well for individuals harmed by any of the listed actions if the defendant causes some sort of measurable damage.[28] Virginia case law suggests that the "any damages" standard is a fairly low one, and mere unauthorized use-of-service can potentially cause legally-actionable "damage."[29]

1. Computer Fraud [CF]

To be liable for computer fraud under Virginia Code § 18.2-152.3(1), our putative defendant, Ms. Student, must meet four conditions: the defendant must (1) use a computer (2) without authority (3) to obtain services (4) by false pretenses.[30]

Virginia's computer-fraud statute has been partially overturned as unconstitutional when it grants a cause of action that interferes in the realm of federal copyright laws.[31] However, the remaining portions are still applicable to other causes of action, and Ms. Student's conduct does not implicate copyright concerns, thus the statute may still apply.

Virginia courts do not require the obtained service to be publically available or have a defined market "value" in order to fall within the purview of the Virginia computer-fraud statute. The Virginia Eastern District court, in *Physicians Interactive v. Lathian Sys., Inc.*, held that the Virginia computer-fraud statute defends a web host's property rights in its internal data.[32] The *Lathian* court further held that a user may not hack this internal data even if the web host grants the user partial authorization to visit the website.[33] In *Am. Online, Inc. v. LCGM, Inc.*, the Virginia Eastern District court found a defendant liable under § 18.2-152.3(1) for sending spam e-mails through AOL's e-mail service that falsely identified AOL as the sender.[34]

There is partial tension within Virginia law as to what constitutes obtaining services by "false pretenses." In *Barnes v. Com.*, the Virginia Court of Appeals held that unauthorized access to DMV database to check VIN of a stolen truck in order to retain the stolen truck constituted "obtain[ing] services by false pretenses," and was therefore a violation of § 18.2-152.3.[35] But the Virginia Eastern District court later decided in *Global Policy Partners, LLC v. Yessin*, without overturning *Barnes*, that unauthorized use of a computer network to access e-mails between wife and lawyer to gain an advantage in a divorce proceeding was not.[36]

2. Computer Invasion of Privacy [CIP]

To be liable for computer invasion of privacy under Virginia Code § 18.2-152.5(A), Ms. Student must meet five conditions: the defendant must (1) use a computer or computer network (2) without authority, and (3) intentionally examine (4) financial or identifying information as defined in § 18.2-186.3, (5) after she knows or should know that she is without authority to view that information.[37] The statute also offers a potential safe-harbor for diagnostics.[38]

In *Plasters v. Commonwealth of Virginia*, the Virginia Court of Appeals held a police dispatcher criminally liable for Computer Invasion of Privacy for running criminal background checks outside of a formal request (in violation of her job's computer policy).[39] The defendant in *Plasters*, as we also saw with *Rodriguez*, probably could have obtained the criminal background information by hiring a personal investigator, putting in a formal request, or using online tools such as Intelius.

Virginia defines "identifying information" by statute as including simple things such as names or dates of birth, as well as more complex things such as computer passwords.[40]

3. Theft of Computer Services [TCS]

To be liable for theft of computer services under Virginia Code § 18.2-152.6, Ms. Student must meet three conditions: the defendant must (1) willfully (2) obtain computer services (3) without authorization.[41] If the obtained services were worth above $2,500, the statute makes the offense a felony.[42]

The Fourth Circuit court in *A.V. ex rel. Vanderhye v. iParadigms, LLC* held that a high school student could potentially be liable for theft of computer services under § 18.2-152.6 when he falsely used another college's password to submit a paper a plagiarism-detection service named Turnitin required by his high school.[43] The *iParadigms* court held that a defendant need not have caused actual damage in order to be liable; consequential damages are sufficient, at least for civil liability.[44]

C. When is Access Illegal for Ms. Student

1. CFAA § 1030(c)(3)

Ms. Student potentially crosses her first legal line when she first accesses a folder on the network that doesn't belong to her. At this point, she may be liable under § 1030(c)(3) of the CFAA. Ms. Student is clearly using a computer. And, as previously noted, the campus network that she is accessing will probably be considered a "protected computer."[45] Thus, the only real issue at play here is whether Ms. Student is "exceeding authorized access."

Ms. Student has authorization to be on the network, but is using that authorization to obtain user data that she was not entitled to obtain. I should note that even the heightened requirement for "exceeds authorized access" that Judge Kozinski outlined in *Nosal* will not save Ms. Student from federal liability under the status quo. Our theoretical network use policy forbids Ms. Student, by contract, from accessing other user data. This is a direct restriction on student access to information, not merely what they do with that information, which satisfies the *Nosal* standard.

2. Computer Fraud

Ms. Student may also potentially be liable under the Virginia CF statute for fraudulently obtaining computer services. Ms. Student is clearly using a computer. As previously noted, the Virginia standard for "without authority" includes violating a network use policy.[46] The court would, thus, likely find Ms. Student to be "without authority."

In both *Lathian* and *Barnes*, the court held defendants liable for obtaining computer "services" in the form of access to information. In both cases, the information was not commercially available.[47] Thus, it seems that a court could at least conceivably find that Ms. Student obtained computer services in some loose sense of the word.

Ms. Student will not likely meet the final "false pretenses" requirement. Ms. Student's actions do not even rise to same level as the *Yessin* defendant's, which the court found insufficient for the "false pretenses" requirement. At the very least, Ms. Student is certainly not attempting to further some sort of fraud like the car theft in *Barnes*.

3. Computer Invasion of Privacy

Ms. Student may be liable under the Virginia CIP statute, depending on what type of files she accesses. The Virginia CIP statute does not require "fraud" on the part of the user, but it does require access to the specific subset of financial or identifying information. Thus, if Ms. Student came across

a file containing some sort of student financial information, password list, or other identifying information, she may be liable if she continued to dig through the file after realizing its nature. By the strict language of the statute, something as simple as a student resume containing the student's name and address may qualify as identifying information.[48] As we saw in *Plasters*, the fact that the information may be available from other sources does not matter.[49]

4. Theft of Computer Services

Ms. Student might be liable under the Virginia TCS (Theft of Computer Services) statute. Taken separately, Ms. Student has arguably met all three statutory requirements. She acted willfully, arguably obtained the service of network usage, and was acting without authority. However, Ms. Student arguably did not "obtain" anything, let alone a "service." Ms. Student was already authorized to access the "services" of Internet connectivity and campus resource access. The network owner did not intend access to other folders to be a separate "service", nor did Ms. Student's access cause any appreciable damage, nor did Ms. Student garner any measurable value by browsing other user folders. Virginia courts have not specifically defined the nature of the "service" that the defendant must obtain to be criminally liable.

However, case law construing § 1030(a)(4) of the CFAA, which similarly requires that the defendant obtain something "of value" to be liable,[50] suggests that Ms. Student may escape liability. In *United States v. Czubinski*, the First Circuit held that the defendant did not obtain "anything of value" by browsing unauthorized tax returns.[51] The *Czubinski* court further held that the defendant did not obtain something of value merely by "satisfy[ing] idle curiosity." In our case, if Ms. Student does nothing more than browse unauthorized portions of the network for her own idle amusement, a court will probably not find her criminally liable under the Virginia TCS statute.

III. Analysis and Critique

A. When Should Access Be Illegal

1. Essence of Crime

Let's stop and think for a moment about what the "essence" of an unauthorized access crime should be. The outcome of actual data being accessed, lost, or taken should not be enough to justify criminal liability. We make distinctions in the law all the time between doing something that you agreed not to do, and actually breaking some "barrier" to achieve the same thing. Take the example of a contract: if I agree to buy widgets from you at a five thousand dollar profit, and then willfully breach the contract, I may be liable to make you whole for what you would have gotten from the contract, but I won't be criminally liable. However, if I complete the contract, and then I go to your house and steal back the five thousand dollars that I paid you in profits, I will be criminally liable.

Why is the second scenario different? In both cases, you lose out on five thousand dollars, and you have a legal right to recover those five thousand dollars from me. However, by breaking into your house, I have actively threatened the security of your home and person in a way that I never could by merely breaking a contract. After all, anyone can renege on their promises—in many cases for perfectly legitimate reasons. It takes a higher level of time, effort, skill, and deviance to break down the barrier into someone's home. This is why there is a fundamentally different standard for addressing the individual who walks across a lawn with a sign that says "please keep off the grass"[52] and the individual who picks a lock to enter a building.[53]

2. Confusing Combination of Elements

The current standard criminally punishes conduct that, broken down into its independent elements, would not be considered criminal. If our student had merely accessed unauthorized portions of the network, without really viewing anything, obtaining anything, or causing network traffic, she wouldn't be criminally liable. If our student had been in a study room and stumbled across a file folder lying open on the ground containing student infornation, she would not be criminally liable if she didn't intend to use the information to defraud the person. But the fact that the file folder happens to be contained on a computer suddenly makes accessing it a crime prosecutable by jail time?

3. Who Should Be Able To Define Crime?

Under the current standard, network owners can essentially define the scope of criminal law through contract. In the website context, courts have scoffed at the notion that a terms-of-service policy should be able to define the contours of criminal law.[54] Why should we not apply the same reasoning to network access as well?

Criminal law must be predictable and objective.[55] Terms of use contracts are neither predictable nor objectively defined. Defining criminal law based on what is contained within a network use contract requires users to carefully read and predict how courts may respond to various terms within the contract. Unfortunately, most Americans are not law-school-educated contract lawyers.[56] Furthermore, network owners should not be permitted to be mini-dictators over

their LAN kingdoms. Criminal law should be defined by the government.

B. How Should the VCCA Be Reformed?

I propose reforming the VCCA by requiring, in a criminal case, the prosecution to show that a defendant willfully subverted some sort of signal-bearing code-based protection before she may be held liable.[57] This solution consists of four discrete elements: (1) bifurcating the civil and criminal standards, (2) bifurcating the concepts of "lacks" and "exceeds" authorization, (3) modifying the definition of "lacks authorization" to encompass only instances where a defendant subverts some code-based restriction, and (4) crafting a coherent definition of what constitutes adequate notice of a code-based restriction.

1. Bifurcate Civil and Criminal Standards

First, Virginia must bifurcate the civil and criminal standards. The status quo forces judges to spin a confusing web of case law applying identical statutes within trials that have differing procedural rules, evidentiary standards, and potential damages. Furthermore, the goals of civil and criminal liability are vastly different. Civil law aims to make a victim who has suffered some sort of tangible harm whole for the actions, blatant or not, of the tortfeasor.[58] Criminal law, on the other hand, seeks to punish wrongdoers for their wrongful actions, and serve as a deterrent for future would-be wrongdoers.[59]

2. Bifurcate "Exceeds Authority" and "Lacks Authority"

Second, Virginia must distinguish "exceeds authority" from "lacks authority," and allow criminal liability only for the latter. As previously noted, there is a fundamental difference between breaking a contract and breaking down some barrier that an individual relied upon for protection.[60]

3. Require Breaking a Signal-Bearing Code-Based Restriction

Third, Virginia must abandon the idea that a user may "lack authority" if she is outside of a contract-based restriction. Virginia must instead redefine "lacks authority" as circumventing some sort of code-based restriction. This standard should be justified based on the kind of "locks" the user must break in order to obtain access. The law should make a bright-line determination that a user "lacks authority" only when he or she subverts some well-marked code-based protection, such as a password-protected login screen or a software-based security certificate. This new requirement puts the impetus on the hosting party to clearly delineate which access is authorized and which is not.

4. Carefully Define a Signal-Bearing Code-Based Restriction

A code-based restriction must serve two functions in order to effectively define the network areas that a user "lacks authorization" to access. First, the code-based restriction must serve a "signaling" function by adequately notifying the user that she is accessing protected material. The network owner can presumptively give the user notice through use of some statutorily defined symbol, akin to the © signal for copyrights or ™ signal for trademarks. To simplify matters, a regulatory body can publish a safe harbor list of code-based restrictions that automatically put the user on notice absent a signal, such as a password-protected login screen. Second, the code-based restriction must create some sort of technological access barrier and require some unique information on the user's side in order to login, such as a password, security certificate, or biometric data. A mere "click-though" screen such as a hyperlink should not be enough to qualify, because the only barrier to entry depends on the implicit contractual request by the owner for the user to stay out.

C. Student Liability under the New Standard

Under this standard, Ms. Student will not be criminally liable under the VCCA for her curious exploration of the V.P.U. LAN folders. She has not circumvented any code-based restrictions, and thus does not "lack authorization" under the new standard. At most, she will "exceed her authorization." At worst, she will be civilly liable to the network owner if she causes some sort of damage.[61]

This is not to say that Ms. Student may not be liable under some other criminal statute. For example, if Ms. Student stumbles across student's Social Security Numbers, and then uses those numbers to start fraudulent bank accounts, she will probably be liable for identity theft.[62] Ms. Student may also be liable for theft or be prosecuted under other traditional criminal statutes, regardless of whether she used a computer to facilitate the crime.

D. Benefits

1. Provides a Clear and Objective Standard

This Paper's solution provides users with a clear and objective standard for criminal liability under the VCCA. The new standard provides network users with two different forms of notice that their conduct is improper and potentially criminal. First, network users who stumble across protected content will be presented with universally recognizable symbol, which should put users on notice that they should tread carefully. Second, network users will be

presented with a code-based barrier, which the user cannot circumvent without taking deliberate action.

There are two ways to circumvent a code-based restriction. First, the user could obtain and use an authorized individual's login credentials. However, the user could hardly argue that she was not on notice of doing something wrong when she logged in with a username and password that did not belong to her. Second, a user could actively hack the code in some way. However, hacking a code-based restriction takes a certain amount of time, effort, and skill, which would also put the user on notice that she is probably doing something wrong. Thus, it is reasonable to assume that a user would know when she is circumventing a code-based restriction.

The new standard also shifts the control over what constitutes a criminal violation away from the network owner to the network user, and provides the user with an objective standard to guide her actions. Under the new standard, courts in a criminal action would no longer have to worry about all of the ins and outs of an owner-defined network use policy, but can now identify criminal conduct entirely from the user's actions. The new standard defines criminal conduct by the actual "bad act" of breaking down the network's front door.

2. Treats Conduct Consistently, and Connects Crime with a Social Policy Rationale

As I mentioned earlier, the hallmark of an unauthorized access crime is the defendant's threat to the owner's assumption of security.[63] I suggest we follow the "breaking and entering" model by requiring a defendant to circumvent some "locked door" in order to be criminally liable. A user should not be criminally liable for merely taking advantage of an open system, because the user has not threatened the assumption of security within the campus network.

The new standard is more harmonious with other unauthorized access crimes such as burglary and breaking-and-entering. It supports a coherent policy rationale: disincentivizing individuals who threaten a victim's personal space and force the victim to adopt additional security measures to avoid future security breaches.

The new standard also treats computer contract law consistently with other types of contract law. Contractual breaches of computer use policies should be treated like other contractual breaches—through civil law. If the network owner wants the freedom to carefully define what conduct he desires on his server, then he should be bound by the limitations of the contract law regime. The network owner is not entitled to have the government, by the force of criminal law, to strong-arm network users into complying with the network owner's policy.

3. Distinguishes "Computer Crimes" From "Crimes Committed With a Computer"

The new standard specifically targets the actual security issues involved with computer misuse. The new standard then allows traditional crimes, such as theft, to be consistently punished without reference to the irrelevant fact that a computer happened to be incidentally involved. Under the new standard, judges will also be better able to craft a coherent body of jurisprudence that is specifically tailored to deal with the unique issues that computer crime statutes seek to address.

E. Responses

1. The Deviant Employee Response

What about the employee who uses her network access to browse employee files after her employers have clearly told her that she is not allowed to do so? Surely this individual is a bad person and should be punished. I would tend to agree. But I see no objective difference between the aforementioned scenario and the scenario where a cubicle worker digs through hard-copy personnel files at work. Both types of employees should be fired, and maybe even sued. But they are not criminals. If Virginia wants to make them criminals, then they should enact statutes that treat them equally under the law.

2. The Social Engineering Response

A lot of computer crime today is committed through so-called "social engineering."[64] In a typical social engineering attack, Mr. Hacker will trick his victims into giving him access to personal information such as computer passwords. Then, Mr. Hacker will use his access to steal the unwitting victim's money from the victim's online banking account.

This type of scheme will be consistently punished under both the new standard and other traditional criminal laws. First, Mr. Hacker outright lacks authorization to the computer service. I doubt that any court would consider the unwitting victim to have actually given Mr. Hacker any sort of authorization because of the fraudulent nature by which the password was obtained. If Mr. Hacker instead pretended to be a locksmith and made an unauthorized copy of the victim's house key, he will probably still be liable for breaking and entering if he used that key to later enter the victim's house. Thus, Mr. Hacker has no initial authorization to "exceed," and cannot take advantage of the bifurcated VCCA standard.

However, even if Mr. Hacker somehow legitimately gained *authorized* access to the victim's account,[65] Mr. Hacker may still be criminally punished under traditional laws for his theft and will likely also be civilly liable for any loss he caused the owner. In summary, Mr. Hacker is guilty of two separate offenses. First, he is guilty of the initial act of subverting the code-based password protection. Second, he is guilty of the subsequent act of taking money from the victim. The new standard does a better job of separating these two offenses and crafting separate criminal standards to deal with each one.

3. Overwhelming Burden on Private Companies

Doesn't the new standard put a huge burden on private companies to carefully demarcate and protect every file, in fear that employees, students, or other semi-authorized users will be able to unabashedly browse to satisfy their curiosity? First, the burden is not overwhelming. Network owners should be able to use a standard template to incorporate the signal into protected content without significant difficulty. Second, network owners can still rely on contract liability and other criminal law to prevent loss. Third, network owners probably should be password-protecting (or placing other forms of technical barriers on) valuable data anyway.

But what if the network owner intended to place a code-based restriction on data but failed to adequately do so? Shouldn't the fact that he intended to protect the data count for something? If an individual, accidentally or not, leaves a file folder in plain view, he cannot then rely on criminal law to avert prying eyes. The purpose of criminal law is not to enforce the particular whims of any member of society, but to protect against a specifically defined subclass of deviant behavior in a manner that comports with a well-defined public policy rationale.[66]

4. Protect ALL the Data (and Back to Square One)

Won't the new standard simply cause network owners to over-secure their files and slap a symbol on every single page? Doubtful. If a network owner allows for an open network that allows for partial access, the owner usually intends that users have uninhibited access to some data. And any data that the network user doesn't want accessed by all individuals probably should be password protected anyway. Network security is a legitimate and growing concern[67]— one that is woefully under-addressed by network owners.[68] The new standard may require network owners to more aggressively protect sensitive data, and this is probably a good thing.

IV. Conclusion

As our economy has become increasingly globalized and interconnected, computer networking has become even more important, especially within our institutions of higher learning. Consequentially, network security has increasingly become a substantial public policy issue. However, the legislative and judicial responses to computer crime have been over-broad and unpredictable, and have resulted in badly-formed jurisprudence. Partial-access problems are difficult to address, but those in government need to better inform themselves about modern computer technology and cyber-crime issues. A reformed VCCA that separates a criminal standard for network breaches from contractual violations would better address the realities of modern computer networking and cyber-crime. ■

Endnotes

1 Juris Doctor Candidate, Washington and Lee University School of Law Class of 2013.

2 *See generally, What is a LAN*, Indiana University Information Technology Services Knowledge Base (Apr. 20, 2011), http://kb.iu.edu/data/aesx.html (last visited Apr. 16, 2012).

3 *See, e.g.*, Computer and Network Usage Policy, Stanford University (Apr. 13, 2012), http://adminguide.stanford.edu/62.pdf ("Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, passwords or other digital materials belonging to other users, without the specific permission of those other users.") (last visited Apr. 16, 2012).

4 Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2008).

5 *Id.*

6 § 1030(a)(2)(A).

7 § 1030(a)(5)(A).

8 *See* § 1030(a)(2)(C) (proscribing conduct when any individual "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . (C) information from any protected computer").

9 *See* § 1030(e)(6) ("[T]he term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.").

10 We will also see this debate in the state context.

11 United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) cert. denied, 131 S. Ct. 2166, 179 L. Ed. 2d 946 (U.S. 2011).

12 *See id.* ("Rodriguez exceeded his authorized access and violated the Act when he obtained personal information for a nonbusiness reason.").

13 *See id.* at 1261 ("After Fennell returned to her home in Mississippi, she received flowers from Rodriguez on Valentine's Day even though she had not given Rodriguez her address. Rodriguez later arrived at Fennell's doorstep unannounced,

and Fennell was surprised and frightened by his presence.").

14 Intelius, http://www.intelius.com/people-search.html (last visited Apr. 16, 2012).

15 United States v. Teague, 646 F.3d 1119, 1124 (8th Cir. 2011).

16 *Id.* at 1121.

17 United States v. Nosal, 10-10038, 2012 WL 1176119 (9th Cir. 2012) ("Because Nosal's accomplices had permission to access the company database and obtain the information contained within, the government's charges fail to meet the element of 'without authorization, or exceeds authorized access' under 18 U.S.C. § 1030(a)(4).").

18 *See id.* ("This narrower interpretation is also a more sensible reading of the text and legislative history of a statute whose general purpose is to punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets—a subject Congress has dealt with elsewhere.").

19 *See id.* ("Therefore, we hold that "exceeds authorized access" in the CFAA is limited to violations of restrictions on access to information, and not restrictions on its use.").

20 *See id.* ("No other circuit that has considered this statute finds the problems that the majority does.") (Silverman dissent).

21 *Supra* notes 10–12, 14–15 and accompanying text.

22 *See* § 1030(e)(2)(B) (defining "protected computer" as a computer "used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States"). The CFAA also considers certain government and financial institution computers to constitute "protected computers," but that definition is not relevant to this Article. § 1030(e)(2)(A).

23 *See* United States v. Willis, 476 F.3d 1121, 1125 (10th Cir. 2007) ("A plain reading of the statute reveals that the requisite intent to prove a violation of § 1030(a)(2)(C) is not an intent to defraud (as it is under (a)(4)), it is the intent to obtain unauthorized access of a protected computer.")

24 *See id.* ("That is, to prove a violation of (a)(2)(C), the Government . . . need not also prove that the defendant had the intent to defraud in obtaining the information or that the information was used to any particular ends.").

25 Va. Code § 18.2-152.2 (2010) ("A person is 'without authority' when he knows or reasonably should know that he has no right, agreement, or permission or acts in a manner knowingly exceeding such right, agreement, or permission.").

26 *See, e.g.*, Plasters v. Com., 1870-99-3, 2000 WL 827940 (Va. Ct. App. 2000) ("The defendant was using the VCIN computer to access data without authorization and without any request for the information. Each time the defendant accessed VCIN, the terminal displayed the warning that use of any information was limited to criminal justice purposes only.")

27 *See* Albertson v. Albertson, 73 Va. Cir. 94 (2007) ("[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."),

28 Va. Code § 18.2-152.12(A) (2010) ("Any person whose property or person is injured by reason of a violation of any provision of this article or by any act of computer trespass set forth in subdivisions A 1 through A 8 of § 18.2-152.4 regardless of whether such act is committed with malicious intent may sue therefor and recover for any damages sustained and the costs of suit.").

29 *See* A.V. ex rel. Vanderhye v. iParadigms, LLC, 562 F.3d 630, 647 (4th Cir. 2009) (holding that evidence of consequential damages from a high-school student's unauthorized use of a college password to verify his paper on an anti-plagiarism website fell within the "any damages" requirement for a civil cause of action under the VCCA, even though the high school had its own account under the same website).

30 Va. Code § 18.2-152.3(1) (2005).

31 *See* Rosciszewski v. Arete Associates, Inc., 1 F.3d 225, 230 (4th Cir. 1993) ("Therefore, Rosciszewski's cause of action under [Virginia Code § 18.2-152.3] is preempted to the extent that it is based on reproduction of the copyrighted computer program.").

32 *See* Physicians Interactive v. Lathian Sys., Inc., CA 03-1193-A, 2003 WL 23018270 (E.D. Va. Dec. 5, 2003) ("The website invitation to Internet users to visit a website, gather information, and sign up for services is not an invitation for Internet users to hack the website's host computer file server and copy company financial statements or personnel files. No sign need be posted on a website to protect the web host's property rights.").

33 *Id.*

34 *See* Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451 (E.D. Va. 1998). ("[A]s a result, defendants illegitimately obtained the unauthorized service of plaintiff's mail delivery system and obtained free advertising from AOL because AOL, not defendants, bore the costs of sending these messages.").

35 *See* Barnes v. Com., 2693-98-1, 2000 WL 291436 (Va. Ct. App. 2000)

("We cannot say that the trial court was plainly wrong or without evidence to support its finding that Barnes used a computer network without authority in 1992 and in 1996 to help her brother retain the stolen truck.")

36 *See* Global Policy Partners, LLC v. Yessin, 686 F. Supp. 2d 631, 640 (E.D. Va. 2009)

("No such facts are alleged here; the purported access to the computer network was not in order to accomplish the conversion of property, but rather was in order to gain an advantage in divorce proceedings. On these alleged facts, a law prohibiting obtaining, embezzlement, or conversion of property simply does not apply. Accordingly, Mr. Yessin's motion to dismiss must be granted with respect to Count 12.")

37 Va. Code § 18.2-152.5(A) (2005).

38 *See* Va. Code § 18.2-152.5(F) (2005) ("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.").

39 *See* Plasters v. Com., 1870-99-3, 2000 WL 827940 (Va. Ct. App. 2000) ("The defendant was using the VCIN computer to

access data without authorization and without any request for the information. Each time the defendant accessed VCIN, the terminal displayed the warning that use of any information was limited to criminal justice purposes only.")

40 Va. Code § 18.2-186.3(C) (2009).

41 Va. Code § 18.2-152.6 (2005).

42 *Id.*

43 A.V. ex rel. Vanderhye v. iParadigms, LLC, 562 F.3d 630, 647 (4th Cir. 2009)

44 *See id.* ("We conclude that the evidence of consequential damages presented by iParadigms came within the 'any damages' language of the VCCA, and therefore that the district court erroneously granted summary judgment because there was no evidence of 'actual or economic damages.').

45 *Supra* part II.A.3.

46 *Supra* part II.B.

47 In *Barnes*, the defendant obtained internal DMV records. Barnes v. Com., 2693-98-1, 2000 WL 291436 (Va. Ct. App. 2000). In *Lathian*, the defendant obtained internally-hosted user information. Physicians Interactive v. Lathian Sys., Inc., CA 03-1193-A, 2003 WL 23018270 (E.D. Va. Dec. 5, 2003).

48 *Supra* part II.B.2.

49 Plasters v. Com., 1870-99-3, 2000 WL 827940 (Va. Ct. App. 2000).

50 *See* 18 U.S.C. § 1030(a)(4) ("[Whoever] knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer . . . .")

51 *See* United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997) ("[The defendant's] searches of taxpayer return information did not satisfy the statutory requirement that he obtain 'anything of value.' The value of information is relative to one's needs and objectives; here, the government had to show that the information was valuable to Czubinski in light of a fraudulent scheme. The government failed, however, to prove that Czubinski intended anything more than to satisfy idle curiosity.").

52 Which would probably not be considered criminal.

53 Which almost certainly would.

54 *See* United States v. Drew, 259 F.R.D. 449, 465 (C.D. Cal. 2009) ("[B]y utilizing violations of the terms of service as the basis for the section 1030(a)(2)(C) crime, that approach makes the website owner-in essence-the party who ultimately defines the criminal conduct. This will lead to further vagueness problems.")

55 *See generally Theories of Criminal Law*, Stanford Encyclopedia of Philosophy (Apr. 14, 2008), available at http://plato.stanford.edu/entries/criminal-law (last visited Apr. 16, 2012).

56 And even those of us that are current or future contract lawyers tend to become befuddled when presented with terms of use contracts.

57 I refer to this theoretical reformed VCCA as the "new standard," and the status quo as the "old standard."

58 *See generally Theories of Tort Law*, Stanford Encyclopedia of Philosophy (Aug. 26, 2010), available at http://plato.stanford.edu/entries/tort-theories (last visited Apr. 16, 2012).

59 *See generally Theories of Criminal Law*, Stanford Encyclopedia of Philosophy (Apr. 14, 2008), available at http://plato.stanford.edu/entries/criminal-law (last visited Apr. 16, 2012).

60 *Supra* part III.A.1.

61 *Supra* parts II.B–C.

62 *See* Va. Code § 18.2-186.3(B)(2) (2009) ("It shall be unlawful for any person without the authorization or permission of the person who is the subject of the identifying information, with the intent to sell or distribute the information to another to: . . . 2. Obtain money, credit, loans, goods or services through the use of identifying information of such other person;").

63 *Supra* part III.A.1.

64 *See generally* Social Engineering & Cybercrime, PC Tools (Jan. 11, 2011), http://www.pctools.com/security-news/social-engineering-cybercrime (last visited Apr. 16, 2012).

65 If, for example, Mr. Hacker happened to be the victim's actual bank teller.

66 *Supra* part III.D.2.

67 *See* Gene J. Korowski, *Study: Data Loss, Network Vulnerabilities Top Security Issues*, TechNewsWorld (Dec. 29, 2005), http://www.technewsworld.com/story/47833.html (last visited Apr. 16, 2012) ("A new survey indicates that 'catastrophic data loss' and network vulnerabilities are the security issues of greatest concern for computer industry leaders today.").

68 See, e.g., Ellen Messmer, *Hospitals Seeing More Patient Data Breaches*, PCWorld (Apr. 15, 2012), http://www.pcworld.com/article/253827/hospitals_seeing_more_patient_data_breaches.html (last visited Apr. 16, 2012) ("A bi-annual survey of 250 healthcare organizations shows that the percentage experiencing a patient data breach is up. And with the growth in electronic records-keeping, more of those problems are originating from laptops and mobile devices rather than a human slip-up in handling paper documents."); Amber Corrin, *US' intellectual capital is easy prey*, Defense Systems (Apr. 4, 2012), http://defensesystems.com/articles/2012/04/04/fose-cyber-defense-intellectual-property.aspx?admgarea=DS (last visited Apr. 16, 2012) ("Already, the U.S. has lost at least hundreds of billions of dollars to malicious cyber infiltration."); Ellen Messmer, *Survey: Screwing up network changes one of biggest causes for security, management failures*, PC Advisor UK (Apr. 10, 2012), http://www.technewsworld.com/story/47833.html (last visited Apr. 16, 2012) ("Yes, it's internal IT screw-ups caused by unscheduled out-of-process changes to systems that are in place, especially firewalls, that have resulted in either an outage, a data breach or an audit failure, according to 77% of the survey's respondents.").

Privacy Law Committee

The Information Technology (IT) Law Section of the State Bar of Michigan is pleased to announce the formation of the **Privacy Law Committee**. The Privacy Committee is a forum for discussing this new and developing area of the law affecting a broad range of practices at the state, national and international levels. It also works to help educate members of the bar about the privacy and security obligations of both their own organizations and those of their clients.

Who Should Join? Whether you are in-house counsel or a member of a firm, if you are active in any of the following areas, you may benefit from becoming a member of the Privacy Committee:

- Advertising and marketing law
- Corporate governance
- Employment law
- Financial services law
- Healthcare law
- IT law
- International litigation
- Mergers & Acquisitions (domestic or international)

Who is Eligible for Membership? Membership in the Privacy Committee is free of charge and open to all members of the SBM IT Law Section.

How Do I Sign-up? It's easy. Email one of the Co-Chairs at the address listed below and express your interest in participating. An "I want to join" message is sufficient.

Bob Rothman, Co-Chair
rrothman@privassoc.com
Privacy Law Committee

Keith Cheresko, Co-Chair
kcheresko@privassoc.com
Privacy Law Committee

This is a great opportunity to become involved in what is quickly developing into the next new legal specialty. We look forward to your participation!

Information Technology Law Section, State Bar of Michigan Mission Statement

The purposes of the Section are to review, comment upon, and appraise members of the State Bar of Michigan and others of developments in the law relating to information technology, including:

(a.) the protection of intellectual and other proprietary rights;

(b) sale, leasing, distribution, provision, and use of, hardware, software, services, and technology, including computer and data processing equipment, computer software and services, games and gaming, information processing, programming, and computer networks;

(c.) electronic commerce

(d.) electronic implementation of governmental and other non-commercial functions;

(e.) the Internet and other networks; and

(f.) associated contract and tort liabilities, and related civil and criminal legal consequences.

The Information Technology Law Section's bylaws can be viewed by accessing http://www.michbar.org/it/councilinfo.cfm and clicking the 'Bylaws' link.

2013 Edward F. Langs Writing Award

Essay Competition Rules

1. Awards will be given to up to three student essays, which in the opinion of the judges make the most significant contribution to the knowledge and understanding of information technology law. Factors to be taken into consideration include: originality; timeliness of the subject; depth of research; accuracy; readability; and the potential for impact on the law.

2. Essay must be original, deemed to be of publishing quality, and must not have been submitted to any other contest within the previous 12 months.

3. Essay must be typed, double spaced, at least ten pages in length, must contain proper citations listed as either endnotes or footnotes, and must have left, right, top, and bottom margins of one inch.

4. Essay must include the submitter's name, email address, mailing address, telephone number, and school attended.

5. A total of $1,500 in US dollars shall be divided between the award winning essays, and all rights to award winning essays shall become the property of the State Bar of Michigan.

6. The Information Technology Section of the State Bar of Michigan reserves the right to make editorial changes, and to publish award winning essays in the Section's newsletter, the *Michigan IT Lawyer*.

7. Essay must be submitted as a Microsoft Word document, postmarked by June 30, 2013, and emailed to dsyrowik@brookskushman.com.

Publicly Available Websites for IT Lawyers

Following are some publicly available websites relating to varying aspects of information technology law practice. Some of these websites may require payment for certain services. Neither the State Bar of Michigan nor the IT Law Section endorses these websites, the providers of the website, or the goods or services offered in connection therewith. Rather these websites are provided for information purposes only and as possible useful tools for your law practice.

Please provide any feedback or recommendations for additional websites to michael@gallo.us.com.

Legal Sites

- *http://www.justice.gov/dag/iptaskforce* - United States Department of Justice, Intellectual Property Task Force - The Department of Justice Task Force on Intellectual Property is part of a Department-wide initiative to confront the growing number of domestic and international intellectual property (IP) crimes.
- *http://www.whitehouse.gov/omb/intellectualproperty* - Office of the U.S. Intellectual Property Enforcement Coordinator
- *http://www.iprcenter.gov* – National Intellectual Property Rights Coordination Center. As a task force, the IPR Center uses the expertise of its member agencies to share information, develop initiatives, coordinate enforcement actions, and conduct investigations related to IP theft.
- *http://www.unc.edu/~unclng/public-d.htm* - 'When U.S. Works Pass into the Public Domain', a chart by Professor Lolly Gasaway of University of North Carolina
- *http://portal.unesco.org/culture/en/ev.php-URL_ID=14076&URL_DO=DO_TOPIC&URL_SECTION=201.html* – United Nations Educational, Scientific and Cultural Organizations – Collection of National Copyright Laws ■