Washington Journal of Law, Technology & Arts

Volume 10 | Issue 3 Article 4

1-1-2015

The Code-Based Interpretation of Authorization: An Incomplete Picture

Nicholas R. Ulrich

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 10, ISSUE 3 WINTER 2015

THE CODE-BASED INTERPRETATION OF AUTHORIZATION: AN INCOMPLETE PICTURE

Nicholas R. Ulrich[*]

Cite as: 10 Wash. J.L. Tech. & Arts 221 (2015)
http://digital.lib.washington.edu/dspace-law/handle/1773.1/1435

ABSTRACT

The definition of authorization under the Stored Communications Act raises questions about implied authorization in situations where someone fails to secure an email account properly. The few cases that have addressed this issue under the federal act or its state equivalents have not created a bright-line rule. Instead, the question of authorization has been highly fact-dependent. Two leading interpretive theories have emerged on the question of authorization: the code-based theory and the trespass theory. While the code-based interpretation of authorization seems pleasing because it appears to provide highly predictive outcomes, it fails in some circumstances. This failure is especially obvious when someone inadvertently and unintentionally gives someone else permanent access to an email account by, for instance, saving their username and password in the browser of a shared computer. Courts interpreting cases in this context implicitly reject the code-based interpretation of authorization, which would provide no remedy, in favor of the trespass theory. Ultimately, the code-based model does not provide enough flexibility to fit all situations in which the courts wish to provide a remedy. The best test, therefore, involves aspects of both theories.

---

[*] Nicholas R. Ulrich, University of Washington School of Law, Class of 2015.
Thank you to my adviser Peter Winn and my editor Shira Zucker; their help and advice were invaluable.

TABLE OF CONTENTS

Introduction 222
I. Background 223
A. The Stored Communications Act 223
B. Civil Cause of Action 224
C. State Statutes 224
II. Courts Apply Two Interpretations of Authorization 225
A. The Code-Based Interpretation is Narrow in Scope 225
B. The Trespass Theory is a More Fluid Model 226
III. Implied Authorization is More Complicated than the Code-Based Interpretation Allows 227
A. The Context in which an Email Account is Inadvertently Left Open Demonstrates the Incompleteness of the Code-Based Theory of Authorization 227
B. The Context of a Computer Shared Between Spouses Demonstrates the Predictive Appeal of the Code-Based Interpretation 230
C. Cases in which a Person Inadvertently Grants Permanent Access to Someone Else Demonstrate Courts' Unwillingness to be Constrained by the Code-Based Model 231
IV. The Appropriate Approach to Authorization Looks to Both the Code-Based and Trespass Theories 234
Conclusion 235

INTRODUCTION

At a time where anything and everything is done online, and when our computer, phone, or tablet can store all of our private email accounts and passwords, when do we implicitly grant someone else authorization to access that information? The question is not as clear-cut as some would like to think. There are two models of interpreting the ultimate question of what constitutes *authorization* under the federal Stored Communications Act ("SCA"): the code-based theory and the trespass theory. The code-based theory relies on whether the user bypasses code-based protections of the computer or system, whereas the trespass theory analogizes to trespass law to determine implied authorization. Depending on the facts of the case, the

outcome may necessarily be different depending on which model is used. While the code-based theory is growing in popularity, it fails to provide a remedy in all cases where society and the courts appear to see the need for one. In those circumstances, the courts implicitly reject the code-based interpretation in favor of the more fluid trespass model, often leaving the ultimate determination of implied authorization to the jury.

I. BACKGROUND

As technology developed, privacy protection laws needed to as well. A wiretap statute that only penalized voice interception proved inadequate once communications started becoming electronic and digital.[1] Further, courts lacked guidance as to what extent common law protections extended to electronic communications. Recognizing these problems, Congress passed the Electronic Communications Privacy Act ("ECPA") in 1986.[2] This Act expanded the Wiretap Act to include the "interception" of electronic communications.[3] Congress also recognized that electronic communications are not always in transit; service providers also place them in temporary storage.[4] The ECPA, therefore, included the Stored Communications Act to protect communications in electronic storage.[5]

A. The Stored Communications Act

Congress passed the Stored Communications Act ("SCA") to extend privacy protections to electronic communications stored on a server that provides email or other electronic communication service.[6] The Act provides that whoever "(1) intentionally accesses

---

[1] *See* United States v. New York Telephone Co., 434 U.S. 159, 167 (1977) (recognizing that the Wiretap Act only applies where there is "aural acquisition of the contents" of a message).

[2] *See generally*, H.R. REP. NO. 99-647 (1986); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

[3] *Compare* 18 U.S.C. § 2511 (2008), *with* Wiretap Act of 1968, Pub. L. 90-351, Title III, § 802, 82 Stat. 213.

[4] *See* H.R. REP. NO. 99-647, at 22 (1968).

[5] *Id.*

[6] *See* S. REP. NO. 99-541, at 5 (1986).

without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility . . . shall be punished . . . ."[7]

The classic problem Congress designed the SCA to address is when an individual hacks into an email provider and reads another individual's emails. As one departs from the archetypal example, however, the analysis becomes more complicated. This Article does not attempt to answer the ultimate question of when a person can and cannot implicitly have authorization. Instead, this Article attempts to demonstrate the highly fact-dependent nature of the inquiry.

B. Civil Cause of Action

The SCA provides for a civil cause of action, which allows persons who are "aggrieved" by the violation of the SCA to recover damages from the violator.[8] Notably, the civil cause of action requires a lesser mens rea: from intentional to either "knowing or intentional."[9] The SCA also guarantees a minimum of a $1,000 recovery, grants the court power to award the prevailing party costs and attorney's fees, and allows for the possibility of punitive damages if the conduct was "willful or intentional."[10]

C. State Statutes

Certain states have adopted comparable statutes to the SCA.[11] For example, New Jersey expanded its Wiretap Act to include language equivalent to that of the federal SCA.[12]While New Jersey's version has a different grammatical structure than its federal counterpart, the

---

[7] 18 U.S.C. § 2701(a) (2002).

[8] *Id.*

[9] *Id.*

[10] *Id.* § 2707(c).

[11] The following is a non-exhaustive list of states that have some variation of the SCA: Alaska, Delaware, Florida, Massachusetts, New Jersey, Pennsylvania, Virginia, and Wisconsin. *See* 1 ROBERT D. BROWNSTONE & TYLER G. NEWBY, DATA SEC. & PRIVACY LAW § 9:47, at 1 n.1 (2014); N.J. STAT. ANN. § 2A:156A-27 (West 2013).

[12] N.J. STAT. ANN. § 2A:156A-27 (West 2013).

phrasing and requirements are virtually identical.[13] Further, New Jersey's version of the SCA also provides for a civil cause of action for a violation by any person "aggrieved by any violation" of the Act.[14] Due to these similarities, it is not surprising that New Jersey courts interpret the federal and state versions similarly, and they look to federal precedent when questions arise as to the New Jersey Act's scope.[15] Likewise, federal courts occasionally consider state decisions on state equivalents to the SCA.[16]

II. COURTS APPLY TWO INTERPRETATIONS OF AUTHORIZATION

Authorization is, by its very nature, a fact-specific inquiry. Even in the single context of email, several different factual variants arise requiring different approaches and interpretations. Courts use one of two predominant theories to determine whether a person accessed the communications with authorization.[17] The first, code-based interpretation is growing in popularity but does not provide enough versatility to the courts to meet the varied situations where a remedy is appropriate. The trespass model is, in comparison, much more versatile but makes predicting outcomes more challenging.

A. The Code-Based Interpretation is Narrow in Scope

The code-based approach, at its most basic, prohibits access where a person "bypasses [the] code-based protections designed to limit his use of the computer system."[18] This happens commonly

---

[13] *Compare id.*, *with* 18 U.S.C. § 2701 (2002).

[14] N.J. STAT. ANN. § 2A:156A-32 (West 1993).

[15] *See* White v. White, 344 N.J. Super. 211, 218–22 (2001) (recognizing the similarities between the SCA and New Jersey's Act and applying federal precedent to interpret New Jersey's Act).

[16] *See, e.g.*, Lazette v. Kulmatycki, 949 F. Supp. 2d 748, 754 (N.D. Ohio 2013) (considering and distinguishing two state cases).

[17] The concept of authorization is not limited to the SCA. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2008) ("CFAA"), also deals with the issue. Courts interpret authorization the same under both acts. *See* Theofel v. Farey–Jones, 359 F.3d 1066, 1078 (9th Cir. 2003) (referring to discussion of authorization under SCA when considering authorization under CFAA).

[18] Katherine Mesenbring Field, Comment, *Agency, Code, or Contract:*

when someone determines the password using a password-cracking computer program, but also covers others situations, such as where a person hacks around a password barrier or other security device, or uses social engineering to trick someone into disclosing their password to the hacker.[19] Though this approach covers a wide swath of activity, it is still narrow in that only limited types of conduct constitute code-based violations.

One reason for using this approach is clarity. Another is that it limits the number of situations that would constitute a violation of the SCA. Recognizing that statutes like the SCA impose criminal liability, some argue that the rule of lenity[20] should apply to require this narrow interpretation of authorization.[21] Therefore, this method of understanding authorization limits liability to when someone *explicitly* tricks a computer system or uses deceit to induce a human into giving more information or privileges than the person otherwise would have.[22]

B. The Trespass Theory is a More Fluid Model

Another, more fluid theory of interpreting authorization involves linking violations to the tort of trespass. This theory operates mainly by analogy between trespass law and computer systems.[23] In *Theofel*, the court found a violation of the SCA when a company sought to execute a clearly invalid subpoena on an email provider.[24] After recognizing that the SCA serves a comparable role to the tort of

---

Determining Employees' Authorization Under the Computer Fraud and Abuse Act, 107 MICH. L. REV. 819, 825 (2009).

[19] *Id.*

[20] The Rule of Lenity requires that ambiguous laws imposing criminal liability be interpreted in favor of the defendant when their ambiguity cannot be clarified through traditional means of statutory interpretation. *See* Bell v. United States, 349 U.S. 81, 83–84 (1955).

[21] *See* Warren Thomas, Comment, *Lenity on Me:* LVRC Holdings LLC v. Brekka *Points the Way Toward Defining Authorization and Solving the Split over the Computer Fraud and Abuse Act*, 27 GA. ST. U. L. REV. 379 (2011) (arguing for lenity to be applied in interpreting authorization under the CFAA).

[22] Field*, supra* note 18, at 825.

[23] *See*, *e.g.*, Theofel v. Farey–Jones, 359 F.3d 1066, 1072–73 (9th Cir. 2003). *Theofel* is the leading and arguably first case to apply the trespass model.

[24] *See id.* at 1074.

trespass, the court examined a number of situations of trespass to determine the question of mistaken authorization.[25]

The *Theofel* trespass theory is softer in the sense that it does not have the rigidness of the code-based interpretation, which looks to explicit conduct bypassing the computer protections. As such, it is better able to capture situations where the code-based interpretation fails to address society's normative intuitions. It covers the situation, for instance, when someone forgets to secure his or her system and an intruder takes improper advantage of the situation to intrude on the personal privacy of the computer's owner.[26]

III. IMPLIED AUTHORIZATION IS MORE COMPLICATED THAN THE CODE-BASED INTERPRETATION ALLOWS

Even within the restricted context of implied authorization to access someone's email, different factual scenarios yield different results. Further, the courts do not always follow the code-based interpretation, even when it would produce a definitive answer to the question of authorization.

A. The Context in which an Email Account is Inadvertently Left Open Demonstrates the Incompleteness of the Code-Based Theory of Authorization

When someone inadvertently leaves an email account open, and the next user of the computer stumbles across it, the second user does not violate the SCA by looking at the emails.[27] This result is obvious under the code-based interpretation. Despite this fact, some courts do not take the easy path by deciding the issue as a matter of law and ultimately leave the question to the jury to answer as a matter of

[25] *See id.* at 1072–73 (noting the distinction between a nosy neighbor who deceives her way into a person's home by posing as a meter reader and a wire-cop who only conceals that he intends to repeat what he hears).

[26] *See* Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW. 1395, 1420 (2007) (arguing the insufficiency of the code-based model).

[27] *See, e.g.*, Marcus v. Rogers, A-2937-09T3, 2012 WL 2428046 (N.J. Super. Ct. June 28, 2012); Doe v. City & Cnty. of San Francisco, 835 F. Supp. 2d 762, 767 (N.D. Cal. 2011).

fact.[28]

In *Marcus v. Rodgers*, a school employee used a computer after another employee who had not logged off of her email.[29] The subsequent user discovered the email inbox open on the screen and then opened two emails where the email subject indicated that he was discussed.[30] While he did not have to do anything to see the inbox contents, he did have to click on each of the two individual emails to see their text.[31] He eventually printed and disseminated the content of the emails.[32] Criminal charges were brought against Rodgers but ultimately dismissed.[33] Thereafter Marcus, the owner of the email account, sued under New Jersey's equivalent of the SCA.[34] The trial court denied a motion for summary judgment and let the issue go to a jury.[35] The jury found that Rodgers did not violate the act.[36]

On appeal, the court found that Marcus could not establish that the defendant acted without authorization because she left her email account open and accessible.[37] The court noted that the defendant did not circumvent a username or password but merely accessed what was open and available to him.[38] This analysis implies a code-based approach to interpreting authorization.

However, the court did not close the door on further analysis beyond the simple code-based inquiry. While the code-based approach appeared to resolve the first question of whether the defendant had authorization, the court looked further to whether the defendant "knowingly *exceeded* his authorization."[39] As to this second step, the court focused on the mens rea requirement: "plaintiffs had to establish that [Rogers] *knowingly* exceeded his

---

[28] *Marcus*, 2012 WL 2428046, at *5.
[29] *Id.* at *1.
[30] *Id.* at *1–2.
[31] *Id.*
[32] *Id.* at *1–3.
[33] *Id.* at *3.
[34] *Id.*
[35] *Id.* at *1.
[36] *Id.*
[37] *Id.*
[38] *See id.* at *5.
[39] *Id.* (emphasis added).

authorization."[40] The court held that whether he *knowingly* exceeded his implied authorization was ultimately for the jury to determine.[41] Leaving this question to the jury speaks to the fact-based nature of this question and suggests that the code-based approach did not resolve the question completely.

Similarly, in *Doe v. City and County of San Francisco,*[42] the plaintiff sued (under the Federal SCA) after her supervisor obtained emails from her personal email account and tried to use them in a disciplinary action.[43] The plaintiff's employer provided computers on which the employees could check personal email.[44] One of the defendants printed twenty-eight of Doe's emails.[45] The defendants claimed that Doe left these emails opened in minimized windows and that one of the defendants discovered them upon using the computer after Doe.[46] Doe maintained that she did not leave these emails open and that one of the defendants discovered them upon a search of her email folders.[47]

Defendants moved for summary judgment, which the trial court denied, recognizing that there was a genuine issue of material fact over how the defendants gained access to the emails.[48] The jury returned a verdict in favor of Doe.[49] Defendants moved for a judgment as a matter of law, which the court denied as to the SCA claim.[50] In denying the motion, the court recognized that the Ninth Circuit applies the trespass framework.[51] The court also reiterated that there was a factual question as to how the defendants came by the emails, i.e., whether they were left open or not, and expressed

---

[40] *Id. at* *5–6.
[41] *See id.*
[42] 835 F. Supp. 2d 762 (N.D. Cal. 2011).
[43] *Id.* at 766.
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] *Id.* at 770.
[49] Doe v. City & Cnty. of San Francisco, No. C10-04700 TEH, 2012 WL 2132398, at *1 (N.D. Cal. June 12, 2012).
[50] *Id.* at *3.
[51] *Id.* at *2–3 (citing Theofel v. Farey–Jones, 359 F.3d 1066 (9th Cir. 2003)).

skepticism as to the defendants' story.[52]

The juxtaposition of these two cases serves to highlight how highly fact-dependent the outcomes of these cases are. While it is important to note that these cases deal with different statutes in different jurisdictions,[53] both indicate the unwillingness of courts to leave the question to the simple code-based approach. Ultimately, and despite the simple answer under the code-based approach, both courts left the question to the jury.

B. The Context of a Computer Shared Between Spouses Demonstrates the Predictive Appeal of the Code-Based Interpretation

Feuding spouses provide another context in which questions of implied authorization arise. In these cases, the code-based model seems applicable and largely outcome-determinative.

In *White v. White,*[54] the wife hired a private agency to investigate her husband for information that she could use to obtain a divorce.[55] The agency looked at a computer that was for family use and found that the husband had backed up all his emails on the hard drive.[56] Not knowing that the emails would be available without username or password, he did not attempt to secure the emails.[57] The wife's investigator copied the emails from the hard drive.[58] In the resultant custody proceeding, the husband moved to suppress the emails, arguing that the private investigator accessed them in violation of New Jersey's version of the SCA.[59]

In denying the motion, the court briefly addressed the concept of authorization. It stated, "'without authorization' means using a computer from which one has been prohibited, or using another's

---

[52] *Id.*

[53] *Marcus* applies the New Jersey equivalent to the SCA, while *Doe* applies the federal SCA.

[54] 344 N.J. Super. Ct. 211 (2001).

[55] *Id.* at 215–16.

[56] *Id.*

[57] *Id.* at 216.

[58] *Id.* at 217.

[59] *Id.* at 214–15.

password or code without permission."[60] The court held that, because the wife had authority to access the computer, she did not violate the act.[61]

A different factual situation arose in *Miller v. Meyers*.[62] In *Miller*, the defendant was able to access his wife's email account by installing a "key-logger" program[63] on a computer primarily used by the wife and thereby obtained her email password.[64] The court granted summary judgment for the wife, finding no issue of material fact.[65]

In this context, the code-based interpretation of authorization is predictive. The *Miller* case demonstrates a code-based violation: the husband installed a secret program on the computer to bypass the code-based protections. When the court granted summary judgment for the wife, it implicitly affirmed the code-based model. By contrast, in *White* there was no code-based violation: the wife's private investigator merely stumbled upon saved emails. An attorney could easily predict the outcomes for both of these cases if he or she were assured that the courts would apply the code-based interpretation. However, courts sometimes completely reject the code-based model in favor of the trespass model, making accurate prediction challenging.

C. Cases in which a Person Inadvertently Grants Permanent Access to Someone Else Demonstrate Courts' Unwillingness to be Constrained by the Code-Based Model

A third context of implied authorization occurs when a person inadvertently allows someone else access to his or her email system. In this situation, repeated access may violate the SCA. In this

---

[60] *Id.* at 221 (citing Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817 (E.D. Mich. 2000)).

[61] *Id.* at 221.

[62] 766 F. Supp. 2d 919 (W.D. Ark. 2011).

[63] A key-logger program is a program that, once installed, runs in the background of a computer and records every key stroke made by a user. *See* Oxford English Dictionary Online (Drft. Rev. Dec. 2012), http://www.oed.com (enter "key-logger"; then click "go").

[64] *Miller*, 766 F. Supp. 2d at 920.

[65] *Id.* at 923.

scenario, courts may reject the code-based interpretation of authorization in favor of the more fluid trespass theory.

In *Lazette v. Kulmatycki*,[66] Verizon issued Lazette, an employee, a BlackBerry for business and personal use.[67] Verizon allowed the employee to check her personal Gmail account on the BlackBerry.[68] At the end of her employment, she returned the BlackBerry with all her personal emails deleted but without disabling or removing the Gmail account access.[69] Subsequently, her supervisor used the BlackBerry and continually monitored her personal email account from it.[70]

Lazette sued, alleging a violation of the SCA.[71] The defense filed a 12(b)(6) motion to dismiss and argued that her failure to secure the system deprived her of a claim under the SCA.[72] The court declined to dismiss, stating that "negligence [in failing to remove the account] is, however, not the same as approval, much less authorization."[73] The court followed the trespass model, analogizing the situation to someone who "fails to leave the door locked when going out" as opposed to "one who leaves it open knowing someone [will] be stopping by."[74]

In another case, *Pure Power Boot Camp v. Warrior Fitness Boot Camp*,[75] plaintiffs brought action against defendants for theft of business model, violation of trademarks and copyrights, and breaching fiduciary duties.[76] Defendants moved to exclude from evidence certain emails obtained in violation of the SCA.[77] Mr. Fell, owner of the defendant corporation, left his username and password for his personal email account stored on his work computer, such that it auto-filled when an employee of plaintiff corporation accessed the

---

[66] 949 F. Supp. 2d 748 (N.D. Ohio 2013).
[67] *Id.* at 751.
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.* at 751.
[72] *Id.* at 756.
[73] *Id.* at 757.
[74] *Id.*
[75] 587 F. Supp. 2d 548 (S.D.N.Y. 2008).
[76] *Id.* at 551.
[77] *Id.*

email account.[78]

The plaintiff[79] argued that authorization was implied because Fell left his username and password stored on the work computer.[80] The court applied the trespass model, likening plaintiff's conduct to leaving "a key to his house on the front desk [of the plaintiff's corporation]" and maintained that in such a situation, "one could not reasonably argue that he was giving consent to whomever found the key, to use it to enter his house and rummage through his belongings."[81] The court held that there was no implied authorization for plaintiff's employees to access his personal email directly from his Hotmail account and other accounts by using a password stored on plaintiff's computers.[82]

One final case does not involve inadvertence but express permission. In *Cardinal Health 414, Inc. v. Adams*,[83] two employees, Adams and Young, exchanged their usernames and passwords so they could access each other's email and other work materials when one was replacing the other as manager. After a couple of years, Adams left the company.[84] Though Adam's own username and password ceased to work once he left, he continued to access information on the employer's server using Young's account information.[85] He ultimately obtained information that was proprietary in nature.[86]

The company eventually sued under, inter alia, the SCA. Both sides moved for summary judgment. Despite the fact that Young freely gave Adams his username and password, the court granted judgment for the plaintiff, finding an SCA violation as a matter of law.[87] The court first noted that "[c]ommon sense should have been sufficient to indicate to Adam that [his] behavior was wrong."[88] Then the court applied the trespass model:

---

[78] *Id.* at 552.
[79] The plaintiff was the non-movant for the motion.
[80] *Pure Power Boot Camp,* 587 F. Supp. 2d at 559, 561.
[81] *Id.* at 561.
[82] *Id.* at 562.
[83] 582 F. Supp. 2d 967, 970 (M.D. Tenn. 2008).
[84] *Id.*
[85] *Id.* at 970–71.
[86] *Id.* at 972.
[87] *Id.* at 977.
[88] *Id.*

> Drawing the analogy to trespassing, it is as if, two years earlier, Young asked Adams to water the plants in his office while he was on vacation and, for this purpose only, Young gave Adams an extra key to his office. Then, two years later, after Adams left the company, Adams used the key to come back in the office, snoop around, and take some of Young's work-related materials. Such conduct would clearly be trespassing.[89]

The first two of these cases suggest that, when a person inadvertently leaves another individual permanent access to his or her password, he or she does not grant the other individual authorization to access the email account. The final case suggests that inadvertence may not even be required. In all three situations the courts comfortably used an analogy, likening the situation to trespass law, thereby applying the trespass theory of authorization. Additionally, in all three cases the courts implicitly rejected the code-based analysis by finding breach of the act for simply using the password someone had access to. These cases demonstrate that the code-based approach is insufficient. It does not provide a remedy in every situation where society would expect one. The trespass theory is more fluid and can fit these unusual cases. If *Lazette*, *Pure Power Boot Camp*, and *Cardinal Health* are any indication, courts tend to abandon the code-based interpretation of authorization in situations where the code-based interpretation would not provide (from the court's perspective) an adequate remedy.

IV. THE APPROPRIATE APPROACH TO AUTHORIZATION LOOKS TO BOTH THE CODE-BASED AND TRESPASS THEORIES

It is important to note that the code-based and trespass approaches to authorization are not mutually exclusive. The predictive benefit of the code-based model can, at least in part, be utilized while still allowing a more fluid trespass model to emerge and protect individuals when needed. In fact, the best approach to determining authorization would involve both approaches working in tandem. As

[89] *Id.*

a threshold inquiry, the courts should look to whether the defendant bypassed any code-based protections. If the answer to that question is yes then there is no need to examine trespass theories, as those actions would amount to a violation as a matter of law.[90] If the answer is no then the court should still use the trespass model to see if it indicates a violation. This second step is in accord with the court's examination of whether the defendant knowingly exceeded his or her authorization.[91] This question will often be left to the jury, as the mens rea of "knowingly" is a material fact.

This combined approached is advantageous because it preserves the best of both theories. The main benefit of the code-based approach is its predictive nature and addressing the more clear-cut case of hacking. Further, the advantage of the trespass model is its fluid nature. If the code-based theory does not establish a violation, the trespass model allows courts to address the normative issues that the code-based theory does not fully capture.

CONCLUSION

The question of authorization under the SCA is complex and largely fact-specific. The different interpretations of authorization provide the courts tools for addressing these complications. The code-based theory of authorization, being the more popular of late, may seem appealing at first because it is narrower in scope, incorporates familiar concepts of lenity, and seemingly provides the ability to predict outcomes. In some circumstances, however, the courts choose to abandon the code-based theory where a different result seems appropriate based on social norms. Thus, even when no code-based violation seems apparent, as in *Marcus*, the trespass model permits courts to leave the issue to the jury.[92] There is no bright-line rule. The strong predictive ability of the code-based model is valuable as one measure of a trespass but is not the only measure. While picking the lock of one's back door makes for an easy case of trespass, walking through the open front door may also be a trespass under the right

[90] *See, e.g.*, Miller v. Meyers, 766 F. Supp. 2d 919 (W.D. Ark. 2011).

[91] *See, e.g.*, Marcus v. Rogers, A-2937-09T3, 2012 WL 2428046 (N.J. Super. Ct. App. Div. June 28, 2012).

[92] *See id.* at *5.

facts. So too, in the computer trespass context, practitioners should be aware that slightly distinguishable facts can create vastly different outcomes. The best model would involve using aspects of both approaches together. Thus, a court can get some of the predictive ability of the code-based approach while still having the freedom to find violations under analogies to trespass law when the facts and societal norms demand it.