The John Marshall Journal of Information Technology & Privacy Law

Volume 26
Issue 4 *Journal of Computer & Information Law - Summer 2009*

Article 3

Summer 2009

The Black Box Canon of Statutory Interpretation: Why the Courts Should Treat Technology Like a Black Box in Interpreting Computer Crime Statutes, 26 J. Marshall J. Computer & Info. L. 487 (2009)

Peter V. Roman

THE BLACK BOX CANON OF STATUTORY INTERPRETATION: WHY THE COURTS SHOULD TREAT TECHNOLOGY LIKE A BLACK BOX IN INTERPRETING COMPUTER CRIME STATUTES

PETER V. ROMAN*

I. INTRODUCTION

Computer crime statutes exist in a particular universe where misinterpretations are easy to make and hard to undo. When reading computer crime statutes, federal courts sometimes study the minutiae of technology at the expense of congressional intent, plain language, and fair warning to criminal defendants. By focusing on the actual, but transient and morally irrelevant, design of information systems, the courts are undermining criminal law in the digital world.

Traditional tools of statutory interpretation have failed to stop this approach to the interpretation of computer crime statutes. Courts need a new tool to help them apply computer crime statutes in a consistent manner across increasingly complex and constantly evolving technology. When interpreting computer crime statutes, courts should focus less on the transitory technicalities of how things work, in the digital world at that particular moment, and more on the moral purpose of the law.

By treating the design of the underlying technology as a black box, essentially ignoring the transitory and legally irrelevant behavior of information systems, courts will have an easier time making consistent decisions that reflect the moral and constitutional underpinnings of computer criminal law. This will make the interpretation of computer

* Peter V. Roman is an associate at Arnold & Porter LLP in the firm's litigation practice group where he also maintains a small pro bono criminal law practice. Before attending law school, he worked for fourteen years in information technology, primarily as a consultant in large-scale mission-critical database design and administration. Georgetown University Law Center, J.D. 2008; Vassar College, A.B. 1990.

crime statutes more consistent with congressional intent and the relevant decisions more predictable.

II. BACKGROUND & ANALYSIS

There are two fundamental reasons why courts should avoid examining the underlying technology in computer crime statutes. First, the common user of technology does not know, nor care, how the underlying technology works. Making decisions based on irrelevant or unknown technological minutiae both denies the criminal defendant fair warning that their behavior violates the law and undercuts the intent of the statute. Second, the rapid changes in the underlying technology mean that decisions based on that technology may quickly become obsolete as new technology replaces it. However, neither the courts nor Congress can move as to update the law as quickly as the rapid pace of change in the underlying technology would require, especially if technology continues to be subject to detailed analysis by courts interpreting computer crime statutes. Such holdings also deny criminal defendants fair warning and undermine the intent and effectiveness of the statute.

A. Technological Minutiae are Irrelevant or Unknown to Users

Because the design of the underlying technology at issue in computer crime statutes is unknown or does not matter to ordinary users, neither should it matter to the courts.[1] Since the underlying technological minutiae are unknown or irrelevant, examining it when interpreting a computer crime statute may undermine the intent of the statute. Similarly, because such technology is irrelevant or unknown, basing the interpretation of ambiguous words in the statute upon an examination of the technology may violate the fair warning doctrine.

Examining the underlying technological design when interpreting a computer crime statute may undermine the intent of the statute. This problem is especially evident in relation to the Electronic Communications Privacy Act of 1986 ("ECPA"),[2] as demonstrated in the series of decisions beginning with *Steve Jackson Games, Inc. v. U.S. Secret Service*[3] and ending, at least temporarily, with *United States v. Councilman* (*Councilman II*).[4] The "ECPA was a[n] effort to protect electronic communications in two forms—from real-time monitoring or interception as

1. *See* United States v. Gilboe, 684 F.2d 235, 238 (2nd Cir. 1982) (holding that the electronic means by which money was transported is irrelevant); *see also* United States v. Thomas, 74 F.3d 701, 707 (6th Cir. 1996) (holding the same for pictures).

2. Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2521, 2701-2710, 3121-3126 (2007)).

3. Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994).

4. United States v. Councilman (*Councilman II*), 418 F.3d 67 (1st Cir. 2005) (en banc).

they were being delivered [the Wiretap Act], and from searches when they were stored in record systems [the Stored Communications Act]."[5] This series of decisions "eviscerated the protections that Congress established back in the 1980s."[6]

Congress originally wrote Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Wiretap Act")[7] in part, to codify the heightened scrutiny that the Fourth Amendment requires when the government conducts continuous surveillance, including wiretaps, and to apply it to the public.[8] Congress based the Wiretap Act on the constitutional holdings of *Katz v. United States*[9] and *Berger v. New York*.[10]

Katz is the seminal Fourth Amendment and wiretapping case.[11] In *Katz*, the Supreme Court held that the Constitution protects communications when the individual under surveillance has a reasonable expectation of privacy.[12] The Fourth Amendment requires particularity for a warrant, and in the context of the *Burger* case, the Court held the government must particularly describe the information it seeks, and by definition could not do so when asking to perform continuous surveillance.[13] The Court further compared continuous surveillance to general warrants, which it had previously declared unconstitutional.[14] Congress wrote the Wiretap Act to codify these holdings and apply them to the public.[15]

The ECPA modified the Wiretap Act by adding electronic communications to the list of communications it protected from continuous surveillance.[16] The ECPA also created the Stored Communications Act ("SCA") to protect stored communications, specifically voicemail and e-

5. Brief for the Center for Democracy and Technology et al. as Amici Curiae Supporting Appellants, *Councilman II*, 418 F.3d 67 (1st Cir. 2005) (No. 03-1383), 2003 U.S. 1st Cir. Briefs 1383 (citing 214 CONG. REC. S7893-96 (daily ed. July 9, 2004) (statement of Sen. Leahy)).

6. Saul Hansell, *You've Got Mail (and Court Says Others Can Read It)*, N.Y. TIMES, July 6, 2004, at C1, *available at* http://www.nytimes.com/2004/07/06/technology/06net.html?scp=6&sq=youve%20got%20mail&st=cse (quoting Marc Rotenberg, executive director of the Electronic Privacy Information Center); *see Councilman II*, 418 F.3d at 72.

7. 18 U.S.C. §§ 2510-2521 (2007).

8. Brief for the Center for Democracy and Technology et al. as Amici Curiae Supporting Appellants, *Councilman II*, 418 F.3d 67 (1st Cir. 2005) (No. 03-1383), 2003 U.S. 1st Cir. Briefs 1383 [hereinafter Amicus Brief].

9. Katz v. United States, 389 U.S. 347 (1967).

10. Berger v. New York, 388 U.S. 41 (1967).

11. *Katz*, 389 U.S. at 347.

12. *Id.* at 359.

13. *Berger*, 388 U.S. at 58-60.

14. *Id.* at 58.

15. Amicus Brief, *supra* note 8.

16. Pub. L. No. 99-508, tit. I, 100 Stat. 1848 (codified at 18 U.S.C. § 2511(1)).

mail, from one-time searches.[17] A one-time search is a discrete acquisition that would cover only the objects present on the day the search was executed and potentially only some of those objects. Congress exempted stored communications from the higher level of scrutiny required by the Wiretap Act because one-time searches are a much lesser invasion of constitutional rights than continuing surveillance.[18] After the recipient has read the communication, it becomes is stored communications and can be requested on a much more particularized basis than continuing surveillance; therefore, it is subject to the lesser protections of the SCA.[19]

Federal courts have repeatedly attempted to define "intercept" and "electronic communications" in light of current technology, even though the statute already defines both terms.[20] In ECPA "electronic storage" cases, the combination of the courts' tendency to delve into the minutiae of technology and the weight of precedent has led to a series of decisions that undermine the purpose of the ECPA and have produced complex and tortured readings of the Wiretap Act. As a result of to the federal courts' interpretation of ECPA in finding that e-mail could not be intercepted almost anywhere at all, a panel of the First Circuit noted that "[i]t may well be that the protections of the Wiretap Act have been eviscerated as technology advances."[21] However, technological advancement was not the culprit. The culprit was the court's unnecessary examination of the technology.

By reframing the issue around whether the objects of the search were moving or not, the courts completely missed the point of both the Wiretap Act and *Berger*. If the purpose of the Wiretap Act was to prevent continuing surveillance, then there are two questions courts need to consider: (1) was the conduct at issue continuing surveillance; and (2) did it search electronic communications? Regardless of whether the objects of the search are at rest at the moment when they are acquired, so long as they are still collected on a continuing basis, then the data collection should be considered continuing surveillance, and therefore subject to the Wiretap Act.

Steve Jackson Games[22] is the first in a line of cases that delves into the technical workings of e-mail and emerges with black letter law com-

17. *See Councilman II*, 418 F.3d at 78-79.

18. *Id*. at 76 (citing *Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice, H. Comm. on the Judiciary*, 99th Cong. 214, 230 (1986) (statement of James Knapp, Deputy Assistant Attorney General, Criminal Division, U.S. Dep't of Justice)).

19. 18 U.S.C. § 2701-11 (2007).

20. *Id.* at § 2510(4), (12).

21. United States v. Councilman (*Councilman I*), 373 F.3d 197, 203 (1st Cir. 2004).

22. *Steve Jackson Games*, 36 F.3d at 457.

pletely at odds with the intent of Congress and the *Berger* Court and any common sense or plain meaning interpretation of the Wiretap Act.[23] The court got the right result for the wrong reason, and that reason has haunted the Wiretap Act ever since.

In *Steve Jackson Games*, the Secret Service confiscated a bulletin board server that also held a number of unopened e-mails.[24] The plaintiffs sued for damages under the Wiretap Act.[25] They claimed that the Secret Service intercepted their e-mail in violation of the Wiretap Act's provisions against the interception of electronic communication.[26] The district court held that the e-mail that was stored, even if the intended recipient had not read it yet, and was not intercepted because its acquisition was not contemporaneous with the communication.[27]

The district court based its decision in *Steve Jackson Games* on a previous case before the Fifth Circuit, *United States v. Turk*.[28] In *Turk*, police seized a tape recording of a phone conversation.[29] The plaintiffs sued under the Wiretap Act, claiming that this was an interception.[30] The statute defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[31] The plain meaning of the definition in the statute does not include any limits on when the acquisition takes place.[32] The Fifth Circuit placed limits on the statute when it held that an interception required the "contemporaneous acquisition of the communication."[33] Under this holding, confiscating the recording of a completed conversation was not an interception.[34] This holding corrected a plain language interpretation of the Wiretap Act that was clearly not the intent of Congress.

In *Steve Jackson Games*, the district court supported the *Turk* court's gloss on the word "intercept" and applied it to e-mail by finding that "an intercept require[s] participation by the one charged with an 'interception' in the contemporaneous acquisition of the communication."[35] The potential danger is already becoming apparent. Because

23. *Id*.
24. *Id*. at 459.
25. *Id*.
26. *Id*.
27. *Id*. at 459-60.
28. United States v. Turk, 526 F.2d 654 (5th Cir. 1976).
29. *Id.* at 656.
30. *Id.* at 654.
31. 18 U.S.C. § 2510(4) (2007).
32. *Turk*, 526 F.2d at 657 (stating "[interception] could be said to occur whenever someone [gets] the contents of a communication").
33. *Id.* at 658.
34. *Id.*
35. *Steve Jackson Games*, 36 F.3d at 460.

the district court looked too closely at the underlying technology, it held that an e-mail conversation that was not finished was the same as a phone conversation that was.

The Fifth Circuit in *Steve Jackson Games* agreed that an e-mail conversation that was not finished was the same as a phone conversation that was, although on different grounds. The Fifth Circuit analyzed the statute and found that the meaning of "electronic communications" excluded anything in electronic storage.[36] Then the Fifth Circuit, like the district court, examined the underlying technology. Specifically it looked at how the e-mail traveled from the writer to the intended recipient.[37] It discovered that e-mail came to rest for some period in the intended recipient's mailbox.[38] Having come to rest, even temporarily, the Fifth Circuit decided that it was no longer in transit, even though the intended recipient had not yet received the message.[39] Based on their examination, the court found that sent but unopened e-mail in a user's mailbox was in electronic storage.[40] Therefore, it could not be intercepted.[41] In effect, the deciding issue in whether an e-mail can be intercepted became whether the message was in motion or stationary at the moment when it was acquired, instead of whether the intended recipient had received the message.

Examining whether an e-mail was in motion or stationary at the moment when it was acquired completely misses the point of having greater scrutiny for continuing surveillance than one-time search and seizure. In *Steve Jackson Games*, the Fifth Circuit acknowledged that "Congress' purpose in enacting the ECPA [was] to include providing protection for [e]-mail and bulletin boards."[42] However, it argued that "obviously, the language of the Act controls."[43] The court analyzed congressional intent, but did so in favor of its understanding of the then-current design of the relevant information technology.[44] With that handicap, it was inevitable that the court would not realize how its understanding of the technology was warping the statute.

Neither the district court's nor the Fifth Circuit's rationale would have stood up at all if the courts had not made its decisions in light of the underlying technology involved. The district court's holding that e-mail that had not yet reached its intended recipient, but had reached his

36. *Id.* at 461.
37. *Id.* at 458.
38. *Id.*
39. *See Id.* at 460.
40. *Id.*
41. *Steve Jackson Games*, 36 F.3d at 461-62.
42. *Id.* at 460.
43. *Id.* at 461.
44. *Id.* at 461-64.

mailbox, could not be intercepted, is at odds with common sense, the intent of the statute, and the holding in *Berger*. The Fifth Circuit's alternative rationale, that messages at rest during the course of their journey are exempt from the Wiretap Act, also fails the intent of the statute and *Berger*. The court had to know that the e-mail had stopped moving in order to support its decision.

B. Examining the Underlying Technology Denies the Criminal Defendant Fair Warning

In computer crimes, as in other crimes, defendants must have fair warning that their behavior violates the law. Because most users are unaware of the technological minutiae underlying their computerized actions, and because that underlying technology changes so rapidly, often without any obvious difference in the user's experience, convictions based on the underlying technology deny defendants fair warning that their behavior is illegal. "The [fair warning doctrine] . . . is that no man shall be held criminally responsible for conduct which he could not reasonably understand to be proscribed."[45]

> There are three related manifestations of the fair warning requirement. First, the vagueness doctrine bars enforcement of "a statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application." Second, . . . [the] rule of lenity, ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered. Third, . . . due process bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope. In each of these guises, the touchstone is whether the statute, either standing alone or as construed, made it reasonably clear at the relevant time that the defendant's conduct was criminal.[46]

The courts cannot expect anyone to understand what behavior computer crime statutes proscribe if the courts base their interpretation of the statute on the underlying design of the technology, because the design changes so frequently, and is so complicated to begin with. The technological minutiae of how information systems work "may make no difference to the users, but they make an enormous difference to the privacy that e-mail is accorded under federal law."[47] Most casual e-mail users would be very surprised to learn that their e-mail moved indirectly

45. United States v. Lanier, 520 U.S. 259, 265-66 (1997) (quoting Bouie v. City of Columbia, 378 U.S. 347, 351 (1964) (quoting United States v. Harriss, 347 U.S. 612, 617 (1954))).

46. *Lanier*, 520 U.S. at 266-67 (quotations omitted).

47. Hansell, *supra* note 6; *see also* Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 Geo. L.J. 357, 361 (2003) (stating "significant changes in the behind-the-scenes workings of the Internet can go entirely unnoticed by users").

from the writer to the intended recipient.[48] They are no more likely to know that e-mail is stored and forwarded than to know what BIOS is, or how their voice is transmitted through the phone lines.[49] In fact, most people would not assume, as the courts did in *Steve Jackson Games* and numerous later cases, that the protection ended when the e-mail reached their mailbox.[50] The mailbox is not where legal protection for normal mail ends.[51]

The fact that the court requires an expert to explain how the technology works is evidence that the reasonable layperson could not know such details. By delving into the inner workings of incredibly complicated technology, the courts are replacing the "man of common intelligence" in this analysis with a computer science Ph.D. Because the public is operating without this knowledge, any decision based on the technological underpinnings is likely to *per se* fail the fair warning requirement, even if it matches the language in the statute.

Because legal precedents change slowly and technological design changes rapidly, the power of precedent means that once the technological underpinnings of a holding are gone, they still can affect decisions for years, even decades, to come. Therefore, courts should avoid looking too closely at the precise technology at work at a particular moment.

In 1965, Gordon Moore, a co-founder of Intel, first articulated the maxim known as Moore's Law, which effectively says that computing power will double every eighteen months.[52] Given the apparent truth of this standard,[53] it is difficult to know exactly when things will stabilize enough that an in-depth look at the underlying technology of a particular computer crime statute will not quickly become an anachronism. Forty-years ago, the Supreme Court noted that the law "has not kept pace with these advances in scientific knowledge."[54] The technology that the

48. Hansell, *supra* note 6 (quoting Marc Rotenberg, executive director of the Electronic Privacy Information Center); Kerr, *supra* note 47.

49. *See generally* Hansell, *supra* note 47, at C1 (quoting Marc Rotenberg, executive director of the Electronic Privacy Information Center); Kerr, *supra* note 47.

50. Hansell, *supra* note 47, at C1 (quoting Marc Rotenberg, executive director of the Electronic Privacy Information Center); Kerr, *supra* note 47.

51. *See, e.g.*, United States v. Hill, 579 F.2d 480, 482 (8th Cir. 1978) (stating "until the addressee or his authorized agent received the mail, [federal protections] applied." (citing Maxwell v. United States, 235 F.2d 930, 932 (8th Cir. 1956))).

52. Gordon E. Moore, *Cramming More Components Onto Integrated Circuits*, 38 ELECTRONICS 8 (Apr. 19, 1965).

53. *See, e.g. Moore's Law at 40, Happy Birthday*, THE ECONOMIST, Mar. 26, 2005, *available at* http://economist.com/displaystory.cfm?story_id=3798505; John Markoff, *It's Moore's Law, but Another had the Idea First*, N.Y. TIMES, Apr. 18, 2005, *available at* http://www.nytimes.com/2005/04/18/technology/18moore.html.

54. *Berger*, 388 U.S. at 49 (1967).

courts observe to interpret computer crime statutes today may not exist tomorrow.

1. *Examining Rapidly Changing Underlying Technology Undermines the Statute's Intent*

Because precedent changes so much more slowly than technology, court decisions based on current technology may undermine the intent of computer crime statutes in the future when the technological design changes. The actions and intentions of the various parties should be what is at issue, not whether the technology has changed in some way that is irrelevant to the intent of the law.

The effect of the holding in *Steve Jackson Games* on *United States v. Councilman (Councilman I)*[55] shows how court decisions based on ever-changing underlying technology can undermine the computer crime statute's intent in future decisions. . In *Steve Jackson Games*, the court interpreted the Wiretap Act based on the current design of e-mail technology. At the time, users wrote e-mail on their computer and then uploaded it to a bulletin board server.[56] The e-mail stayed on the bulletin board server until the intended recipient dialed in by phone, downloaded the e-mail, and read it.[57] The recipient might then save the e-mail on the server.[58] The entire sequence of events took place between two computers, the user's computer and the bulletin board server. At that time, when a piece of e-mail stopped it would fall out of the jurisdiction of the Wiretap Act and into the SCA, at least until that e-mail had made it to the intended recipient's mailbox.[59]

Ten years after the *Steve Jackson Games* decision, e-mail had evolved into a much more complicated system, although the precedent remained the same. "An e-mail message, which is composed using an e-mail program, is transferred from one computer to another [multiple times] on its way to its final destination, the addressee."[60] "These intermediate computers occasionally retain backup copies of the e-mails that they forward and then delete those backups a short time later."[61] Ten years later, e-mail stopped multiple times between the sender's and the recipient's mailbox. Now there are many places where e-mail can be in "electronic storage" and the first one may be nowhere near the intended recipient's mailbox.

---

55. *Councilman I*, 373 F.3d at 197.
56. *Steve Jackson Games*, 36 F.3d at 458.
57. *Id.*
58. *Id.*
59. *Id.*
60. *Councilman I*, 373 F.3d at 199.
61. *Id.* at 205.

In *Councilman I*, the defendant argued and the district court agreed that since the e-mail was in electronic storage it could not be intercepted, even though it was not in the recipient's mailbox.[62] The defendant/appellee told his employees to capture all e-mail going to his subscribers from Amazon.[63] The defendant acquired the e-mail before it got to the user's mailbox.[64] The government charged the defendant with conspiracy to violate the Wiretap Act by intercepting electronic communications.[65] The panel of the First Circuit also agreed, relying on the contemporaneous interception definition and the holding defining when information is in electronic storage from *Steve Jackson Games*.[66]

In *United States v. Councilman (Councilman II)*,[67] however, the First Circuit, sitting *en banc*, found that *Councilman I*'s "interpretation of the Wiretap Act [was] inconsistent with Congress' intent."[68] The court in *Councilman II* found that Congress' only intention in creating a distinction between wire and oral communications was to protect voicemail.[69] In addition, the *Councilman I* court admitted at the time that its decision might eviscerate the Wiretap Act.[70] Whatever Congress' intent regarding e-mail protection, it cannot have intended to write a law that technology would eviscerate within a few years.

The court found that the *Councilman I* decision incorrectly created an "existential oddity" where "messages—conceded by stipulation to be electronic communications—briefly cease to be electronic communications for very short intervals, and then suddenly become electronic communications again."[71] This existential oddity was not a significant problem under the technology of *Steve Jackson Games*.[72] The court still got the right result because the e-mail was in the recipient's mailbox. It became a problem once the court held the same thing about e-mail in an unknown computer that could be miles away from the recipient's mailbox. The precedent could not adapt as fast as the technology did.

62. *Id.* at 200.
63. *Id.* at 199.
64. *Id.*
65. *Id.* at 199-00.
66. *Councilman I*, 373 F.3d at 202-04.
67. *Councilman II*, 418 F.3d at 67.
68. *Id.* at 72.
69. *Id.* at 78-79.
70. *Councilman I*, 373 F.3d at 203.
71. *Councilman II*, 418 F.3d at 78.
72. *Steve Jackson Games*, 36 F.3d at 457.

2. *Examining Rapidly Changing Underlying Technology Denies Criminal Defendants Fair Warning*

The indeterminacy of the solution in interpreting computer crime statutes may deny criminal defendants fair warning because the design of technology changes faster than precedent. As in other areas of the law, there needs to be consistency in the court's approach in order to provide a potential criminal defendant with fair warning that his action might violate the statute.[73] If ordinary people cannot tell which perspective a court will take in interpreting a computer crime statute, then they will have no idea how to obey it.

The fair warning doctrine protects criminal defendants from prosecution for conduct that they "could not reasonably understand to be proscribed."[74] The fair warning doctrine has three manifestations, all of which apply here. First, "[a] statute is unconstitutionally vague . . . if it 'prohibits . . . an act in terms so uncertain that persons of average intelligence would have no choice but to guess at its meaning and modes of application.'"[75] Here, even if the statute was not inherently vague, the court's interpretation based on rapidly changing underlying technology creates vagueness. These holdings created a "storage-transit dichotomy," effectively changing the basis for decisions from whether the interception is of a series of communications to whether the communications were in motion or at rest when they were intercepted.[76] This is not at all clear in reading the statute, and once *Councilman II* reverts back to the test for a series of interceptions, it is unclear which test a court will apply as the other circuits may continue to follow the test of whether the e-mail was in motion when intercepted.

Second, the fair warning doctrine manifests itself in the rule of lenity, which "resolv[es] ambiguity in a criminal statute as to apply it only to conduct clearly covered."[77] Here it is not clear what conduct is covered, reading an e-mail while in motion or reading an e-mail before it gets to the recipient's mailbox.

Third, fair warning doctrine and "due process bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope."[78] When courts base decisions on current technology, a court cannot later modify its holding by reviewing the new underlying

---

73. *See Lanier*, 520 U.S. at 265-66.

74. *Id.* at 265.

75. *Councilman II*, 418 F.3d at 84 (citing United States v. Hussein, 351 F.3d 9, 14 (1st Cir. 2003)).

76. *Councilman I*, 373 F.3d at 203; Amicus Brief, *supra* note 8.

77. *Lanier*, 520 U.S. at 266.

78. *Id.* at 266.

technology so that a defendant's behavior that was legal using the old technology would not be legal using the new technology.

Such a lack of fair warning may have consequences outside the courtroom as well. In order to protect users, and themselves, from unintentional illegal action, computer programmers will avoid whole areas of potential development or will stop innovating once the court has ruled based on an existing technological solution. To protect ordinary people from accidentally committing crimes, and to preserve the innovative character of the web, the courts should choose a single method of interpreting computer crime laws.

III. PROPOSAL

In order to avoid examining the morally irrelevant and effervescent technology, the courts should treat the design of the underlying computer technology involved as black box. Given the rapid transformation of underlying technology, it is imperative that federal courts find a way to read computer crime statutes and not get lost in the temporary geography of the computer world. To avoid interpreting criminal laws in ways that will quickly become obsolete, or worse, counter-productive, courts should avoid making decisions based on technological realities that are not directly and obviously relevant to the issue before it. Therefore, if there is ambiguity in a computer crime statute, and there is no specific requirement for the court to examine the design of the underlying technology, courts should apply the black box canon of construction.

A black box is "[a] device or theoretical construct with known or specified performance characteristics but unknown or unspecified constituents and means of operation."[79] Computer programmers use the black box construct frequently in designing applications. Programmers often write computer code in parts, called modules or objects, with different programmers potentially working on each part. Each programmer may be unaware of how another module of code works when he is working on his part of the code. He only knows what information he needs to give the module and what information will come out of it. The other modules of code he uses are black boxes. For example, if a programmer needed to multiply every number in a series by a random number to encrypt data, he could use an existing randomizer program to do it. His program sends the series of numbers to the randomizer, and the randomizer spits out a series of new numbers. The programmer has no idea what the underlying programming for the randomizer looks like.

In the real world, people treat objects as black boxes all the time. Most people have no idea how a phone sends their voices through wires

79. THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (4th ed. 2007), *available at* http://www.answers.com/topic/black-box-theater.

to another person, or how a television gets images from a TV station. Nor do most people know how e-mail works or how L.L. Bean receives online orders.[80] Moreover, most people do not care.

When interpreting computer crime statutes using the black box canon of construction, the first task is to figure out exactly where the edges of that black box should be. To accomplish this, courts should apply real world analogies to the computer system at issue. When the analogous real world crime would not care about the particular details of the underlying technology, neither should the cybercrime.[81] Once the analysis passes this threshold, no further examination of the technology should occur.

A real world analogy looks at computer programs as having equivalent objects or systems in the real world. For example, e-mail is the equivalent of real or "snail" mail as well as shopping online at www.llbean.com is analogous to shopping by mail through their catalog. Not everything in cyberspace has a ready real world analogy, but most things do. Real world analogies are not just a tool for lawyers to use when interpreting the law, but they are also the modeling clay that programmers use in designing computer systems. E-mail could just as easily have been called e-speak or e-communicate, but the real world analogy to use e-mail was obvious and intentional. Real world analogies may not always be an exact fit, but they can help courts avoid examining irrelevant and fleeting technology when applying computer crime statutes. Applying real world analogies to computer crime statutes using the black box canon of construction has the added advantage of allowing both nontechnical and technical people to be able to understand what a computer crime law covers.

In the *Steve Jackson Games* and *Councilman I* decisions, the black box canon of construction would have prevented the courts from connecting the underlying technology to the dubious assertion that Congress wanted to protect e-mail at rest less than e-mail in motion. In the real world, the law protects postal mail from the moment it goes into a mailbox, until the intended recipient opens it.[82] The law protects postal mail regardless of whether it changes hands multiple times, flies, drives, or walks any part of its journey.[83] Similar to postal mail, e-mail should

80. *Hansell*, *supra* note 6; *see also Kerr*, *supra* note 47, at 361.

81. *See Gilboe*, 684 F.2d at 238 (holding that the electronic means by which money was transported is irrelevant); *Thomas*, 74 F.3d at 707 (holding the same for pictures).

82. *See, e.g.*, 18 U.S.C. § 1702 (2007); *Hill*, 579 F.2d at 482 (stating "until the addressee or his authorized agent received the mail, [federal protections] applied" (citing Maxwell v. United States, 235 F.2d 930, 932 (8th Cir. 1956))).

83. *Hill*, 579 F.2d at 482.

be treated the same when interpreting the ECPA.[84] This would result in a simple, more appropriate, and just end in these cases.

In *Steve Jackson Games*, the court only protected e-mail until it reached the intended recipient's mailbox, because they were looking at the underlying technology.[85] By protecting the e-mail from the moment the author of the letter "dropped it in the mailbox" by hitting the send button until the recipient actually opened the letter as a black box, the court would have respected the intent and plain meaning of the statute. Doing so would have prevented the court from considering whether the e-mail was at rest or in motion. It also would have prevented the court's decision from becoming technologically obsolete within less than a decade.

In *Councilman I*,[86] applying the black box canon of construction would have prevented the court from considering whether the e-mail was at rest or in motion before Councilman read it. Again, from a real world analogy perspective, whether mail stops in between placement into a mailbox and the opening by the intended recipient is irrelevant.[87] Because the black box prevents the court from examining the store and forward e-mail method, the court would not have been able to support a decision removing stored and forwarded e-mail from the Wiretap Act's protections. Left with the defendant's actions, reading people's e-mails before they had opened them, the court would have had to find that Councilman could have conspired to intercept his subscribers' e-mails.

IV. CONCLUSION

The black box canon of construction can help the judiciary interpret computer crime laws. In the end, it is the job of the judiciary to interpret computer crime laws. As demonstrated, investigation of the morally irrelevant workings of information systems can lead courts to undermine the intent of the law and deny criminal defendants fair warning. Computer systems change frequently and in unpredictable ways. How computer systems change is often irrelevant or unknown to the people who use them. The courts must be aware of this when interpreting computer crime laws. They must be prepared to limit their evaluations of technology using a standard that respects congressional intent and gives potential criminal defendants' fair warning. The black box canon of construction can help the courts do this.

---

84. *See generally Gilboe*, 684 F.2d at 238 (holding that the electronic means by which money was transported is irrelevant); *Thomas*, 74 F.3d at 707 (holding the same for pictures).

85. *Steve Jackson Games, Inc.*, 36 F.3d at 457.

86. *Councilman I*, 373 F.3d at 197.

87. 18 U.S.C. § 1702 (2007).