COMMENT

Can the Eye Be Guilty of a Trespass? Protecting Noncommercial Restricted Websites After *Konop v. Hawaiian Airlines*

*W.M. Motooka**

TABLE OF CONTENTS

* Executive Editor, U.C. Davis Law Review. J.D. Candidate, U.C. Davis School of Law, 2004.

INTRODUCTION

In the famous case of *Boyd v. United States*, the United States Supreme Court acknowledged that "the eye cannot by the laws of England be guilty of a trespass."[1] Recently, the Supreme Court, citing *Boyd*, reaffirmed the long-standing innocence of the inquiring human eye under the laws of the United States.[2] But with the advent of the internet, it may now be time to hold the eye accountable for trespass. Suppose a person were to create a website through which to share news and pictures of her family: births, deaths, weddings, graduations, family vacations, illnesses, successes, failures, etc. She may not want this website to be open to the general public. She may want only authorized users to have access to it, most likely family members and close friends, dispersed across the country or overseas. She could protect the site from strangers by requiring users to type in a valid password before entering. Yet skillful computer users may be able to deliberately defeat her security measures, and view her website without her permission. If they do so, have their eyes trespassed?

The law has had difficulty adapting to the evolving technology of the internet, particularly in the area of internet property rights.[3] Currently, no clear law governs the boundaries of electronic trespass ("e-trespass").[4] Courts have considered the question of e-trespass under a variety of theories, including copyright, misappropriation, trademark dilution, computer fraud, unfair competition, breach of contract, unjust enrichment, and by analogy to trespass to land and trespass to chattel.[5]

---

[1] 116 U.S. 616, 628 (1886) (citing Entick v. Carrington, 95 Eng. Rep. 807 (K.B. 1765)) (protecting defendant's private business papers from government's prying eyes).

[2] Kyllo v. United States, 533 U.S. 27, 34-35 (2001) (finding that thermal imaging device, directed at residence, constitutes search).

[3] *See, e.g.*, Maureen A. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 BERKELEY TECH. L.J. 561, 562-65 (2001); Laura Quilter, *Cyberlaw: Regulating Conduct on the Internet*, 17 BERKELEY TECH. L.J. 421, 423 (2002). *See generally* STUART BIEGEL, BEYOND OUR CONTROL? CONFRONTING THE LIMITS OF OUR LEGAL SYSTEM IN THE AGE OF CYBERSPACE 123-86 (2001) (discussing recent developments in cyberspace law in last decade).

[4] O'Rourke, *supra* note 3, at 580-97; Quilter, *supra* note 3, at 435-44.

[5] O'Rourke, *supra* note 3, at 581-97; *see* Ticketmaster Corp. v. Tickets.com, Inc., No. CV 99-7654 HLH(BQRX), 2000 WL 525390, at *1 (C.D. Cal. Mar. 27, 2000) (litigating unauthorized use of "spiders" to aggregate pricing data as copyright infringement, breach of contract, unjust enrichment, misappropriation, and trespass); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 241 (S.D.N.Y. 2000) (litigating unauthorized collection and use of user data as trespass to chattels, breach of contract, computer fraud, and trademark confusion in violation of Lanham Act); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1063 (N.D. Cal. 2000) (litigating unauthorized use of spider to aggregate pricing data under trespass, false advertising, trademark dilution, computer fraud, unfair competition,

Most of these e-trespass cases have addressed unwanted electronic access in a commercial context.[6] Accordingly, the analyses of these cases have focused on the often conflicting interests of protecting the property of business owners, benefiting consumers, and maintaining the internet as a public "commons."[7] Website privacy, as a value in and of itself, has not yet figured into the analysis.[8] If no commercial interest is at stake, it is unclear whether a website owner has any enforceable right against unwanted visitors.[9] Yet noncommercial restricted websites may serve useful social purposes, such as keeping family members abreast of family news, or hosting confidential online support groups for people who might otherwise never meet.[10] An enforceable expectation of

---

misappropriation, and unjust enrichment).

[6] *See* TicketMaster Corp. v. Tickets.com, Inc., No. 99 CV 7654, 2000 WL 1887522 (C.D. Cal. Aug. 10, 2000) (addressing unauthorized use of "spiders" to aggregate pricing data for tickets to entertainment events); *eBay*, 100 F. Supp. 2d 1058 (addressing unauthorized use of "spiders" to aggregate pricing data for auction website); *Register.com*, 126 F. Supp. 2d 238 (addressing unauthorized use of "spiders" to generate marketing list for provider of web hosting services); CompuServe v. Cyber Promotions, 962 F. Supp. 1015 (S.D. Ohio 1997) (addressing "spamming," or sending of unsolicited bulk e-mail); Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468 (Ct. App. 1996) (litigating unauthorized access to phone lines).

[7] *See* Dan L. Burk, *The Trouble With Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 54 (2000) (warning that applying trespass theory to protect internet property may result in unproductive "anti-commons"); O'Rourke, *supra* note 3, at 563-67 (discussing whether aggregators of pricing data should first secure permission before engaging in internet data collection).

[8] As website technologies and uses become more widespread, the law may redefine the protections available. *See* Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (discussing need to develop new privacy law in face of new technologies). On the current state of internet privacy law, see RICHARD A. SPINELLO, REGULATING CYBERSPACE: THE POLICIES AND TECHNOLOGIES OF CONTROL 175-204 (2002) (discussing privacy rights and internet, and recommending private self-regulating solutions rather than governmental regulation).

[9] *See infra* Part II.

[10] The internet is already being used to organize support groups. An internet Google search for "support group" yields numerous hits, see, for example, SupportPath.com, *at* http://www.supportpath.com (last visited Oct. 8, 2003) (directory for numerous support-related online communications); Androgen Insensitivity Syndrome Support Group, *at* http://www.medhelp.org/www/ais/01_INTRO.HTM (last modified July 28, 2002) (consortium of worldwide support groups concerning testicular feminization syndrome); Mood Disorders Support Group of New York City, *at* http://www.mdsg.org (last visited Oct. 8, 2003) (self-help organization concerning depression and manic-depression); Pick's Disease Support Group, *at* http://www.pdsg.org.uk (last visited Oct. 8, 2003) (support group concerning frontotemporal dementia); PPD Support Group, at http://www.ppdsupport.com (last visited Oct. 8, 2003) (support group concerning postpartum mood disorders); Premature Ovarian Failure Support Group, *at* http://www.pofsupport.org (last visited Oct. 8, 2003) (support group concerning premature ovarian failure); Unique: Rare Chromosome Disorder Support Group, *at*

privacy may facilitate such beneficial uses of the internet.

This Comment discusses the legal theories currently available to protect the privacy of noncommercial restricted websites. By "noncommercial restricted website," I mean websites, not operated as a business for profit, that use technological security measures (such as passwords or licensing agreements) to limit user access. I argue that current law inadequately protects these websites. Part I defines the problem of website trespass as it arose recently in *Konop v. Hawaiian Airlines*.[11] The *Konop* case involved an airline employee who created a website specifically for fellow employees, and specifically not for management.[12] Konop's fitful journey through the federal court system illustrates the difficulty of identifying a proper legal action for e-trespass.[13] Part II discusses the applicability of contract law, tort law, and the federal Electronic Communications Privacy Act,[14] and describes why these laws do not deter website trespass. Finally, Part III proposes that Congress amend the federal Electronic Communications Privacy Act to clarify and augment the protections available to website owners.

I. BACKGROUND

A. Website Security and Konop v. Hawaiian Airlines, Inc.

Pilot Robert Konop was displeased with his employer, Hawaiian Airlines ("Hawaiian"), and his labor union, the Air Line Pilots Association ("ALPA").[15] To express his dissatisfaction to his fellow employees, he created and maintained a website critical of Hawaiian, its officers, and ALPA.[16] To control access to the site, Konop created a list of the website's eligible users, mainly pilots and other employees.[17] This list specifically excluded Hawaiian's management.[18]

---

http://www.rarechromo.org (last visited Oct. 8, 2003) (support group for families of children with rare chromosome disorders).

[11] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002).

[12] *Id.* at 872-73.

[13] *See* Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035 (9th Cir. 2001), *withdrawn and pet. for reh'g en banc mooted by* 262 F.3d 972 (9th Cir. 2001), *aff'd in part, rev'd in part* 302 F.3d 868 (9th Cir. 2002), *cert. denied*, 537 U.S. 1193 (2003).

[14] Electronic Communications Privacy Act, Pub.L. No. 99-508, 100 Stat. 1848 (1986).

[15] *Konop*, 302 F.3d at 872.

[16] *Id.*

[17] *Id.*

[18] *Id.* at 873.

Konop secured the site with a "clickwrap" or "web wrap" licensing agreement[19] that informed visitors of the site's terms and conditions of use.[20] The website allowed entry only when a visitor typed in the name of an eligible user, created a password, and then agreed to the site's terms and conditions by clicking on a "SUBMIT" button.[21] The terms

---

[19] Clickwrap or web wrap licensing agreements are commonly used by software vendors. Typically, a clickwrap license displays the software's terms of use on the computer screen the first time a user operates the software. To proceed, a user must accept the terms by clicking on a "yes" button or taking some other specified action. *See* Stephen T. Keohane, *Mass Market Licensing*, 704 PLI/PAT 269, 277 (2002) (discussing different types of mass-market licenses and their enforceability); Margaret Jane Radin, *Retooling Contract for the Digital Era*, *in* PUBLIC POLICY AND THE INTERNET: PRIVACY, TAXES, AND CONTRACT 115, 122-26 (Nicholas Imparato ed., 2000) (discussing contractual infrastructure for e-commerce).

[20] *Konop*, 302 F.3d at 872-73. Before visitors could enter the site, they saw a screen that warned:

> This is the gateway for NEWS UPDATES and EDITORIAL COMMENTS directed only toward Hawaiian Air's pilots and other employees, not including HAL management. By entering, you acknowledge and agree to the terms and conditions of use as specified below. You must read this entire page before entry. Others should simply find *something else* to do with their time.
>
> If you are already a registered user, you may fill in your name along with the other information required below, then enter the system. If you want to visit the system, and you belong to the authorized group, you must supply the proper information before you will be allowed to enter. Make note of the password you enter for your first visit, otherwise future visits may be delayed. Visits by others will be strictly prohibited.

Below this text were boxes into which visitors type their names and passwords, followed by a choice between clicking on one of two buttons, either "SUBMIT" or "CLEAR." The warning then continued:

> . . . All name and contact information will be kept strictly confidential. Any effort to defeat, compromise or violate the security of this website will be prosecuted to the fullest extent of the law.
>
> WARNING!
>
> The information contained herein is CONFIDENTIAL, and it is not intended for public dissemination! By requesting entry in the system, you must agree not to furnish any of the information contained herein to any other person or for any other use. Republication or redistribution of this information to any other person is strictly prohibited. Anyone found to disseminate this information to anyone other than those specifically named and allowed here will be banned from this website and held liable to prosecution for violation of the terms and conditions of use and for violation of this contract.

Id. at 876 n.3.

[21] *Id.* at 872-73.

specified that only members of the authorized group were welcome, and that users could not reveal to anyone the contents of the site.[22]

In December of 1995, Hawaiian vice-president James Davis began to log onto the site, using the name of pilot Gene Wong.[23] Wong, who was eligible to enter the site, had permitted Davis to use his name.[24] Later that day, Konop received a call from ALPA chairman, Reno Morella.[25] Morella allegedly told Konop that Hawaiian president Bruce Nobles was upset at the accusations and disparaging statements contained on Konop's website.[26] At first, Konop did not know how Nobles could have viewed the site. Eventually, after studying the system logs, Konop realized that Davis had entered the site by using Wong's name.[27]

Davis continued to access the site through April 1996.[28] According to Konop's records, Davis logged on over twenty times as Wong, and at least fourteen times as another pilot, James Gardner.[29] Gardner had also given Davis permission to use his name.[30]

Konop filed suit against Hawaiian, alleging several claims, including violations of the federal Wiretap Act and the Stored Communications Act ("SCA").[31] The federal district court for the District of Hawai'i granted summary judgment to Hawaiian on these two claims, and Konop appealed.[32] In January 2001, the Ninth Circuit reversed the summary judgment for Hawaiian. The circuit court found that Konop's complaint had raised triable issues of fact under the federal Wiretap Act and under the SCA.[33] Hawaiian filed a petition for rehearing, which was mooted when the court withdrew its opinion in August 2001.[34] One year later, in August 2002, the court issued a revised opinion, affirming the district court's ruling on the Wiretap Act claim, but reversing on the SCA

---

[22] *Id.* at 873.

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] Wiretap Act, 18 U.S.C. §§ 2510-2522 (2000); Stored Communications Act, 18 U.S.C. §§ 2701-2711 (2000). Konop's other claims arose from the Railway Labor Act and state tort law. *Konop*, 302 F.3d at 872.

[32] *Konop*, 302 F.3d at 873.

[33] Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035, 1048 (9th Cir. 2001), *vacated by* 302 F.3d 868 (9th Cir. 2002).

[34] *Konop*, 302 F.3d at 872.

claim.[35]

In reaching its revised opinion, the Ninth Circuit first noted that rapid technological innovation has created confusion and uncertainty in cyberspace law.[36] Statutes written with a mind to older forms of technology, such as telephones, are ill-suited to modern internet communications.[37] In reaching its revised ruling, the court confronted the difficulty of this poor statutory fit.[38] The main difference between the withdrawn opinion and the reissued opinion lay in the court's analysis of the word "interception."[39] Specifically, the court revisited the question of how to apply the telephone-era definition of "interception" to the computer-age reality of electronic communications.[40]

The Wiretap Act prohibits the intentional "interception" of wire, oral, and electronic communications.[41] The court readily determined that Konop's website was an "electronic communication."[42] It wrestled, however, with the meaning of "interception" as applied to the stored electronic communications on Konop's site.[43] The court observed that by statutory definition, "interception" could mean "acquisition of the contents" of electronic communication.[44] Yet case law, the court noted, has narrowly construed "interception" to mean "acquisition of a communication contemporaneous with transmission."[45] The question, therefore, was whether this contemporaneity requirement meant that the Wiretap Act could never protect *stored* electronic communications, such

---

[35] *Id.* at 886.

[36] *Id.* at 874.

[37] *Id.*

[38] *Id.* (observing that "the existing statutory framework is ill-suited to address modern forms of communication like Konop's secure website").

[39] *Compare* Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035, 1042-46 (9th Cir. 2000) (holding that stored electronic communications can be "intercepted") *with Konop*, 302 F.3d at 876-79 (finding that stored electronic communications cannot be "intercepted").

[40] *See supra* note 39.

[41] *Konop*, 302 F.3d at 876. The relevant statute is 18 U.S.C. § 2511(1)(a) (2000).

[42] *Konop*, 302 F.3d at 876.

[43] *Id.* at 876-79.

[44] *Id.* at 876.

[45] *Id* at 876-77. The court relied on *United States v. Smith*, 155 F.3d 1051 (9th Cir. 1998) (finding narrow definition of "intercept" appropriate with regard to electronic communications), *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994) (holding that government's acquisition of e-mail stored on electronic bulletin board system, but not yet retrieved by intended recipients, was not "interception" under Wiretap Act), and the clarification of Congress' intent evident in the recently enacted USA Patriot Act, section 209, 115 Stat. at 283 (amending Wiretap Act to eliminate stored voice-mail from definition of wire communication, thereby reducing protection of voice mail to lower level of protection provided other electronically stored communications).

as websites, because communications in storage are, by definition, not in transmission.[46]

Further confusing the issue was a 1986 amendment to the federal Wiretap Act that explicitly extended the statute's protection to stored wire communications such as voice-mail.[47] Logic would suggest that either interception cannot require contemporaneity with transmission, or the Wiretap Act cannot apply to stored electronic communications.[48] Nonetheless, the plain language of the amended statute indicated Congress' intent to protect stored wire communications from "intercept."[49]

The Ninth Circuit's reissued opinion reconciled this apparent inconsistency by distinguishing the protections Congress created for wire communications from those that Congress created for electronic communications.[50] The court recognized that the narrow definition of "intercept," which requires contemporaneous acquisition, leaves electronic communications virtually unprotected.[51] Electronic communications travel between users at the speed of light, and are stored in various servers along the way.[52] It is practically impossible to acquire an electronic communication contemporaneously with its transmission, making protection under the Wiretap Act illusory.[53] The

---

[46] *Konop*, 302 F.3d at 887 (Reinhardt, J., concurring in part, dissenting in part).

[47] *Id.*

[48] In the words of Judge Reinhardt:

> The majority's reading of the statute simply doesn't work: while explicitly holding that stored electronic communications are within the term "electronic communications" and that the intercept prohibition of the Wiretap Act applies to electronic communications, it also explicitly holds that interception of electronic communications is limited to contemporaneous acquisition, thereby *simultaneously* including and excluding stored electronic communications from the intercept prohibition.

Id. at 888.

[49] The need to reconcile the meaning of "intercept" with the definition of "stored electronic communications" has since been obviated by Congressional amendment of the Wiretap Act. As the court noted, the USA Patriot Act section 209, 115 Stat. at 283, eliminated stored communications from the scope of the Act. *Konop*, 302 F.3d at 878.

[50] *Konop*, 302 F.3d at 878.

[51] *Id.* at 879 n.6.

[52] *Id.*; *see* Tatsuya Akamine, Note, *Proposal for a Fair Statutory Interpretation: E-mail Stored in a Service Provider Computer is Subject to an Interception Under the Federal Wiretap Act*, 7 J.L. & POL'Y 519, 561-65 (1999) (noting that transmission of electronic communications requires storage); Jarrod J. White, *E-Mail@Work.Com: Employer Monitoring of Employee E-mail*, 48 ALA. L. REV. 1079, 1083 (1997) (noting that temporary storage follows transmission of electronic communications almost immediately).

[53] *Konop*, 302 F.3d at 879 n.6. In other words, under the narrow definition of the term,

court concluded that Congress intended this illusory protection: "Congress chose to afford stored electronic communications less protection than other forms of communication."[54]

Having found the Wiretap Act inapplicable to Konop's case, the court next considered what protections, if any, Konop might expect under the SCA.[55] The SCA provides criminal and civil penalties for persons who "intentionally access[] without authorization a facility through which an electronic communication service is provided."[56] The statute creates some exceptions, however. Under 18 U.S.C. section 2701(c)(1), liability does not attach if the service provider authorizes access to the electronic communications. Nor does liability attach, under 18 U.S.C. section 2701(c)(2), if a service user authorizes access to "a communication of or intended for that user."[57]

The district court's ruling relied on the exception contained in section 2701(c)(2) when it ruled in Hawaiian's favor on the SCA claim.[58] The district court found that because Wong and Gardner had consented to Davis's use of their names, Davis's access to Konop's site was proper under section 2701(c)(2).[59] The district court reasoned that Wong and Gardner were "users" of Konop's "service," because Konop had made them eligible to visit his website.[60] Furthermore, the communications on the site were "intended" for them.[61] The district court therefore concluded that under 18 U.S.C. section 2701(c)(2), Wong and Gardner had the authority to permit Davis's use of the site.[62]

On review, the Ninth Circuit acknowledged that the district court's holding was consistent with other parts of the Wiretap Act and the

---

to "intercept" internet communications requires the interceptor to catch the communication as it pulses across the wires that connect servers, and not while the information is stored at its final destination or in intermediate servers along the way. *Id.*

[54] *Id.*; *see also* Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (finding that electronic communications by definition cannot be "intercepted" while in electronic storage).

[55] *Konop*, 302 F.3d at 879. The relevant SCA provision is 18 U.S.C. § 2701(a)(1) (2000).

[56] 18 U.S.C. § 2701(a)(1). The offense, if committed for commercial advantage, malicious destruction, or private commercial gain, is punishable by fine or imprisonment, either as a misdemeanor or as a felony. *Id.* § 2702(b). Civil damages may include equitable relief, actual damages, punitive damages, and reasonable attorney's fees. *Id.* §§ 2702(b), 2707(c).

[57] *Id.* § 2701(c)(2).

[58] *Konop*, 302 F.3d at 880.

[59] *Id.*

[60] *Id.*

[61] *Id.*

[62] *Id.*

SCA.[63] Both acts allow intended recipients of electronic communications to permit access to third-party users.[64] The court further noted that the legislative history indicated that Congress presumed intended recipients of electronic communications would have the authority to permit third-party access to those communications.[65] The circuit court, however, did not accept the district court's equation of "users" with "eligible users."[66]

The Ninth Circuit rejected the district court's reasoning because of the unambiguous and controlling language of section 2701(c)(2).[67] The statute defines "user" as one who "uses" the service with proper authorization.[68] Because the statute does not define the word "use," the circuit court applied the ordinary, dictionary definition of "use" as "to put into action or service, avail oneself of, employ."[69] Accordingly, the court distinguished between *actual* "users" under the dictionary definition, and those who were merely *eligible* to use.[70]

Turning to the record, the court found no evidence that Wong had ever used Konop's website.[71] It further found that Gardner may have used the site, but it could not establish whether that use occurred before or after Gardner permitted Davis to use his name.[72] The court concluded that the district court erred in presuming that Wong and Gardner were "users" based solely on the fact that Konop had made them eligible to use the website.[73] The problem with the district court's approach, the circuit court stated, is that it reads the "user" requirement out of section 2701(c)(2).[74] Properly construed, section 2701(c)(2) permits a person to authorize third-party access to an electronic communication only if: 1) the person is an actual "user" of the service, and 2) the communication was intended for that user.[75] Because the record did not establish that Wong and Gardner were "users," the Ninth Circuit reversed the district court's summary judgment in favor of Hawaiian on the SCA claim, and

---

[63] *Id.*

[64] *Id.*

[65] *Id.* n.9.

[66] *Id.* at 880.

[67] *Id.*

[68] *Id.*

[69] *Id.*; *see also* WEBSTER'S NEW COLLEGIATE DICTIONARY 1299 (9th ed. 1985).

[70] *Konop*, 302 F.3d at 880.

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] *Id.*

remanded the case for further proceedings.[76]

B. Intended Users, the Intentions of Providers, and Authorized Use

The district court now may have to determine whether Wong and Gardner were "users." If Wong and Gardner were "users," with authority to permit third-party access to the website, then Hawaiian has no liability under the SCA. To reach this conclusion, however, the court must analyze two distinct and difficult questions: first, what constitutes a "user," and second, whether the SCA gives all "users" a non-negotiable right to permit third-party access to electronic communications.

The meaning of "user" is simple in theory, but fuzzy in fact. It is unclear exactly what activities would be sufficient to turn Wong and Gardner into "users" of Konop's website. Would a single visit to the site make Wong and Gardner "users"? Or would the pilots have to show a frequent and/or regular pattern of use in order to be "users"? If a single visit is sufficient, would it matter what the duration or nature of that visit was? For example, would the pilots' visit to the website have to be long enough to allow them to read its contents? Would the pilots actually have to read the contents? Would they have to read the entire site, or only some of it? Would it matter whether the pilots visited and read the site for a purpose other than that contemplated by Konop?

Once the district court determines the definition of a user, it must next decide whether the section 2701(c)(2)'s liability exception inexorably follows, or whether the presence of Konop's protective clickwrap license curtailed users' legal rights under the SCA.[77] The Ninth Circuit stated that the plain language of section 2701(c)(2) establishes that a user of an electronic communication service can authorize third-party access to the electronic communications.[78] According to the Ninth Circuit, the

---

[76] *Id.* at 886.

[77] At least one of the websites mentioned, *supra* note 10, attempts, like Konop, to use pop-up licensing in order to shape its legal relation to its users. Before signing onto the member discussion forums at Unique: Rare Chromosome Disorder Support Group, *at* http://www.rarechromo.org (last visited Oct. 8, 2003), the user must agree to the site's terms and conditions of use. These terms are available at http://www.rarechromo.org /forum/ShowTermsAndConditions.asp. The specific terms on this site do not seek to enforce a privacy requirement. Rather, they require users to abide by certain rules of conduct, and to accept all risks associated with using or relying on the content of the site, including the consequences of publishing personal information. Like Konop's site, this site's licensing agreement requires users to give up some of their legal rights in exchange for access to the website. Would the Unique website license be enforceable, while Konop's is preempted?

[78] *Konop*, 302 F.3d at 880.

statute's legal definition of "user" has two elements: a person must 1) actually use the service, 2) while duly authorized to do so.[79] If Wong and Gardner, as eligible users, had in fact used Konop's website prior to authorizing Davis's visits, one might conclude that Davis's use of the site falls properly within section 2710(c)(2)'s liability exception. If Wong and Gardner are users, then they may authorize third-party access under the SCA.

This conclusion, however, presumes that Konop's clickwrap license had no legal effect concerning the definition of user.[80] In other words, it presumes that the SCA preempts the terms of Konop's clickwrap license. No existing legal theory requires this presumption. Konop's license takes the form of a contract. In clear and definite terms, the license offered access to the website in exchange for two promises.[81] Visitors had to assert truthfully that they were members of the authorized group, and they had to agree not to "furnish" the site's contents to anyone else.[82] No one could enter the site without first receiving notice of these terms, and affirmatively assenting to them by clicking the "SUBMIT" button.[83] Thus, if Wong and Gardner had ever entered the site, they must have accepted the site's terms and conditions of use, including the restriction on revealing its contents to third parties. Under the terms of Konop's license, the website is intended only for those users who waive their right to authorize third-party use. The SCA, however, does not contemplate this type of arrangement. Instead, section 2701(c)(2) presumes that all intended users of communications have the power to authorize third-party access.[84]

The question boils down to whether the SCA preempts or merely supplements privately contracted definitions of authorized use. If section 2701(c)(2) preempts contract law, then service providers can

---

[79] *Id.*

[80] The court expressly stated that the meaning of "without authorization," in the context of a nonpublic site like Konop's, was not a question currently before the court. *Id.* at 880 n.8. The court chose to address only the narrower question of whether Hawaiian was exempt from liability under section 2701(c)(2), which permits intended users of communications to authorize third-party access. Yet if Konop's clickwrap license is valid, then the questions are indistinguishable. As will be discussed more fully below, the license designated the website's intended users as only those users who agree to the site's terms and conditions of use. *Supra* note 20. Since Wong and Gardner did not abide by the site's terms and conditions, their access would appear to be unauthorized under the license.

[81] *Konop*, 302 F.3d at 876 n.3.

[82] *Id.*

[83] *Id.*

[84] 18 U.S.C. § 2701(c)(2) (2000).

never restrict users from permitting third-party use of electronic communications. If, however, the SCA's definitions are just the default terms, then parties may reach their own agreements concerning the meaning of "authorized use" under section 2701(c)(2). The policy question is whether the SCA should enforce a uniform meaning of "authorized use," or whether it should enforce many different meanings, as defined by private parties through contract.

If the uniform-meaning view of the SCA prevails, giving all electronic communications users the non-negotiable right to permit third-party access to the communications, then the term "noncommercial restricted websites" is an oxymoron. Without protection under the SCA, owners of noncommercial sites have virtually no legally enforceable means by which to keep their sites restricted.[85] Currently, website privacy may be enforced through actions brought under contract law, common law trespass, and the SCA.[86] The following part discusses these legal approaches, and why they provide inadequate protection for noncommercial websites.

II. LEGAL PROTECTIONS FOR WEBSITE CONTENT

Plaintiffs have pursued e-trespass claims under contract law, common law trespass, and the SCA. As the section below argues, none of these approaches offer sufficient protection for noncommercial websites. Contract law tends to protect only financial interests in websites. Trespass is simply a poor fit in the website context. Trespass protects lands against continuous trespass and chattels against trespass that causes impairment; e-trespass, however, tends to occur as a continuous trespass to chattels that causes no discernible impairment. Finally, the

---

[85] The SCA contains an exclusivity of remedies provision, limiting the remedies available for claim based on conduct regulated by the statute. *Id.* § 2708. One district court has held that the ECPA preempts state-law claims based on conduct regulated by the ECPA. Muskovich v. Crowell, 1995 WL 905403 (S.D. Iowa 1995) (holding that ECPA preempts state-law intentional infliction of emotional distress claim based on obscene phone calls made to unlisted telephone number acquired in violation of ECPA). If the statute is so broadly preemptive, and its definitions are frozen by the statutory text, it is doubtful that its remedies will be able to keep up with fast developing technologies and the conduct they enable.

[86] *See* Burk, *supra* note 7 (suggesting new theory of digital nuisance to resolve computer access disputes); Raymond T. Nimmer, *New Property Rights and E-Commerce*, 697 PLI/PAT 9 (discussing available property rights in information age); O'Rourke, *supra* note 3 (recommending more flexible property rules with respect to website than those traditionally applied to real property); John D. Saba, Jr., Comment, *Internet Property Rights: E-Trespass*, 33 ST. MARY'S L.J. 367 (2002) (discussing need for internet property rights).

scope of the SCA's protection is uncertain, given the question raised in *Konop* concerning the legal meaning of "authorized user."

A. Contract Law and Clickwrap Licensing Agreements

Commercial websites enjoy the protection of contract law via clickwrap licensing agreements.[87] A clickwrap license displays a message on the user's computer screen, requiring the user to assent to the terms of the licensing agreement by clicking on an icon.[88] Users may not obtain the product until they manifest acceptance of the terms by clicking on the icon.[89] The courts that have considered clickwrap licenses have found them to be enforceable contracts.[90]

1. *ProCD v. Zeidenberg* and the Binding Commercial Clickwrap License

Clickwrap licenses first gained legal recognition as enforceable contracts seven years ago in *ProCD v. Zeidenberg*.[91] In *ProCD*, the Seventh Circuit upheld the validity of software licensing agreements that restrict the licensee's authority to share the product with other users.[92] Defendant Zeidenberg had bought plaintiff ProCD's database of phone numbers and addresses, and had then resold the information over the internet for commercial gain.[93] ProCD argued that its software's licensing agreement prohibited Zeidenberg's conduct.[94] Zeidenberg argued that the contract was not binding because the terms of the licensing agreement were hidden at the time of purchase; they were not

---

[87] *See* Raymond T. Nimmer, LAW OF COMPUTER TECHNOLOGY § 14:87 (4th ed. 2003).

[88] Specht v. Netscape Communications Corp., 150 F. Supp. 2d 585, 594-95 (2001), *aff'd*, 306 F.3d 17 (2d Cir. 2002).

[89] *Id.*

[90] *Id.* at 594; *see* I. Lan Sys., Inc. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328 (D. Mass. 2002) (holding that under Massachusetts law, clickwrap license is enforceable contract); *In re* RealNetworks, Inc., Privacy Litigation, 2000 WL 631341 (N.D. Ill. May 8, 2000) (holding that arbitration clause included in licensing agreement on website is enforceable); Hotmail Corp. v. Van$ Money Pie, Inc., 1998 WL 388389 (N.D. Cal. Apr. 16, 1998) (stating that licensing agreement requiring e-mail subscribers to refrain from "spamming" is likely enforceable); M.A. Mortenson Co. v. Timberline Software Corp., 998 P.2d 305 (2000) (holding that, under Washington law, licensing terms that appear on screen before software is run become part of contract between buyer and seller, if buyer continues to use software); *see also* Ryan J. Casamiquela, *Contractual Assent and Enforceability in Cyberspace*, 17 BERKELEY TECH L.J. 475 (2002) (discussing online licensing agreements and their enforceability).

[91] ProCD v. Zeidenberg, 86 F.3d 1447, 1449 (1996).

[92] *Id.*

[93] *Id.* at 1450.

[94] *Id.*

printed on the outside of the product's packaging.[95] The terms were enclosed in the packaging, however, and they did appear on the computer screen each time the software ran.[96]

The Seventh Circuit, on appeal, ruled that the license was valid and binding.[97] Though Zeidenberg did not know the exact terms of the license at the time of purchase, he did know that the product was subject to a license.[98] Moreover, Zeidenberg did not return the product for a refund after opening the software and discovering its specific terms. The court found that under these circumstances, Zeidenberg had assented to the terms.[99]

In reaching its decision, the circuit court emphasized the necessity of protecting business interests through licensing agreements.[100] The court observed that ProCD had spent more than ten million dollars to compile the database, and that it continued to spend large sums to keep the database current.[101] The court reasoned that ProCD's profitability depended on the company's capacity to engage in price discrimination between commercial and noncommercial buyers.[102] The company relied on charging its commercial customers more than its noncommercial customers, but would be unable to do so if the noncommercial buyers could resell the database.[103] The "institution of contract" was ProCD's means of preventing noncommercial buyers from reselling the database to commercial buyers.[104] Accordingly, the court enforced ProCD's license because ProCD could not remain profitable without it.[105]

2. Clickwrap Licenses in the Noncommercial Context

Since *ProCD*, several other courts have upheld the validity of commercial clickwrap licenses.[106] These rulings would appear to protect a site like Konop's. Konop restricted his site using language that read

---

[95] *Id.*
[96] *Id.*
[97] *Id.* at 1451.
[98] *Id.* at 1450.
[99] *Id.* at 1451.
[100] *Id.* at 1449-50.
[101] *Id.* at 1449.
[102] *Id.* at 1449-50.
[103] *Id.* at 1450.
[104] *Id.*
[105] *Id.* at 1449-50.
[106] *See* sources cited *supra* note 90.

like a clickwrap license.[107] He offered access to the site in exchange for the visitor's promise not to disclose the site's contents, and he required the visitor to indicate assent by clicking on the "SUBMIT" button.[108] Yet the rationale of the *ProCD* holding does not squarely apply to Konop's site, because his clickwrap license did not protect socially valuable commercial profits.[109] Possibly, Konop's license may be unenforceable for lack of consideration.[110] Yet the greatest barrier to an effective contract action, however, would likely be the difficulty of finding an appropriate remedy for breach of a noncommercial website's licensing agreement.

The available judicial remedies for breach of contract are: 1) damages compensating for the injury caused by the breach, 2) restitution of a specific thing or payment for a performance rendered, and 3) specific performance.[111] Damages for emotional disturbance and punitive damages are generally not available for breach of contract.[112] If Konop's only remedies are damages, restitution, and specific performance, then even an enforceable licensing agreement may be insufficient to secure his site. Because his site is noncommercial, he may be unable to show

---

[107] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 n.3 (9th Cir. 2002). Konop's clickwrap agreement with his users would appear to satisfy the legal requirements necessary for the formation of an informal contract. *See* RESTATEMENT (SECOND) OF CONTRACTS § 19 (1981).

[108] *Konop*, 302 F.3d. at 876 n.3.

[109] The *ProCD* court's analysis of the licensing issue strongly emphasizes the public value of enforcing ProCD's license. *ProCD*, 86 F.3d at 1449. The court found that without the ability to engage in effective price discrimination between commercial users and the general public, ProCD would have to charge the general public substantially more. *Id.* ProCD's clickwrap license, the court reasoned, benefits consumers. *Id.*

[110] Consideration is performance or a return promise that was bargained for. RESTATEMENT (SECOND) OF CONTRACTS § 71 (1981). In *Specht v. Netscape Communications Corp.*, 150 F. Supp. 2d 585, 591 n.8 (S.D.N.Y. 2001), the court speculated that the downloading of free software, under a clickwrap license, might nonetheless support a finding of no contract, since a person who downloads software for free is giving nothing in return. Konop's website provided free information. On the other hand, courts have accepted the enforceability of a clickwrap license, despite the fact that the offered product was free. *See In re* RealNetworks, Inc., Privacy Litigation, 2000 WL 631341 (N.D. Ill. May 8, 2000) (holding that license pertaining to use of free software is enforceable); Hotmail Corp. v. Van$ Money Pie, Inc., 1998 WL 388389 (N.D. Cal. Apr. 16, 1998) (holding that license pertaining to use of free e-mail service is enforceable).

[111] RESTATEMENT (SECOND) OF CONTRACTS § 326 (1981).

[112] Recovery for emotional disturbance is not available under breach of contract unless the breach was of a nature such that serious emotional disturbance would be a particularly likely result. *Id.* § 353. The breach of contract action does not allow punitive damages unless the conduct constituting the breach is also a tort for which punitive damages are available. *Id.* § 355. As it is unclear whether a tort was committed against Konop, his breach of contract remedy may be limited to contract damages only.

money damages or any basis for restitution. An injunction for specific performance may be available once breach has already occurred, but it will do little to deter future unauthorized use by anyone other than the present defendants.[113] Because it provides no adequate remedy, contract law offers only illusory privacy protection for noncommercial website owners.

B. Remedies Under the Theory of Trespass

Like contract law remedies, the common law action of trespass also imperfectly fits the cyberworld. Common law trespass encompasses two distinct causes of action: 1) trespass to land, and 2) trespass to chattels.[114] Neither of these causes of action are fully analogous to the situation of internet trespass.[115]

Trespass to land may offer an effective cause of action through which to enforce internet property rights, because the cause of action protects the inviolability of the owner's right to exclude even harmless intrusions.[116] Under the trespass to land theory, website owners may sue successfully without having to calculate and demonstrate their injury.[117] Additionally, courts may award a preliminary injunction as a remedy for a continuing trespass to real property.[118]

Unfortunately, computers and computer systems are not real property; they are chattels, not land.[119] And the trespass to chattels cause of action provides a less effective remedy. First, the cause of action is available only to the possessors of chattels who can show actual injury caused by the trespass.[120] Second, legal authority seldom recognizes the appropriateness of a preliminary injunction against continuous trespass

---

[113] An injunction operates *in personam*, requiring a particular party to do or not do a particular thing. 1 HOWARD C. JOYCE, A TREATISE ON THE LAW RELATING TO INJUNCTIONS § 1, at 2-3 (1909).

[114] Quilter, *supra* note 3, at 424-30.

[115] *Id.*

[116] RESTATEMENT (SECOND) OF TORTS § 163 cmt.D (1965).

[117] On the difficulty of calculating damages resulting from cyber trespass, see eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1064-66 (N.D. Cal. 2000); Compuserve Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1027-28 (S.D. Ohio 1997); Burk, *supra* note 7, 34-37.

[118] *eBay*, 100 F. Supp. 2d at 1067.

[119] The difficulty in conceptualizing a website as property arises from its simultaneous status as a metaphorical place (a "site") and as a literal object (a computer program residing on a tangible server). *See* O'Rourke, *supra* note 3, at 580-81.

[120] RESTATEMENT (SECOND) OF TORTS § 218 (1965).

to chattels.[121] As a result, under a strict trespass to chattels theory, there is no legal remedy for an ongoing trespass to chattels that will never amount to actual injury.[122]

1. Internet Trespass and *eBay v. Bidder's Edge*

The case of *eBay v. Bidder's Edge* illustrates the difficulty of applying the theory of common law trespass to cyberspace.[123] In *eBay*, a Northern California district court addressed the legality of using software "robots" or "spiders," which automatically "crawl" the web to create aggregated, current databases for worldwide web search engines.[124] The dispute began when the online auction company eBay attempted to exclude from its site software robots sent by Bidder's Edge ("BE").[125] BE is an auction aggregation website that consolidates information from various auction sites across the internet.[126] BE's website allows users to search for products listed on these various auction sites without having to log onto each site individually.[127] eBay sought to deny access to BE's spiders, because it disliked the manner in which BE ran its searches.[128] After failed efforts to reach a licensing agreement and unsuccessful technological efforts to block BE's robots, eBay filed suit, alleging several claims, including trespass.[129]

To support its trespass action, eBay argued that BE's robots were burdening eBay's servers and causing economic harm.[130] The district court stated that under the theory of trespass to chattels, eBay's remedy would be limited to recovery of the actual damages it suffered from

---

[121] *eBay*, 100 F. Supp. 2d at 1067.

[122] *See id.*

[123] *Id.* at 1060-70.

[124] *Id.* at 1060-61. On the operation of "spiders" and search engines, see Niva Elkin-Koren, *Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing*, 26 U. DAYTON L. REV. 179 (2002); Richard Warner, *Border Disputes: Trespass to Chattels on the Internet*, 47 VILL. L. REV. 117, 127-29 (2002).

[125] *eBay*, 100 F. Supp. 2d at 1062-63.

[126] *Id.* at 1061.

[127] *Id.*

[128] *Id.* at 1062. eBay wanted BE to search the eBay site only when a customer actually queried for an item, while BE wanted to crawl eBay's site recursively to create a database. *Id.* The former method would limit the load on eBay's system and provide more accurate information, but BE customers would have to wait longer for the information. *Id.* The latter method, which BE elected, increased the search speed for BE's customers, allegedly at eBay's expense. *Id.*

[129] *Id.* at 1062-63.

[130] *Id.* at 1064-65.

impairment of its servers or the loss of their use.[131] The court was skeptical, however, of the economic harm eBay alleged, as eBay admitted that BE's robotic activities represented only 1.11% to 1.53% of the total traffic on eBay's servers.[132]

The court next considered the theory of trespass to real property.[133] Under this theory, eBay could seek injunctive relief.[134] While the court noted the analytical difficulty of treating a computer system as land rather than chattels, it nonetheless granted preliminary injunctive relief to eBay.[135] As discussed above, preliminary injunctive relief should not be available for trespass to chattels. Commentators have suggested that courts, in confronting internet trespass cases, have in fact created a new form of property protection, distinct from either trespass to chattels or trespass to land.[136]

2. The Shortcomings of the Trespass Theory

Whether under a theory of trespass to chattels, trespass to land, or a hybrid of the two, the trespass cause of action generally affords poor protection to noncommercial website owners. First, the trespass to chattels action gives standing only to possessors of chattels, for the action protects the possessor's ability to exclude others from using the chattels.[137] The *eBay* court found that eBay's computer servers were chattels, and that impairment of the servers' capacity constituted an interference with eBay's possessory interest in the servers.[138] BE's trespass occurred on eBay's servers, not on its website.[139] Following this

---

[131] *Id.* at 1065.

[132] *Id.* at 1064-65.

[133] *Id.* at 1067.

[134] *Id.*

[135] *Id.*; *see also* Intel Corp. v. Hamidi, 43 P.3d 587 (2002) (enjoining disgruntled former employee, who sent voluminous e-mails critical of employer to former colleagues, from sending further e-mails to employer's servers under trespass to chattels theory); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (2000) (holding that evidence that defendant's search robot occupied some of plaintiff's computer system capacity is sufficient to establish harm necessary for claim of trespass to chattels). *But see* Ticketmaster Corp. v. Tickets.com, Inc., 2000 WL 1887522 (C.D. Cal. Jan. 2002) (holding that spiders' very small use of computer system, without interfering with system's regular business, is insufficient to support harm requirement of trespass to chattels action).

[136] *See* Burk, *supra* note 7 at 33; Quilter, *supra* note 3, at 437. *See generally* O'Rourke, *supra* note 3.

[137] A person who is in possession of chattel is one who has physical control of it. RESTATEMENT (SECOND) OF TORTS § 216 (1965).

[138] *eBay*, 100 F. Supp. 2d at 1071.

[139] BE argued that it could not have trespassed on eBay's website because the site is

line of reasoning, the only proper plaintiff in a trespass to chattels case would be the server's owner.[140] In short, plaintiffs must own the servers upon which their websites reside. The trespass to chattels action would thus more likely protect only corporate plaintiffs, like eBay, and others wealthy enough to own their own servers. A plaintiff whose website resides on the server of a commercially available internet service provider does not appear to have a protectable interest as a possessor of chattels.[141]

Second, even in cases in which website owners do also own their servers, the owners may have great difficulty showing actual harm to a noncommercial website. The *eBay* court struggled with the problem of how to measure and monetize the injury that resulted from BE's trespass.[142] It would be even all the more difficult for a noncommercial website to show economic injury, because loss of profits will not factor into the analysis. Internet trespassers on noncommercial websites risk little in compensatory damages.[143] Accordingly, the trespass to chattels action may have no deterrent effect.

Finally, injunctive relief, the most likely relief available under a trespass to land or hybrid land/chattels action, would also do little to defend against unauthorized website access. If available at all, injunctive relief would only guard against future repetitions of the same conduct by the same defendant.[144] To protect the website, the owner would have to be prepared to sue each and every new trespasser, as each trespass occurred. If the purpose of restricting a website is to keep the site private, then injunctive relief is unwieldy and inadequate. An injunction

---

publicly accessible. The court dismissed this argument, describing eBay's servers as "private property, conditional access to which eBay grants the public." *Id.* at 1070. In reaching its decision, the court relied heavily on the fact that eBay owns its servers. *Id.*

[140] The *eBay* court suggested only that the "owner" of personal property may recover actual damages suffered from impairment of the property or the loss of its use. *Id.* at 1065. It is unclear whether an individual subscriber to an internet service provider (ISP) would have, by virtue of the subscription, a legal ownership interest in the ISP's server sufficient to establish a trespass to chattels action.

[141] If the impairment of server capacity is the measure of harm, as the *eBay* court found, then it would appear that the only proper plaintiff in a trespass to chattels case would be the owner of the impaired server.

[142] According to eBay, the load on its servers represented by BE's unauthorized spiders was between 1.11% and 1.53% of the total load. *eBay*, 100 F. Supp. 2d at 1064.

[143] Konop alleged that Davis logged onto his site at least 34 times under the names of Wong and Gardner. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 873 (9th Cir. 2002). What would compensatory damages amount to in such a case? Davis's activity did not diminish Konop's profits, because Konop was not in business. Even if Konop owned the server, would Davis's activity have impaired its value in an appreciable amount?

[144] *See supra* note 113.

cannot un-invade privacy. Once the cat is out of the bag, an injunction will not put the cat back in.

C. The Electronic Communications Privacy Act

1. The Stored Communications Act

Federal statutory law may offer a better way to protect restricted websites than do contract and tort law. Congress enacted the Electronic Communications Privacy Act in 1986 as an amendment to the Omnibus Crime Control and Safe Streets Act of 1968.[145] The SCA is Title II of the Electronic Communications Privacy Act. According to its legislative history, the SCA's purpose is "to protect privacy interests in personal and proprietary information."[146] Specifically, Congress sought to address the increasing problem of computer users who deliberately gain unauthorized access to electronic communications not intended for the general public.[147] Protected communications specifically include "electronic bulletin boards," which may take the form of noncommercial, password-protected networks operating for users who "share special interests."[148] Congress stated that these bulletin boards could be public or semi-public, "depending on the degree of privacy sought" by the users or organizers of the systems.[149] The legislative history explicitly states that the SCA does not "hinder the development or use" of electronic bulletin boards.[150]

Section 2701(a)(1) of the SCA prohibits unlawful access to stored communications.[151] Recognizing that some publicly accessible computer facilities also contain restricted areas, Congress enacted section 2701(a)(2) to prohibit authorized subscribers from exceeding the scope of their authorization.[152] For example, under section 2701(a)(2), authorized users of an internet service may lawfully access their own e-mail and the

---

[145] S. REP. NO. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555. The Electronic Communications Privacy Act was passed as Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[146] S. REP. NO. 99-541, at 3.

[147] *Id.* at 35.

[148] *Id.* at 8-9.

[149] *Id.* at 9.

[150] *Id.* at 36.

[151] 18 U.S.C. § 2701 (2000).

[152] S. REP. NO. 99-541, at 36.

public portions of the service.[153] They may not, however, access other subscribers' private e-mail and other nonpublic portions of the service.[154] These examples, included in the legislative history, suggest that Congress intended the statute to protect internet service providers from so-called "hackers" — expert computer users who deliberately break into computer networks to cause mischief.[155] The penalties for violating subsection (a) are spelled out in subsection (b).[156]

Section 2701(c), however, creates an exception to the offenses enumerated in subsection (a).[157] Under subsection (c), a "user" of the electronic communications service may permit third-party access to communications intended for the user.[158] For example, sharing an e-mail account with a visiting friend would not violate the SCA. How to interpret the meaning of subsection (c), however, is the question that the *Konop* case raises.[159]

2. The SCA and *Konop v. Hawaiian Airlines, Inc.*

In *Konop*, the Ninth Circuit remanded the case to the district court to determine whether the pilots Wong and Gardner, who authorized Davis's use, were themselves "users" of Konop's website.[160] If they were not users, the case under the SCA is simple: Hawaiian violated the Act and cannot claim that the permission of a "user" exempts it from liability.[161] If, however, the court finds that Wong and Gardner were users, then it may have to decide whether Konop's clickwrap license effectively alters the meaning of section 2701's subsection (c).[162]

---

[153] 18 U.S.C. § 2701.

[154] *Id.*

[155] "Hackers" are commonly thought to be sophisticated, destructive computer users. Within the computer community, however, "hacker" generally designates a sophisticated user, while destructive hackers are called "crackers." JAN SAMORISKI, ISSUES IN CYBERSPACE: COMMUNICATION, TECHNOLOGY, LAW, AND SOCIETY ON THE INTERNET FRONTIER 186 (2002).

[156] Penalties include fines and imprisonment for up to two years. 18 U.S.C. § 2701(b).

[157] S. REP. NO. 99-541, at 36.

[158] *Id.*

[159] *See supra* notes 57-76 and accompanying text.

[160] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 880 (9th Cir. 2002).

[161] 18 U.S.C. § 2701(a).

[162] While it is too soon to tell how this case will proceed on remand, it is reasonable to speculate that the enforceability of the Konop's license may be an issue. Given that commercial licenses have been enforced, see *supra* notes 87-106 and accompanying text, the court may not have to address the question.

Courts tend to uphold clickwrap licenses, particularly when the terms of use "pop up" on the screen and do not allow the user to continue without clicking assent.[163] Konop's license did not allow visitors to enter the site without agreeing to his terms of use.[164] One of these terms was the requirement that users not "furnish" the site's contents to anyone else.[165] Authorizing third-party visits to the site probably constitutes "furnishing" the site's contents to others. The dictionary definition of "furnish" is simply to "to provide."[166] By permitting Davis to visit the site using their names, Wong and Gardner were in effect providing the site's contents to Davis. They were authorizing third-party access, which section 2701(c) permits, but which Konop's clickwrap license disallows.

The meaning of "user," therefore, may depend on the validity of Konop's clickwrap license. If Konop's licensing agreement is enforceable, then it divides "eligible users" into two groups: 1) non-users and 2) users who have already bargained away their right to permit third-party access by accepting Konop's terms. In other words, under Konop's license, being a "user" is synonymous with relinquishing authority to share the site with others. The language of subsection (c) presumes that all users of electronic communications services will retain their right to permit third-party access, a right that Konop's clickwrap license requires all users to surrender. In effect, eligible users must give up their rights under section 2701(c), as the price of becoming actual users of Konop's website.

At present, it remains an open question how courts should interpret the section 2701(c), and its purpose, in light of clickwrap licensing restrictions like Konop's. The statute does not speak to the situation. It presumes that users will retain the right to permit third-party access. Yet private actors may want to eliminate this right through contract, while still retaining the protections of the SCA. As discussed above, the SCA is the best legal protection available to noncommercial restricted websites. It is very likely, therefore, that parties may want to contract around section 2701(c), without losing the protection of sections 2701(a) and (b).

---

[163] *See supra* note 90. The *Specht* court in particular emphasized the significance of a clickwrap license that does not allow the user to proceed without assenting. Specht v. Netscape Communications Corp., 150 F. Supp. 2d 585, 592 (S.D.N.Y. 2001).

[164] *Konop*, 302 F.3d at 876 n.3.

[165] *Id.*

[166] OXFORD MODERN DICTIONARY 429 (1992).

III. PROPOSAL TO AMEND THE ECPA

Under the current state of the law, noncommercial website operators have little or no protection from unauthorized access to their sites.[167] The relation between private contract law and the SCA is uncertain. At least one court has ruled that the SCA's exclusivity of remedies provision preempts all state-law claims based on conduct that falls within the statute.[168] If the SCA preempts contract law, then electronic service providers cannot arrange with their users to keep website information private. Yet this result is not in keeping with the overall tenor of the SCA. Rather, the legislative history makes clear that Congress intended the Act to protect "electronic bulletin boards," and that "users, operators, and organizers" could select "the degree of privacy" appropriate for their networks.[169] If the SCA generally permits users, operators, and organizers to determine how private to keep their websites, then it would be contrary to the statute's purpose to read section 2701(c) in such a way as to eliminate that freedom by transferring it entirely to the discretion of "users." If subsection (c) really does grant all users the right to permit third-party access, it would appear to undermine Congress' stated purpose in enacting the SCA.

To give noncommercial websites real protection from unauthorized access, Congress should amend section 2701(c)(2) to clarify that the SCA does not preempt private licensing agreements. The amended section 2701(c)(2) might read as follows:

> (c) Exceptions. — Subsection (a) of this section [prohibiting intentional, unauthorized use] does not apply with respect to conduct authorized —
>
> (1) by the person or entity providing a wire or electronic communications services;
>
> (2) by a user of that service with respect to a communication of or intended for that user, under all applicable terms and conditions of use; or
>
> (3) in section 2703, 2704 or 2518 of this title.

---

[167] *See supra* notes 87-158 and accompanying text.

[168] Muskovich v. Crowell, 1995 WL 905403, at *1 (S.D. Iowa Mar. 21, 1995) (preempting state law intentional infliction of emotional distress claim based on obscene phone calls made to unlisted number acquired in violation of SCA). More often, decisions concerning the SCA's exclusivity of remedies clause, 18 U.S.C. § 2708, have addressed whether to suppress evidence gathered in violation of the SCA. 18 U.S.C. § 2708 (2000). *See, e.g.*, United States v. Smith, 155 F.3d 1051, 1056 (1998) (holding that section 2708 preempts exclusion as remedy).

[169] S. REP. NO. 99-541, at 9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.

This amendment to subsection (c) would permit private parties to modify the scope of a user's ability to authorize third-party access. If an enforceable licensing agreement eliminates the user's authority to share the site, then subsection (c) would no longer serve as a defense for third parties who enter the restricted site. Even with permission from a user, third parties who click through the pop-up license to reach the restricted website would be knowingly violating subsection (a)(2). The pop-up license would put them on notice that they were exceeding the scope of the user's authorization, because the user was never authorized to permit third-party use.

Under the facts in *Konop*, and presuming that the clickwrap license on the site was enforceable, this amendment to the SCA would protect the noncommercial website. The terms of Konop's license would establish that Wong and Gardner could never have had the authority to consent to Davis's visits. The prominence of the clickwrap license on the screen would show that Davis knew or should have known that his visits were unauthorized. By visiting the site nonetheless, Davis would have violated the SCA by intentionally exceeding Wong and Gardner's authorization to access the electronic communications facility.

CONCLUSION

One unavoidable consequence of strengthening privacy protections for noncommercial websites would be the further privatization of the internet. Strong privacy protections would close off parts of cyberspace. Some have argued that we should value the internet as a new and wonderful public commons, rather than rushing to enclose it as private property.[170] Yet legal protections for noncommercial websites might actually promote, rather than impede, valuable communal uses of the internet, such as family news sharing, counseling networks, support groups, and other social or ministerial endeavors yet to be imagined.

To protect the privacy of interests of noncommercial websites, Congress should amend the Stored Communications Act to recognize private licensing agreements among electronic communications users, organizers, and operators. Tort law applies awkwardly in cyberspace,

---

[170] *See* Lawrence Lessig, *The Architecture of Innovation*, 51 DUKE L.J. 1783 (2002) (arguing for less privatization of internet); Lawrence Lessig, Foreword, *Cyberspace and Privacy: A New Legal Paradigm?*, 52 STAN. L. REV. 987 (2000) (arguing for maintaining "open access" end-to-end internet architecture); Richard Stallman, *The GNU Project*, *at* http://www.gnu.org/gnu/thegnuproject.html (last visited Aug. 22, 2002) (describing history and purpose of "open source" movement). On the open source movement, see Mark H. Webbink, *Open Source Software – Bridging the Chasm*, 691 PLI/PAT 663 (2002).

and contract law grows feeble outside the presence of money. The amended Stored Communications Act would provide a statutory remedy, made flexible through the institution of contract, for those who wish to shield their websites from trespassing eyes.