No. 05-13687-CC

UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

MICHAEL SNOW,

Plaintiff/Appellant,

v.

DIRECTV, INC. et al.,

Defendants/Appellees.

ON APPEAL FROM
THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA

AMICI CURIAE BRIEF OF ELECTRONIC FRONTIER FOUNDATION AND U.S. INTERNET INDUSTRY ASSOCIATION IN SUPPORT OF APPELLEES

Cindy A. Cohn
Cal. Bar No. 145997
Kevin S. Bankston
Cal. Bar No. 217026
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333
(415) 436-9993 (fax)
Attorneys for Amici Curiae

September 30, 2005

UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

MICHAEL SNOW,

Plaintiff/Appellant,

v.

DIRECTV, INC., et al.,

Defendants/Appellees.

Docket No. 05-13687-CC

APPEAL

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT

Pursuant to Eleventh Circuit Rules 26.1-1, 26.1-2, and 26.1-3, counsel for Amici Curiae Electronic Frontier Foundation and U.S. Internet Industry Association certify that the following is a complete list of the persons and entities who have an interest in the outcome of this case:

Robert S. Apgood, Counsel for Appellant

Lauren E. Bush, Counsel for Appellees

Cindy A. Cohn, Counsel for *Amici Curiae*

CarpeLaw, Counsel for Appellant

Hon. Sheri Polster Chappell, U.S. Magistrate Judge, U.S. District Court for the Middle District of Florida

Hon. Virginia M. Hernandez Covington, U.S. District Judge, U.S. District Court for the Middle District of Florida

DIRECTV, Inc., Appellee

DIRECTV Enterprises, LLC, Parent Company of DIRECTV, Inc.

DIRECTV Holdings LLC, Parent Company of DIRECTV Enterprises, LLC

The DIRECTV Group, Inc., Parent Company of DIRECTV Holdings LLC

Christian S. Genetski, Counsel for Appellees

Michael Snow, Appellant

The News Corporation Limited

Sonnenschein Nath & Rosenthal, LLP, Counsel for Appellees

Electronic Frontier Foundation, *Amicus Curiae*

U.S. Internet Industry Association, *Amicus Curiae*

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *Amici Curiae* certify that no publicly held corporation or other publicly held entity owns 10% or more of any *Amicus Curiae.*

TABLE OF CONTENTS

TABLE OF CITATIONS

Cases

Statutes

Other Authorities

Law Review Articles and Treatises

The Electronic Frontier Foundation and the U.S. Internet Industry Association respectfully submit this brief *amicus curiae* in support of Appellees DirecTV, Inc.; Stump, Storey, Callahan, Dietrich & Spears; and Yarmuth, Wilsdon & Calfo, PLLC (collectively, "DirecTV"). *Amici* urge this Court to remand Appellant Snow's suit to the district court for dismissal based on the alternate reasoning specified herein. Although the district court reached the correct result, its opinion is mistaken in law and poses a grave threat to Internet users' privacy, as well as to the interests of those who offer private communications services over the World Wide Web.

STATEMENT OF AMICUS CURIAE'S IDENTITY, INTEREST AND AUTHORITY TO FILE

The Electronic Frontier Foundation ("EFF") is a nonprofit, member-supported legal foundation that litigates to protect free speech and privacy rights in the online world. As part of that mission, EFF has served as counsel or *amicus* in a number of key cases addressing electronic privacy statutes. *See, e.g., Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994); *U.S. Telecom Ass'n v. F.C.C.*, 227 F.3d 450 (D.C. Cir. 2000); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002), *cert. denied*, 537 U.S. 1193 (2003); *Doe v. Ashcroft*, 334 F.Supp.2d 471 (S.D.N.Y. 2004), *appeal pending*; and *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005). With more than 10,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age. EFF opposes

misguided legislation, initiates and defends court cases preserving individuals' rights, launches global public campaigns, introduces leading edge proposals and papers, hosts frequent educational events, engages the press regularly, and publishes a comprehensive archive of digital civil liberties information at one of the most linked-to web sites in the world, www.eff.org.

The U.S. Internet Industry Association ("USIIA") is the nation's oldest, largest and most active trade association for providers of broadband and IP services, with more than 200 members engaged in Internet commerce, content, and connectivity. Its mission is to promote the deployment and use of advanced IP-based services, from broadband Internet and IP Video to telephony and other advanced services. The Web Hosting Council of USIIA, a council of members representing the interests of companies that host IP services, includes those engaged in web hosting, electronic communication hosting and ASP applications hosting.

Amici have obtained the consent of all parties.

STATEMENT OF THE ISSUES

The question presented in this case is whether DirecTV's accessing of Snow's web site, which was stored in facilities configured to be readily accessible to the general public, violated 18 U.S.C. § 2701 of the Stored Communications Act.

INTRODUCTION AND SUMMARY OF ARGUMENT

From small mistakes, grave injustices may come, and such is the

threat here. The district court correctly found that the Stored Communications Act ("SCA") does not protect the privacy of communications posted to Snow's public web site. However, the court's reasoning in reaching that result was mistaken, and if adopted by this Court may eviscerate the statutory protections for private communications made over the World Wide Web.

Snow alleges that DirecTV violated 18 U.S.C. § 2701 of the SCA by accessing the contents of his web site without his authorization, based on textual warnings published on the site stating that DirecTV representatives were not authorized to enter. Document 1 ("Complaint") at pp. 5-6. Despite the warning banners, however, the computer hosting the site was configured to be readily accessible to the general public: any Internet user could enter Snow's site and register to use its bulletin board. Complaint at 5. [1]

The Electronic Communications Privacy Act ("ECPA"), of which the SCA is a part,[2] plainly forbids SCA claims based on access to electronic

---

[1] Although not the subject of this brief, *amici* agree that Snow's warnings did not turn DirecTV's access to Snow's public web site into an "unauthorized" access under the SCA. *See* Appellees' Br. at 34-40. Additionally, *amici* agree that a ruling otherwise would violate public policy: as DirecTV succinctly puts it, "[u]pholding such restrictions would shield wrongdoers" by allowing them to "bring civil actions against any competitor, press outlet or public watchdog group, merely by including an express prohibition against access by such groups in their public web site's terms of use." *Id*. at 40, 40 n. 53, and *generally* 40-43.

[2] The SCA is the common name for that portion of the ECPA regulating stored communications and records, codified at 18 U.S.C. §§ 2701, *et seq*., in Chapter 121 of Title 18 of the U.S. Code. *See Electronic Communications*

communications that are stored in a system that is configured to be readily accessible to the general public. *See* 18 U.S.C. § 2511(2)(g). Snow's case should have been dismissed solely on this basis. Because it was not made aware of this clear statutory authority,[3] however, the district court was instead forced to dive into what this Circuit has acknowledged as "a complex, often convoluted, area of the law." *U.S. v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003) (internal citation and quotation omitted). The district court emerged from those depths with an overbroad and dangerous holding.

The district court's holding—that the communications posted to the bulletin board on Snow's public web site were not in "electronic storage" because the web site was their "final destination," Document 51 (Amended Report and Recommendation or "AR&R") at p. 5—threatens to deprive legitimately private web communications of the SCA's protection. "While most websites are public," the Ninth Circuit has explained, "many…are restricted," requiring that visitors "enter[] the appropriate information (password, social security number, etc.)" before gaining access. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 876 (9th Cir. 2002), *cert. denied*, 537 U.S. 1193 (2003). Yet by the district court's erroneous logic, these private sites would also be the "final destinations" of the messages posted to them;

Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of Title 18).

[3] *Amici* agree with DirecTV that this omission in the briefing below does not prevent this Court from relying on 18 U.S.C. § 2511(2)(g) in its decision. *See* Appellees' Br. at 26 n. 33, 27 n. 34.

those communications would not be in "electronic storage" and therefore would not be protected by the SCA.

The consequences of stripping away the privacy protections enacted by Congress are dire for both the users and proprietors of web-based services that allow private communications. If this Court were to agree that communications posted to a web site are not in "electronic storage," then 18 U.S.C. § 2702, which protects a user's stored communications from unauthorized disclosure, would no longer protect web-based communications. Similarly, 18 U.S.C. § 2703's carefully crafted regulations of a service provider's disclosure of stored communications to the government, which typically require a search warrant for communications in "electronic storage," would no longer apply—the government could simply subpoena those communications.

As described more fully below, the district court's reasoning contradicts the plain language as well as the legislative and judicial history of ECPA and the SCA, endangers Internet users' privacy, and imposes costs on providers of private web services. To avoid upsetting the understanding of "electronic storage" upon which industry and users depend for basic privacy protections, *amici* respectfully urge this Court to follow the language and intent of Congress, and find that the messages on Snow's web site were indeed in "electronic storage." Snow's suit must instead be dismissed based on 18 U.S.C. § 2511(2)(g)'s prohibition against SCA claims based on access to publicly-accessible communications.

ARGUMENT

I. The Stored Communications Act Does Not Protect the Contents of Snow's Web Site, which Were Communicated Through an Electronic Communication System Configured to Be Readily Accessible to the General Public.

Snow alleges that DirecTV's accessing of the contents of his web site, which were stored in the computer facilities of electronic service provider Globat,[4] violated 18 U.S.C. § 2701 of the SCA.[5] Courts start a statutory analysis with the language of the statute itself, *see Gwaltney of Smithfield, Ltd. v. Chesapeake Bay Found.*, 484 U.S. 49, 56 (1987), and the plain language of the ECPA bars Snow's claims because his web site was configured to be publicly accessible:

> It shall not be unlawful under…chapter 121 of this title [i.e., the SCA] for any person…to…access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public….

18 U.S.C. § 2511(2)(g). No party disputes that the postings to Snow's web site were "electronic communications"[6] made through an "electronic

---

[4] Complaint at 6.

[5] Under 18 U.S.C. § 2701, an offense is committed by anyone who: "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided;" or "(2) intentionally exceeds an authorization to access that facility; and thereby obtains…[an] electronic communication while it is in electronic storage in such system."

[6] An "electronic communication" is, in relevant part, "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted…by a wire, radio, electromagnetic, photoelectronic or photooptical system." 18 U.S.C. § 2510(12).

communications system."[7] In fact, the arguments of both parties rely upon it.[8] And the record shows that the relevant system, Globat's web server, was configured such that the communications on Snow's web site were readily accessible to any Internet user who visited. Complaint at 5-6.

Any Internet user could enter Snow's web site without technical restriction, and any Internet user could register and create a password to enter the site's bulletin board. Complaint at 5-6. Snow's "warning" message on the site's home page, and his supposed "access limitation clause" limiting registration for the bulletin board to those who represented that they were

---

[7] An "electronic communications system" is "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14). The facilities used by a provider of an "electronic communication service" are such a system. *See* 18 U.S.C. § 2701 (prohibiting unauthorized access to "a facility through which an electronic communication service is provided…" and accessing communications in storage "in such *system*….") (emphasis added).

[8] Snow alleges that Globat's computer facilities were used for the electronic storage of his electronic communications, Complaint at 6, while DirecTV also argues that Snow's web site was stored in an electronic communication system, albeit one that was readily available to the general public, Appellees' Br. at 26-28. DirecTV misses the point, however, when arguing that Snow's web site is not a facility through which an electronic communications service is provided. Appellees' Br. at 16, n. 23. A web "site" is not a facility at all, but rather a collection of files stored on an Internet-connected computer and made available for download over the web. *See Konop*, 302 F.3d at 875. Globat's facilities, in which the contents of Snow's site were held in electronic storage, are the relevant facilities here, not the notional "site" that those facilities host.

not affiliated with DirecTV, were not "configurations"[9] of Globat's web server such that communications made through that system were not publicly accessible. Rather, they were themselves communications being made through the system, which was configured like all public web sites: to allow complete access by any visitor.[10]

Therefore, even assuming that DirecTV's actions facially violated 18 U.S.C. § 2701's prohibition on unauthorized access to communications in electronic storage, Snow's claim is barred under 18 U.S.C. § 2511(2)(g). Where, as here, the statute is unambiguous, the judicial inquiry is at an end and courts must enforce the congressional intent embodied in that plain wording. *See United States v. Clark*, 454 U.S. 555, 560 (1982).

Even if the language were not clear enough, dismissal under Section 2511(2)(g) would also be consistent with Congress' stated intent. As the Ninth Circuit found when discussing whether the privately-configured web

---

[9] When speaking of computers, "configuration" means "[t]he way in which a computer system is set up," "[t]he set of constituent components, such as memory, a hard disk, a monitor, and an operating system, that make up a computer system," or "[t]he way that the components of a computer network are connected." *The American Heritage Dictionary of the English Language* (4th ed., Houghton Mifflin Company 2000), *available at* http://dictionary.reference.com/search?q=configuration (last accessed on Sep. 30, 2005).

[10] Notably, Globat does offer private configurations that Snow could have taken advantage of. *See* Globat, *The Globat Command Console, available at* http://www.globat.com/features/p-control.php (last accessed on Sep. 30, 2005) ("Want to keep certain folders on your Web site out of public view? The GCC's 'Web Protect' allows you to apply password protection on your Web sites folders, so you can restrict access to whoever you like.").

site at issue in *Konop* was protected by the SCA, "the legislative history of the ECPA suggests that Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards," as opposed to publicly-accessible communications. *See Konop*, 302 F.3d at 875, *citing* S. Rep. No. 99-541, at 35-36, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3599 ("This provision [the SCA] addresses the growing problem of unauthorized persons deliberately gaining access to ... electronic or wire communications that are not intended to be available to the public."); *also citing* H.R. Rep. No. 99-647 at 41, 62-63 (1986) (describing how the configuration of an electronic communications system would determine whether access to the communications stored therein would violate 18 U.S.C. § 2701). This legislative history cited in *Konop* mirrors the language of 18 U.S.C. § 2511(2)(g) and reflects Congress' intent that the SCA not protect communications in "electronic storage" that are also publicly accessible.

In *Konop*, the court found that the contents of the web site at issue, which the parties agreed were in "electronic storage," were not stored on a system configured to be publicly accessible and were therefore protected by the SCA. *See Konop*, 302 F.3d at 875, 879. Snow relies heavily on *Konop* to argue against dismissal here,[11] but Snow's site is easily distinguishable from the site the Ninth Circuit considered. In *Konop*, only those who entered the

[11] Appellant's Br. at 16-18.

name of a pre-defined "eligible person" could register to use the site's bulletin board. *See id.* at 875 n. 3. In contrast, Snow's site did not require that visitors "enter[] the appropriate information" such as the name of an eligible person, or a "password, social security number, etc." before gaining access. *Id.* at 876. Rather, anyone could click "I agree" and enter the site's bulletin board without restriction. Complaint at 6. In other words, and unlike the site in *Konop,* it was readily accessible to the general public.

Dismissal based on 18 U.S.C. § 2511(2)(g) therefore comports with not only the statute's plain language and its legislative history, but also the reasoning in *Konop,* which this Court has cited approvingly. *See United States v. Steiger,* 318 F.3d at 1046-50.

II. Although Ultimately Unprotected by the Stored Communications Act by Virtue of Being Publicly Accessible, the Contents of Snow's Web Site did Constitute Communications in "Electronic Storage."

In deciding that the messages published on Snow's web site were not in "electronic storage," the district court seemed to be trying to justify its common-sense conclusion: that the SCA does not support a cause of action for unauthorized access to publicly accessible communications. As shown above, this correct conclusion is dictated by 18 U.S.C. § 2511(2)(g), not the SCA itself. In a futile search for authority within the four corners of the SCA, the court tried to fit a square peg into a round hole and use the "electronic storage" definition to accomplish this purpose. Unfortunately, the court's holding that messages posted to public web sites are not in

"electronic storage" is flatly incorrect, ignoring the plain language of ECPA and the SCA while significantly misunderstanding the technology involved.

As an initial matter, the mere existence of 18 U.S.C. § 2511(2)(g) proves that publicly-accessible communications can be in "electronic storage" as a matter of law. Congress would not have needed to exempt unauthorized access to publicly-accessible communications from liability under the SCA if these communications were already excluded from SCA coverage via the definition of "electronic storage." "A statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant." *Duncan v. Walker*, 533 U.S. 167, 174 (2001) (internal quotation marks and citation omitted); *see also United States v. Menasche*, 348 U.S. 528, 538-539 (1955) ("It is our duty to give effect, if possible, to every clause and word of a statute." (quoting *Montclair v. Ramsdell*, 107 U.S. 147, 152 (1883)).

Second, the "electronic storage" definition by its terms does not distinguish between public and private messages. "Electronic storage" is defined as:

> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

18 U.S.C. § 2510(17). Whether a communication is public or private simply has nothing to do with whether it is in "electronic storage."

Third, the contents of Snow's web site satisfy the plain language of

the "electronic storage" definition. The district court focused on the "intermediate storage" definition at 18 U.S.C § 2510(17)(A), and found that it only applied to a communication "held by a third party Internet service provider until it is requested to be read," i.e., a communication "waiting to be transferred to a final destination." AR&R at 5.

Even assuming that Subsection (A) is so limited, the contents of Snow's web site do meet these criteria. We commonly think of web "sites" as places to be visited. But in reality, a web site's "pages" are computer files that are downloaded by Internet users from a web "server" or "host" computer.[12] Third parties like Globat, who run these computer servers and provide them to Internet users, are not the intended recipients of the communications posted to the web site, and their facilities are not a message's final destination.

---

[12] As the Ninth Circuit has described:

> Each website has a unique domain name or web address (e.g., Amazon.com or Lycos.com), which corresponds to a specific location within the server where the electronic information comprising the website is stored. A person who wishes to view the website types the domain name into a computer connected to the Internet. This is essentially a request to the server to make an electronic copy of the website (or at least the first page or "home page") and send it to the user's computer. After this electronic information reaches the user's computer, it is downloaded for viewing on the user's screen.

Konop, 302 F.3d at 875; *see generally* Preston Galla, *How the Internet Works* (MacMillan Computer Publishing) (1999); and Wikipedia, *Web Page*, *available at* http://en.wikipedia.org/wiki/Web_pages (last accessed on Sep. 30, 2005).

Indeed, if the web site were in fact the "final destination" of messages posted to it, and a message's journey ended once it reached Globat's facilities, then no one could read the web site at all: a "visitor" to the "site" can only view a message if Globat forwards a copy of it to the visitor's computer.

The key point here is simple: Snow sought to communicate with Internet users, not with Globat. Globat is an intermediary that enables the transfer of messages between speakers (like Snow) and readers (those who access his web site). Globat's storage of those messages is "intermediate" ("in the middle position or state"[13]) between those who post messages to the web site and those who download them, and is therefore necessary and "incidental" to the transmission of the files to readers.

Furthermore, the district court did not even consider the possibility that Snow's web site was in electronic "backup storage." 18 U.S.C. § 2510(17)(B) ("any storage of such communication by an electronic communication service for purposes of backup protection of such communication."). To the extent that Snow's communications have already been retrieved by visitors to the web site, the remaining stored copies of those communications on Globat's web server qualify as "backup storage" that ensures that future users of the site may access its contents, even if those

---

[13] *The American Heritage Dictionary of the English Language* (4th ed., Houghton Mifflin Company 2000), *available at* http://dictionary.reference.com/search?q=intermediate (last accessed on Sep. 30, 2005).

communications have already been downloaded by a previous user. *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2003), *cert. denied*, 125 S.Ct. 48 (2004) (finding that "obvious purpose" for storing a message on the provider's server after delivery is to provide a second copy of the message in the event it needs to be downloaded again). Of course, when future users download such a backup copy, that backup copy is also in "intermediate storage" incidental to that transmission, and satisfies both components of the "electronic storage" definition at the same time.

However, this Court need not attempt to draw a line at the exact point at which Globat's copy of a message posted to Snow's web site falls out of Subsection (A) and into Subsection (B), or back again. It is sufficient to find that Snow's web site message content is stored incidental to transmission for at least some limited period of time, and to the extent it is not, it is stored as backup to allow future downloads. Any finding otherwise could, contrary to Congress' intent, leave many private Internet communications wholly unprotected by the SCA.

III. Affirmance of the District Court's Holding that the Contents of Snow's Web Site Were Not in "Electronic Storage" Would Threaten the Privacy of Web-Based Communications that Are Configured to Be Private.

As already described, the "electronic storage" definition does not distinguish between public and private communications. Therefore, the court's holding that messages posted to Snow's public site were not in "electronic storage" could equally be applied to the contents of any private

web site, and rob them of SCA protection. This would be a disaster for online privacy, affecting a great number of private web-based services serving countless Internet users. For example, both Google and Yahoo! allow users of their web-based "Groups" services to post bulletin board messages that are only accessible to other specified users.[14] Similarly, services such as TypePad and LiveJournal that host web logs or "blogs" typically offer users the ability to restrict access.[15] In fact, the vast majority of people who use a third party to host their web site can take advantage of password protection, because password protection is a feature of the most

---

[14] *See* Yahoo!, *Group Settings Help*, *available at* http://help.yahoo.com/help/us/groups/settings/settings-12.html (last accessed on Sep. 30, 2005) ("If your [Yahoo] group is designed for a specific set of people (and not the general public) and you want to control membership, then you should choose to make your group restricted, which means you must approve all memberships."); *see also* Google, *Groups Help*, *available at* http://groups.google.com/support/bin/answer.py?answer=7922&topic=255 (last accessed on Sep. 30, 2005) ("As a group owner, you can control your group's access setting. When you're creating a group, select "Restricted" under 'Access Level.' You can also change the group's access setting after you've created it.").

[15] For example, using the blog service TypePad, "you can choose to password protect either your entire web site or individual weblogs or photo albums." TypePad, *TypePad Help*, *available at* http://help.typepad.com/panel/site_access.html#setting_up_password_protection (last accessed on Sep. 30, 2005). Other services, such as LiveJournal, offer even more fine-grained access controls. *See* LiveJournal, *LiveJournal Support*, *available at* http://www.livejournal.com/support/faqbrowse.bml?faqid=24 (last accessed on Sep. 30, 2005) ("You can control who can read your entries by setting security levels for them, either when you post them or by editing them later. There are four security levels available: Public, Friends, Custom, and Private.").

common web server software.[16]

Protecting the privacy of the electronic communications stored by these services is wholly consistent with the plain language of the SCA and the intent of Congress, which was to protect stored electronic communications that are not readily accessible to the general public regardless of what particular communications technology is used. *See* 132 Cong. Rec. H 4039, 99th Cong. 2nd Sess., pp. 18-19 (June 23, 1986). ECPA's protections are "not limited to particular types or techniques of communicating," because "[a]ny attempt to write a law which tries to protect only those technologies which exist in the marketplace today…is destined to be outmoded within a few years." *Id.*

Although Congress was speaking there of real-time "interception" of electronic communications governed by other parts of ECPA, as opposed to access to stored communications under the SCA, the principle is equally applicable here. The statute does not support and Congress would not approve of a rule that affords SCA protection to the users of some private

---

[16] A recent survey shows that 70% of web servers run the "Apache" server software. *See* Netcraft, *September 2005 Web Server Survey*, *available at* http://news.netcraft.com/archives/web_server_survey.html (last accessed on Sep. 30, 2005). Apache allows users to control access in a variety of ways. *See* Apache.org, *Authentication, Authorization, and Access Control*, *available at* http://httpd.apache.org/docs/2.1/howto/auth.html (last accessed on Sept. 30, 2005) ("If you have information on your [Apache] web site that is sensitive or intended for only a small group of people, the techniques in this article will help you make sure that the people that see those pages are the people that you wanted to see them.").

methods of communication (e.g., email) while failing to protect the privacy of communications that are posted to a private Yahoo! group or via a private TypePad blog. Yet by holding that messages posted to the web are not in "electronic storage," the district court's holding threatens to establish just such a rule.[17]

Not only would such a rule threaten web users' privacy, it would compromise the ability of service providers to offer truly private web-based services and increase costs to those that do, including many of *amici*'s members. Private web-based communications currently enjoy substantial privacy protections under the SCA only because they are in "electronic storage;" for example, under 18 U.S.C. § 2703(a), the government must use a judicial search warrant to obtain the contents of such communications from service providers. If private web-based communications were not in "electronic storage," then the SCA would not apply, and the government would need only a subpoena to obtain the contents of private web sites such as those offered by Google, Yahoo! and others.[18]

---

[17] The district court's holding may even threaten the privacy of email, where it is communicated via a web-based service such as Yahoo!'s email service (mail.yahoo.com) or Google's "Gmail" (gmail.google.com).

[18] A holding that web-based communications are not in "electronic storage" even calls into question whether those offering web-based services are providing an "electronic communication service." If they were not, individuals would forfeit the SCA's privacy protections governing government access to subscriber records that do not contain communications content. *See* 18 U.S.C. 2703(c).

Similarly, 18 U.S.C. § 2702 generally prohibits providers from disclosing private communications to non-government third parties. Importantly, there is no exception for civil subpoenas.[19] If web-based communications were no longer in "electronic storage," then providers of these web-based services would be subject to civil subpoenas, and experience has shown that such subpoenas are both likely and burdensome. These additional costs of running a private service without the protection of the SCA will not only injure *amici*'s bottom lines and the privacy of their users, but also discourage the development and offering of more private services over the web.

In reaching its troubling holding that messages posted to a web site are not in "electronic storage," the district court was apparently looking for a rationale that would reach the sensible conclusion that Snow's public web site was not under the SCA's protection. Unfortunately, the district court resorted to the most effective option it had *without* Section 2511. But its conclusion is incorrect because the "electronic storage" definition does not distinguish between SCA-protected private communications and unprotected public communications; that is instead the function of 18 U.S.C. § 2511(2)(g), and the district court erred by failing to rely on that provision in

---

[19] *See* 18 U.S.C. § 2702(a)(1); *see also* U.S. Internet Service Provider Association, *Electronic Evidence Compliance—A Guide for Internet Service Providers*, 18 BERKELEY TECH. L. J. 945, 965 (2003) (the SCA does not "permit[] disclosure pursuant to a civil discovery order unless the order is obtained by a government entity....").

dismissing Snow's suit.

CONCLUSION

For the foregoing reasons, *Amici* respectfully request that this Court remand to the district court for dismissal relying on 18 U.S.C. § 2511(2)(g) and based on the publicly-accessible nature of Snow's web site, rather than affirming the district court's dismissal based on the incorrect holding that Snow's web site was not in "electronic storage."

Dated: September 30, 2005

Respectfully submitted,

Cindy A. Cohn
Cal. Bar No. 145997
Kevin S. Bankston
Cal. Bar No. 217026
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333
(415) 436-9993 (fax)

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 4,803 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2000 version 9 in Times New Roman, 14-point font.

Dated: September 30, 2005

Respectfully submitted,

Cindy A. Cohn
Cal. Bar No. 145997
Kevin S. Bankston
Cal. Bar No. 217026
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333
(415) 436-9993 (fax)

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on the 30th day of September, 2005, the undersigned served one (1) true and correct copy of the foregoing AMICI CURIAE BRIEF OF ELECTRONIC FRONTIER FOUNDATION AND U.S. INTERNET INDUSTRY ASSOCIATION IN SUPPORT OF APPELLEES on the interested parties in said cause by Federal Express Overnight Delivery, to the persons at the addresses set forth below:

Albert A. Zakarian
16765 Fishhawk Blvd.
Suite 360
Lithia, FL 33547-3860

Robert S. Apgood
CarpeLaw PLLC
500 Union Street
Suite 510
Seattle, WA 98101-4068

Marc J. Zwillinger
Christian S. Genetski
Lauren E. Bush
Sonnenschein Nath & Rosenthal LLP
1301 K Street, N.W.
Suite 600, East Tower
Washington, D.C. 20005

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Cindy A. Cohn
Cal. Bar No. 145997