HANNI FAKHOURY (SBN 252629)
hanni@eff.org
KURT OPSAHL (SBN 191303)
kurt@eff.org
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993

Attorneys for *Amici Curiae*
ELECTRONIC FRONTIER FOUNDATION AND LAW PROFESSORS CHRISTINE DAVIK, JENNIFER GRANICK, JORDAN KOVNOT AND STEPHEN SCHULTZE

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

CRAIGSLIST, INC., a Delaware corporF. Supp. 2d v.

3TAPS, INC., a Delaware corporation; PADMAPPER, INC., a Delaware corporation; DISCOVER HOME NETWORK, INC., a Delaware corporation d/b/a LOVELY; BRIAN R. NIESSEN, an individual; and Does 1 through 25 inclusive,

Defendants.

3TAPS, INC., a Delaware corporation,

Counter-claimant,

v.

CRAIGSLIST, INC., a Delaware corporation,

Counter-defendant.

Case No. 3:12-cv-03816 CRB

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, CHRISTINE DAVIK, JENNIFER GRANICK, JORDON KOVNOT AND STEPHEN SCHULTZE IN RESPONSE TO THE COURT'S REQUEST FOR SUPPLEMENTAL BRIEFING RE: MOTION TO DISMISS CAUSES OF ACTION NOS. 13 AND 14 IN PLAINTIFF'S FIRST AMENDED COMPLAINT

Date: July 12, 2013
Time: 10:00 A.M.
Courtroom: 6, 17th Floor
Hon. Charles R. Breyer

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

Page(s)

CASES

FEDERAL STATUTES

CALIFORNIA STATUTES

OTHER AUTHORITIES

LEGISLATIVE MATERIALS

INTRODUCTION

Congress passed the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, in 1986 to deter computer hacking and prohibit "intentionally trespassing into someone else's computer files." S.Rep. No. 99-432, at 9 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2487. But in the nearly three decades since its original enactment, the CFAA, and its state law counterpart, the California Comprehensive Computer Data Access and Fraud Act, California Penal Code § 502, have been stretched to cover all sorts of non-hacking behavior.

This case perhaps represents the zenith of this trend: plaintiff craigslist, Inc. ("Craigslist") alleges defendant 3Taps Inc. ("3Taps") violated the CFAA and Penal Code § 502 by copying data on Craigslist's publicly available website and then republishing that information on its own website. Imposing CFAA liability under these circumstances means that it can now become criminal to copy and paste data from a publicly available website intended to be seen by as many people as possible on the Internet. A person using Craigslist to look for an apartment is authorized to write notes on a pen and paper, or manually plot apartment listings on a paper map. The same behavior should not be treated as criminal simply because it was done with a computer.

For the reasons that follow, amici urge this Court to grant defendants' motion to dismiss the CFAA and Penal Code § 502 claims in the complaint.

INTEREST OF AMICI

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported civil liberties organization working to protect free speech and privacy rights in the online world. With more than 21,000 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, and publishes a comprehensive archive of digital civil liberties information at www.eff.org. EFF is particularly interested in ensuring the proper application of the CFAA and state computer crime laws, as well as maintaining constitutional protections for criminal defendants. Toward this end, EFF has filed amicus briefs in cases involving the CFAA such as *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc), *United States v. Cioni*, 649 F.3d 276 (4th Cir. 2011), *Facebook v.*

Power Ventures Inc., 844 F. Supp. 2d 1025 (N.D. Cal. 2012), *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) and *Facebook v. Power Ventures Inc*., 2010 WL 3291750 (N.D. Ca. Jul. 20, 2010) (unpublished).

Christine Suzanne Davik (a.k.a. Christine Davik Galbraith) is a professor at the University of Maine School of Law who teaches and writes about cyberspace, including issues related to the control of information and the CFAA. She is especially concerned about the treatment of non-copyrightable data on publicly available websites and the continued openness of the Internet.

Jennifer Granick is the Director of Civil Liberties at the Stanford Center for Internet and Society. Jennifer practices, speaks and writes about free expression, computer crime and security, electronic surveillance, consumer privacy, data protection, copyright, trademark and the Digital Millennium Copyright Act. She is a well-known lawyer for computer security researchers, hackers and innovative businesses and has served as defense counsel in many cases where individuals or businesses have been accused of violating the CFAA and its state law corollaries. She has filed amicus briefs in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc), *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) and other CFAA cases. Her First Amendment work has focused on the democratic and competitive importance of the free flow of unprotected public information.

Jordan Kovnot is Interim Director of the Center for Law and Information Policy ("CLIP") at Fordham University School of Law. His research work is focused largely on liability for Internet intermediaries and privacy law, specifically issues surrounding children's privacy. Jordan created CLIP's privacy education program - a series of lessons on privacy and technology use designed for middle school students. He has been featured on WNYC's *New Tech City* discussing concerns about the over-application of the CFAA. He signs on in his personal capacity, and his signature does not imply the endorsement of Fordham University or CLIP.

Stephen Schultze is Associate Director of the Center for Information Technology Policy at Princeton University. He is a scholar of Internet law and policy, and commentator on the CFAA and its state counterparts. His work documents the importance of well-established safe harbors for Internet intermediaries and users, and examines how overreach of certain laws can chill speech and

innovation. He signs on in his personal capacity, and his signature does not imply the endorsement of Princeton University.

No one, except for the *amici*, has authored the brief in whole or in part, or contributed money towards the preparation of this brief.[1] No party has objected to the filing of this brief.

STATEMENT OF FACTS

Both the CFAA and its state law counterpart, California Penal Code § 502, impose civil and criminal penalties on anyone who "intentionally accesses a computer without authorization or exceeds authorized access" and obtains "information from any protected computer." 18 U.S.C. § 1030(a)(2), (C); *see Multiven, Inc. v. Cisco Sys., Inc*., 725 F. Supp. 2d 887, 895 (N.D. Cal. 2010) (CFAA and Penal Code § 502 have same elements).[2] Craigslist alleges 3Taps violated the CFAA and Penal Code § 502 by taking information from Craigslist's listings – information publicly available to anyone on the Internet – and aggregating and republishing that information in defendant's own website. *Craigslist Inc. v. 3Taps Inc.*, --- F. Supp. 2d ----, 2013 WL 1819999, *1-2 (N.D. Cal. April 30, 2013).

According to Craigslist, defendants acted "without authorization" because Craigslist' terms of use restrict the use of the Craigslist website (craigslist.org) and grant Craigslist a broad license to use and republish the content submitted by its users. *Craigslist*, 2013 WL 1819999, at *1, 3. As this Court correctly noted, however, Craigslist's allegation is essentially that defendants' violated "use" restrictions rather than "access" restrictions. *Id.* at *4. Specifically, this Court recognized that Craigslist's terms of use did not restrict "who may access information, what information may be accessed, or the methods by which information may be accessed." *Id*. Rather, all the Craigslist terms of use did was limit the purpose for which information on its website could be used. This Court was bound by the Ninth Circuit's decision in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc) which found "the plain language of the CFAA 'target[s] the unauthorized

[1] Craigslist has donated to EFF in the past and its founder, Craig Newmark, is a member of EFF's Advisory Board. Prior to filing this brief, EFF has had discussions with Craigslist, PadMapper and 3Taps regarding this litigation.

[2] Because the CFAA and Penal Code § 502 claims rely on the same legal analysis, in this brief all references to the CFAA also refer to Penal Code § 502 as well.

procurement or alteration of information, not its misuse or misappropriation.'" *Nosal*, 676 F.3d at 863 (quoting *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008)); *see also id.* at 862 (rejecting the "interpretation of the CFAA [under which] posting for sale an item prohibited by Craigslist's policy … will earn you a handsome orange jumpsuit.")

This Court, however, refused to dismiss the CFAA claims because it found the defendants were not authorized to access Craigslist for two reasons: first, Craigslist sent cease and desist letters to defendants to inform them they were "no longer authorized to access . . . craigslist's website or services for any reason." *Craigslist*, 2013 WL 1819999, at *2. Second, Craigslist used "technological measures" to block defendants' access to Craigslist site by blocking IP addresses associated with 3Taps, which 3Taps then bypassed by using different IP addresses and proxy servers. *Id.* at *4.

Despite allowing the CFAA claims to go forward, in a footnote, this Court expressed concern with a fundamental premise of the computer hacking claims: "whether the CFAA applies where the owner of an otherwise publicly available website takes steps to restrict access by specific entities, such as the owner's competitors." *Craigslist*, 2013 WL 1819999, at *4, n. 8. Noting "uncomfortable possibilities" that would allow the CFAA to be "used as a tactical tool to gain business or litigation advantages," this Court nonetheless let the computer hacking claims go forward because of the CFAA's "expansive language." *Id.* (citing *Joseph Oat Holdings, Inc. v. RCM Digesters, Inc.*, 409 Fed. App'x 498, 506 (3d Cir. 2010) ("suits under anti-hacking laws have gone beyond the intended scope of such laws and are increasingly being used as a tactical tool to gain business or litigation advantages")). One month after issuing this ruling, the Court accepted additional briefing on the point. *See* Dkt. 86.

ARGUMENT

The CFAA does not and should not impose liability on anyone who accesses information publicly available on the Internet. Because the CFAA and Penal Code § 502 imposes both civil and criminal liability, it must be interpreted narrowly. That means information on a publicly accessible website can be accessed by anyone on the Internet without running afoul of criminal computer

hacking laws. In the absence of access, as opposed to use, restrictions, Craigslist cannot use these anti-hacking laws to complain when the information it voluntarily broadcasts to the world is accessed, even if it is upset about a competing or complementary business.

Therefore, *amici* respectfully urge this Court to dismiss the CFAA and Penal Code § 502 claims.[3]

A. Because the CFAA and Penal Code 502 are Criminal Statutes Too, They Must Be Interpreted Narrowly.

This Court correctly recognized that the rule of lenity applies here because although this is a civil dispute, the CFAA is also a criminal statute, and permitting Craigslist's computer hacking claims to go forward would also mean creating criminal liability. *Craigslist*, 2013 WL 1819999, at *3, n. 4. Yet despite this recognition of the need to proceed cautiously, this Court also noted the "expansive language" of the CFAA meant it covered "owner-imposed restriction on access to otherwise public information on public websites." *Craigslist*, 2013 WL 1819999, at *4, n. 8. But this Court should reconsider this holding and the new criminal liability it has created.

Criminal statutes must be interpreted narrowly to avoid vagueness. *United States v. Skilling*, --- U.S.----, 130 S. Ct. 2896, 2927-28 (2010); *Kolender v. Lawson*, 461 U.S. 352, 357 (1983). Vagueness in criminal law creates two impermissible problems; it fails to put people on notice what is prohibited and it can encourage "arbitrary and discriminatory enforcement." *Chicago v. Morales*, 527 U.S. 41, 56 (1999) (Stevens, J., plurality opinion). Instead, laws must provide

[3] This brief is concerned solely with the issue raised in footnote 8: whether the CFAA and Penal Code § 502 prohibit accessing information on a publicly accessible website. But *amici* are also troubled by the Court's conclusion that, assuming the CFAA and Penal Code § 502 reached publicly accessible information, defendants are potentially liable because the cease and desist letters sent by Craigslist to defendant, as well as the blocking of defendants IP address by Craigslist, meant defendants were not "authorized" to access information on Craigslist's publicly available site. *See Craigslist*, 2013 WL 1819999, at *4. Cease and desist letters are just a variation of the use restrictions struck down by *Nosal* and cannot be the basis of CFAA or Penal Code § 502 liability because it permits private entities to dictate what is and is not a crime based on their own business interests. IP address blocking and other technical measures put in place to enforce use restrictions – as opposed to access restrictions – are no different than terms of use or a cease and desist letter. That means under *Nosal*, blocking an IP address cannot make access to data "unauthorized." *Amici* would be more than happy to submit additional briefing on these points should the Court request it.

"explicit standards for those who apply them" because vague laws "impermissibly delegate[] basic policy matters to policemen, judges, and juries for resolution on an ad hoc and subjective basis." *Grayned v. Rockford*, 408 U.S. 104, 108-09 (1972).

These fears are especially pronounced when it comes to the CFAA. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561 (2010). In the Ninth Circuit, a statute must "define the offense with sufficient definiteness that ordinary people can understand what conduct is prohibited" and "establish standards to permit police to enforce the law in a non-arbitrary, non-discriminatory manner." *United States v. Sutcliffe*, 505 F.3d 944, 953 (9th Cir. 2007) (quotations omitted). That was the underlying concern in *Nosal*, where the Ninth Circuit worried "significant notice problems arise if we allow criminal liability to turn on the vagaries of private policies that are lengthy, opaque, subject to change and seldom read." *Nosal*, 676 F.3d at 860. This was especially true because "[b]asing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved." *Id.*

But although Craigslist's claims that its terms of use create liability under the CFAA necessarily fail under *Nosal*, applying the CFAA to protect information publicly available on the web results in the same problem: the public would be unable to distinguish in a meaningful and principled way between innocent and criminal activity, which is a constitutional harm. *See Foti v. City of Menlo Park*, 146 F.3d 629, 638 (9th Cir. 1998). It implicates the same concern the Ninth Circuit had in *Nosal*: that companies can "transform whole categories of otherwise innocuous behavior into federal crimes." *Nosal*, 676 F.3d at 860.

Nosal's concern about use restrictions is even more pronounced when it comes to information on publicly accessible websites; simply viewing information on a website is the most innocuous of Internet behavior.

B. Everyone Is "Authorized" to Access Information That is Publicly Available on the Internet.

It is fundamental to remember that websites are generally open and available to the public. When a website owner publishes information on the World Wide Web, they are authorizing others

to view that information. *See United States v. Gines-Peres*, 214 F. Supp. 2d 205, 225 (D.P.R. 2002) (placing information on Internet "subjects said information to being accessed by every conceivable interested party" unless "protective measures or devices" control access). That is a major purpose of the Internet: to freely disseminate information and data to people all over the world.

To the extent someone opts to make a website publically available to virtually everybody with an Internet connection, the site's owner must accordingly relinquish its ability to use a criminal anti-hacking law to enforce who may access and view its contents. Along with the numerous attendant benefits that come from having a public presence on the Internet, website owners should necessarily expect to tolerate some loss of autonomy that the owner of a password protected computer system retains.

But benefits to this openness remain and Craigslist itself is a notable example of these benefits. Craigslist provides a popular and wide reaching classified advertising service, allowing people to post mostly free[4] classified ads that can be seen by anyone anywhere in the world without charge. Craigslist claims that 60 million people use Craigslist in the United States each month, that 100 million classified ads are posted each month and that the site receives 50 billion page views per month. It receives 2 million new job postings a month, supports advertisements posted in 13 different languages and has more than 700 local sites in 70 countries.[5] It is one of the 25 most visited websites in the United States.[6]

Craigslist's enormous success is a result of its openness: anyone anywhere can access any of its websites and obtain information about apartments for rent, new jobs or cars for sale. Its openness means that Craigslist is the go to place on the web for classified ads; it users post on Craigslist because they know their ads will reach the largest audience.

But what Craigslist is trying to do here is to use the CFAA's provisions to enforce the

[4] *See* Craigslist, *about* > *help* > *posting fees*, available at http://www.craigslist.org/about/help/posting_fees, last visited June 17, 2013.

[5] *See* Craigslist, *about* > *factsheet*, available at http://www.craigslist.org/about/factsheet, last visited June 17, 2013.

[6] *See* Press Release, "comScore Announces U.S. Launch of Media Metrix® Multi-Platform to Deliver Unified View of Desktop, Smartphone and Tablet Audience," available at http://www.comscore.com/Insights/Press_Releases/2013/3/comScore_Announces_US_Launch_of_Media_Metrix_Multi-Platform, last visited June 17 2013.

unilateral determinations it has made concerning access to its website, an Internet site that it has already chosen to open up to the general public, attempting to turn a law against computer hacking into a new tool. But prohibiting access to an otherwise publicly available website is not the type of harm that Congress intended to be proscribed in the CFAA, and nowhere in the legislative history is there any suggestion that the CFAA was drafted to grant website owners such unbridled discretion. *See generally* Christine Davik Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 Md. L. Rev. 320, 330-31 (1996) (citing S. Rep. No. 104-357 at 3 (1996)). Commentators have long complained that the CFAA was not intended to prohibit access to an otherwise publicly available website. *See e.g.* Mark A. Lemley, *Place and Cyberspace*, 91 Cal. L. Rev. 521, 528 (2003) ("An even more serious problem is the judicial application of the [CFAA], which was designed to punish malicious hackers, to make it illegal—indeed, criminal—to seek information from a publicly available website if doing so would violate the terms of a 'browsewrap' license.").

A growing number of courts have reached the same conclusion too. Finding individuals who access information on a publicly available website have "authorization" to obtain that data under the CFAA. *See Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 304 (6th Cir. 2011) ("like an unprotected website, Pulte's phone and e-mail systems '[were] open to the public, so [LIUNA] was authorized to use [them].'") (quoting *Int'l Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006)); *see also Cvent, Inc. v. Eventbrite, Inc.*, 739 F. Supp. 2d 927, 932 (E.D. Va. 2010) (cannot exceed authority access to information because data "is publicly available on the Internet, without requiring any login, password, or other individualized grant of access"); *Lockheed Martin Corp. v. Speed*, No. 6:05–CV1580–ORL–31, 2006 WL 2683058, at *5 (M.D.Fla. Aug. 1, 2006) (unpublished) ("without authorization" in CFAA means "no permission to access whatsoever"). And if a visitor to a website is "authorized" to access freely available data, there can be no CFAA liability.

Of course, Craigslist has the right to restrict access to its data through, for example, requiring a username and login, which would password protect access to its other users' advertisements. If defendants bypassed that security measure by trying to break through this barrier

by systematically attempting passwords or "hacking" their way in through some other method, then their access to Craigslist would necessarily have been "unauthorized." *See United States v. Morris*, 928 F.2d 504, 510 (2d. Cir. 1991) (running computer script to guess passwords and gain access to private accounts was "unauthorized" access); *United States v. Phillips*, 477 F.3d 215, 220 (5th Cir. 2007) (guessing password to enter password-protected area of website was "unauthorized access").

But once Craigslist chose not to password protect its data – a decision that would undercut Craigslist's successful business model – it necessarily authorized the public to view the information on the public website.

That includes business competitors. Even if Craigslist did not want 3Taps to use the information on Craigslist's site in the way it did, 3Taps was still as "authorized" to view the data as any other visitor. The First Circuit dealt with a similar situation in *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003). There, Zefer used an automated scraper program to obtain pricing data publicly available on EF's website. 318 F.3d at 60. Recognizing there was "no doubt" that EF would be unhappy with its competitor's practice, that in and of itself did not make Zefer's access to the information "unauthorized." *Id.* at 63. Once EF made the information publicly available on the web for anyone to see, it had no right to complain about the use of its data. Noting that EF would have also "disliked the compilation of such a database manually without the use of a scraper tool," – with a pen or paper for example – it did not and could not "exclude competitors from looking at its website and any such limitation would raise serious public policy concerns." *Id.*

The same public policy concerns are present here as this Court noted.[7] Any member of the public, including defendants, could have manually written down the information in a Craigslist posting and organized that data however it wanted. Just because defendants automated that process to create its services does not make its access to this data "unauthorized." Stated differently, the CFAA does not provide publically accessible website owners with the ability to legally compel

[7] This Court reached the same conclusion as the First Circuit in *EF Cultural Travel*. *See Craigslist*, 2013 WL 1819999, at *4, n. 8 ("Applying the CFAA to publicly available website information presents uncomfortable possibilities. Any corporation could subject its competitors to civil *and criminal* liability for visiting its otherwise publicly available home page; in theory, a major news outlet could seek criminal charges against competing journalists for reading articles on its website.") (emphasis in original).

adherence to their mere predilections over whom or what constitutes an "undesirable" or "authorized" visitor, nor should it.

Applying the CFAA this way would set a dangerous precedent and have serious implications on competition, innovation, and the continued openness of the Internet to the public's detriment. In many instances, factual data contained on a public site provides the basis for more effective competition against the Internet site owner, and in many others it facilitates complimentary services. Despite a website owner's views to the contrary, such activities are desirable. *See* Davik, 63 Md. L. Rev. at 365; *see also* Niva Elkin-Koren, *Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing*, 26 U. Dayton L. Rev. 179, 182 (2001). But using a criminal law to prohibit defendants—or anyone else—from obtaining publically available information from the Internet would impair legitimate competition to the detriment of the general public. Restrictions on access would likely prevent add-on innovation by third-parties, leaving consumers with less options in the marketplace, allowing the current market leader to continue to dominate. Reduced purchasing choice is not in the best interests for consumers.

Moreover, allowing the CFAA to regulate access to information publicly available on the Internet runs into the same vagueness problems the Ninth Circuit was concerned about in *Nosal*. Consider an example from Professor Orin Kerr:

> Imagine that a website owner announces that only right-handed people can view his website, or perhaps only friendly people. Under the contract-based approach, a visit to the site by a left-handed or surly person is an unauthorized access that may trigger state and federal criminal laws. A computer owner could set up a public web page, announce that "no one is allowed to visit my web page," and then refer for prosecution anyone who clicks on the site out of curiosity. By granting the computer owner essentially unlimited authority to define authorization, the contract standard delegates the scope of criminality to every computer owner.

Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1650-51 (2003). If information is publicly available to anyone on the World Wide Web, how can an Internet user discern which websites they can view and take down information from, and those they cannot? As the Eleventh Circuit has noted, liability in cases involving "electronic communications available through the Web" must be demonstrated by showing "communications are not readily accessible" because if visiting an

"otherwise publicly accessible webpage" creates liability, then the "floodgates of litigation would open and the merely curious would be prosecuted." *Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1321 (11th Cir. 2006). The CFAA should not be stretched this way.

As a result, Craigslist's CFAA and Penal Code § 502 claims must be dismissed.

CONCLUSION

Craigslist is a great example of the Internet's ability to make information reachable to millions of far flung people. People who use the Internet should not be saddled with the threat of civil and criminal liability for observing and using – really "accessing" – public information on the web. For the reasons stated above, therefore, this Court should dismiss Craigslist's CFAA and Penal Code § 502 claims.

DATED: June 18, 2013

Respectfully submitted,

ELECTRONIC FRONTIER FOUNDATION

By: */s/ Hanni Fakhoury*

HANNI FAKHOURY
hanni@eff.org
KURT OPSAHL
kurt@eff.org
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993

Attorneys for *Amici Curiae*
ELECTRONIC FRONTIER FOUNDATION AND LAW PROFS. CHRISTINE DAVIK, JENNIFER GRANICK, JORDAN KOVNOT AND STEPHEN SCHULTZE