

Utah Cyber Symposium

September 17, 2010

Breakout Session

“Looking Forward: A Discussion of Hot Topics in Cyberlaw from Consumer and Business Perspectives”

Moderator: Charles Lee Mudd Jr. – Mudd Law Offices

Panelists: Marcia Hofmann – Electronic Frontier Foundation
Jeremiah Johnston – Sedo

I. Introduction

II. Section 230 of the Communications Decency Act - Marcia Hoffman

III. Conflicts of Laws - IP and Domain Names - Jeremiah Johnston

IV. More Assets - Consumer Data - Marcia Hoffman

V. Affect on Entrepreneurial Activity - Jeremiah Johnston

VI. The Future and Final Comments – Panelists and Audience Members

LEXSTAT 47 U.S.C. § 230

UNITED STATES CODE SERVICE
Copyright © 2010 Matthew Bender & Company, Inc.
a member of the LexisNexis Group (TM)
All rights reserved.

*** CURRENT THROUGH PL 111-237, APPROVED 8/16/2010 ***

TITLE 47. TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS
CHAPTER 5. WIRE OR RADIO COMMUNICATION
COMMON CARRIERS
COMMON CARRIER REGULATION

Go to the United States Code Service Archive Directory

47 USCS § 230

§ 230. Protection for private blocking and screening of offensive material

(a) Findings. The Congress finds the following:

- (1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.
- (2) These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops.
- (3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.
- (4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.
- (5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

(b) Policy. It is the policy of the United States--

- (1) to promote the continued development of the Internet and other interactive computer services and other interactive media;
- (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;
- (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;
- (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and
- (5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

(c) Protection for "Good Samaritan" blocking and screening of offensive material.

- (1) Treatment of publisher or speaker. No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
- (2) Civil liability. No provider or user of an interactive computer service shall be held liable on account of--
 - (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user

considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1) [subparagraph (A)].

(d) Obligations of interactive computer service. A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.

(e) Effect on other laws.

(1) No effect on criminal law. Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this Act [47 USCS § 223 or 231], chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, United States Code [18 USCS §§ 1460 et seq. or §§ 2251 et seq.], or any other Federal criminal statute.

(2) No effect on intellectual property law. Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

(3) State law. Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

(4) No effect on communications privacy law. Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law.

(f) Definitions. As used in this section:

(1) Internet. The term "Internet" means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

(2) Interactive computer service. The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

(3) Information content provider. The term "information content provider" means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.

(4) Access software provider. The term "access software provider" means a provider of software (including client or server software), or enabling tools that do any one or more of the following:

(A) filter, screen, allow, or disallow content;

(B) pick, choose, analyze, or digest content; or

(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

HISTORY:

(June 19, 1934, ch 652, Title II, Part I, § 230, as added Feb. 8, 1996, P.L. 104-104, Title V, Subtitle A, § 509, 110 Stat. 137; Oct. 21, 1998, P.L. 105-277, Div C, Title XIV, § 1404(a), 112 Stat. 2681-739.)

HISTORY; ANCILLARY LAWS AND DIRECTIVES

References in text:

The "Electronic Communications Privacy Act of 1986", referred to in this section, is Act Oct. 21, 1896, P.L. 99-508, 100 Stat. 1848. For full classification of such Act, consult USCS Tables volumes.

Explanatory notes:

The bracketed words "subparagraph (A)" have been added in subsec. (c)(2)(B) in order to indicate the reference probably intended by Congress.

Although § 509 of Act Feb. 8, 1996, P.L. 104-104, provided for the addition of this section at the end of Title II of the Communications Act of 1934 (*47 USCS §§ 201 et seq.*), it was added at the end of Part I of such Title (*47 USCS §§ 201 et seq.*) in order to effectuate the probable intent of Congress.

Amendments:

1998. Act Oct. 21, 1998 (effective 30 days after enactment, as provided by § 1406 of such Act, which appears as *47 USCS § 223* note), in subsec. (d)(1), inserted "or 231"; redesignated subsecs. (d) and (e) as subsecs. (e) and (f), respectively; and inserted new subsec. (d).

LEXSEE 521 F.3D 1157

Fair Hous. Council v. Roommates.com, LLC

No. 04-56916, No. 04-57173

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

521 F.3d 1157; 2008 U.S. App. LEXIS 7066; 36 Media L. Rep. 1545

December 12, 2007, Argued and Submitted, Pasadena, California

April 3, 2008, Filed

PRIOR HISTORY: [**1]

Appeal from the United States District Court for the Central District of California. D.C. No. CV-03-09386-PA, D.C. No. CV-03-09386-PA. Percy Anderson, District Judge, Presiding.

Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 489 F.3d 921, 2007 U.S. App. LEXIS 11350 (9th Cir. Cal., 2007)

Fair Hous. Council of San Fernando Valley v. Roommate.com, LLC, 2004 U.S. Dist. LEXIS 27987 (C.D. Cal., Sept. 30, 2004)

DISPOSITION: REVERSED in part, VACATED in part, AFFIRMED in part and REMANDED. NO COSTS.

COUNSEL: Michael Evans, Pescadero, California; Christopher Brancart, Brancart & Brancart, Pescadero, California; Gary Rhoades, Rhoades & Al-Mansour, Los Angeles, California, for the plaintiffs-appellants/cross-appellees.

Timothy L. Alger, Kent J. Bullard, Steven B. Stiglitz and Lesley E. Williams, Quinn Emanuel Urquhart Oliver & Hedges, LLP, Los Angeles, California, for the defendant-appellee/cross-appellant.

Kelli L. Sager, Los Angeles, California; Thomas R. Burke, San Francisco, California; Bruce E. H. Johnson and Ambika K. Doran, Davis Wright Tremaine LLP, Seattle, Washington, for News Organizations as amici curiae in support of the defendant-appellee.

Ann Brick, Margaret C. Crosby and Nicole A. Ozer, American Civil Liberties Union Foundation of Northern California, San Francisco, California, for American Civil Liberties Union of Northern California as amicus curiae

in support of neither party.

John P. Relman, Stephen M. Dane and D. Scott Chang, [**2] Relman & Dane PLLC, Washington, DC; Joseph D. Rich and Nicole Birch, Lawyers' Committee for Civil Rights Under Law, Washington, DC, for National Fair Housing Alliance and Lawyers' Committee for Civil Rights Under Law as amici curiae in support of the plaintiffs-appellants.

JUDGES: Before: Alex Kozinski, Chief Judge, Stephen Reinhardt, Pamela Ann Rymer, Barry G. Silverman, M. Margaret McKeown, William A. Fletcher, Raymond C. Fisher, Richard A. Paez, Carlos T. Bea, Milan D. Smith, Jr. and N. Randy Smith, Circuit Judges. Opinion by Chief Judge Kozinski; Partial Concurrence and Partial Dissent by Judge McKeown McKEOWN, Circuit Judge, with whom RYMER and BEA, Circuit Judges, join, concurring in part and dissenting in part.

OPINION BY: Alex Kozinski

OPINION

[*1161] KOZINSKI, Chief Judge:

We plumb the depths of the immunity provided by *section 230* of the Communications Decency Act of 1996 ("CDA").

Facts

1

1 This appeal is taken from the district court's order granting defendant's motion for summary judgment, so we view contested facts in the light most favorable to plaintiffs. *See Winterrowd v.*

Nelson, 480 F.3d 1181, 1183 n.3 (9th Cir. 2007).

Defendant Roommate.com, LLC ("Roommate") operates a website designed to match people renting [**3] out spare rooms with people looking for a place to live. ² At the time of the district court's disposition, Roommate's website featured approximately 150,000 active listings and received around a million page views a day. Roommate seeks to profit by collecting revenue from advertisers and subscribers.

2 For unknown reasons, the company goes by the singular name "Roommate.com, LLC" but pluralizes its website's URL, www.roommates.com.

Before subscribers can search listings or post ³ housing opportunities on Roommate's website, they must create profiles, a process that requires them to answer a series of questions. In addition to requesting basic information--such as name, location and email address--Roommate requires each subscriber to disclose his sex, sexual orientation and whether he would bring children to a household. Each subscriber must also describe his preferences in roommates with respect to the same three criteria: sex, sexual orientation and whether they will bring children to the household. The site also encourages subscribers to provide "Additional Comments" describing themselves and their desired roommate in an open-ended essay. After a new subscriber completes the application, [**4] Roommate assembles his answers into a "profile page." The profile page [**1162] displays the subscriber's pseudonym, his description and his preferences, as divulged through answers to Roommate's questions.

3 In the online context, "posting" refers to providing material that can be viewed by other users, much as one "posts" notices on a physical bulletin board.

Subscribers can choose between two levels of service: Those using the site's free service level can create their own personal profile page, search the profiles of others and send personal email messages. They can also receive periodic emails from Roommate, informing them of available housing opportunities matching their preferences. Subscribers who pay a monthly fee also gain the ability to read emails from other users, and to view other subscribers' "Additional Comments."

The Fair Housing Councils of the San Fernando Valley and San Diego ("Councils") sued Roommate in federal court, alleging that Roommate's business violates the federal Fair Housing Act ("FHA"), 42 U.S.C. § 3601 *et seq.*, and California housing discrimination laws. ⁴ Councils claim that Roommate is effectively a housing broker doing online what it may not lawfully do off-line. [**5] The district court held that Roommate is immune under *section 230 of the CDA*, 47 U.S.C. § 230(c), and dismissed the federal claims without considering whether Roommate's actions violated the FHA. The court then declined to exercise supplemental jurisdiction over the state law claims. Councils appeal the dismissal of the FHA claim and Roommate cross-appeals the denial of attorneys' fees.

4 The Fair Housing Act prohibits certain forms of discrimination on the basis of "race, color, religion, sex, familial status, or national origin." 42 U.S.C. § 3604(c). The California fair housing law prohibits discrimination on the basis of "sexual orientation, marital status, . . . ancestry, . . . source of income, or disability," in addition to reiterating the federally protected classifications. *Cal. Gov. Code* § 12955.

Analysis

Section 230 of the CDA ⁵ immunizes providers of interactive computer services ⁶ against liability arising from content created by third parties: "No provider . . . of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c). ⁷ This grant of immunity applies only if the [**6] interactive computer service provider is not also an "information content provider," which is defined as someone who is "responsible, in whole or in part, for the creation or development of" the offending content. *Id.* § 230(f)(3).

5 The Supreme Court held some portions of the CDA to be unconstitutional. *See Reno v. ACLU*, 521 U.S. 844, 117 S. Ct. 2329, 138 L. Ed. 2d 874 (1997). The portions relevant to this case are still in force.

6 *Section 230* defines an "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server." 47 U.S.C. § 230(f)(2); *see Carafano v.*

Metrosplash.com, Inc., 207 F. Supp. 2d 1055, 1065-66 (C.D. Cal. 2002) (an online dating website is an "interactive computer service" under the CDA), *aff'd*, 339 F.3d 1119 (9th Cir. 2003). Today, the most common interactive computer services are websites. Councils do not dispute that Roommate's website is an interactive computer service.

7 The Act also gives immunity to users of third-party content. This case does not involve any claims against users so we omit all references to user immunity when quoting and analyzing the statutory text.

A website operator [**7] can be both a service provider and a content provider: If it passively displays content that is created entirely by third parties, then it is only a service provider with respect to that content. But as to content that it creates itself, or is "responsible, in whole or in part" for creating or developing, the website is also a content provider. Thus, a website may be immune from liability for [**1163] some of the content it displays to the public but be subject to liability for other content.⁸

8 See, e.g., *Anthony v. Yahoo! Inc.*, 421 F. Supp. 2d 1257, 1262-63 (N.D. Cal. 2006) (Yahoo! is not immune under the CDA for allegedly creating fake profiles on its own dating website).

Section 230 was prompted by a state court case holding Prodigy⁹ responsible for a libelous message posted on one of its financial message boards.¹⁰ See *Stratton Oakmont v. Prodigy Servs. Co.*, 1995 N.Y. Misc. LEXIS 229, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995) (unpublished). The court there found that Prodigy had become a "publisher" under state law because it voluntarily deleted some messages from its message boards "on the basis of offensiveness and 'bad taste,'" and was therefore legally responsible for the content of defamatory messages [**8] that it failed to delete. 1995 N.Y. Misc. LEXIS 229, [WL] at *4. The *Stratton Oakmont* court reasoned that Prodigy's decision to perform some voluntary self-policing made it akin to a newspaper publisher, and thus responsible for messages on its bulletin board that defamed third parties. The court distinguished Prodigy from CompuServe,¹¹ which had been released from liability in a similar defamation case because CompuServe "had no opportunity to review the contents of the publication at issue before it was uploaded

into CompuServe's computer banks." *Id.*; see *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135, 140 (S.D.N.Y. 1991). Under the reasoning of *Stratton Oakmont*, online service providers that voluntarily filter some messages become liable for all messages transmitted, whereas providers that bury their heads in the sand and ignore problematic posts altogether escape liability. Prodigy claimed that the "sheer volume" of message board postings it received--at the time, over 60,000 a day--made manual review of every message impossible; thus, if it were forced to choose between taking responsibility for all messages and deleting no messages at all, it would have to choose the latter course. *Stratton Oakmont*, 1995 N.Y. Misc. LEXIS 229, 1995 WL 323710 at *3. [**9]

9 Prodigy was an online service provider with 2 million users, which seemed like a lot at the time.

10 A "message board" is a system of online discussion allowing users to "post" messages. Messages are organized by topic--such as the "finance" message board at issue in *Stratton Oakmont*--and the system generally allows users to read and reply to messages posted by others.

11 CompuServe was a competing online service provider of the day.

In passing section 230, Congress sought to spare interactive computer services this grim choice by allowing them to perform some editing on user-generated content without thereby becoming liable for all defamatory or otherwise unlawful messages that they didn't edit or delete. In other words, Congress sought to immunize the *removal* of user-generated content, not the *creation* of content: "[S]ection [230] provides 'Good Samaritan' protections from civil liability for providers . . . of an interactive computer service for actions to *restrict* . . . access to objectionable online material. One of the specific purposes of this section is to overrule *Stratton-Oakmont* [sic] v. *Prodigy* and any other similar decisions which have treated such providers . . . as publishers [**10] or speakers of content that is not their own *because they have restricted access* to objectionable material." H.R. Rep. No. 104-458 (1996) (Conf. Rep.), as reprinted in 1996 U.S.C.C.A.N. 10 (emphasis added).¹² Indeed, the section is titled "Protection for 'good samaritan' blocking and [**1164] screening of offensive material" and, as the Seventh Circuit recently held, the substance of section 230(c) can and should be interpreted consistent with its caption. *Chi. Lawyers' Comm. for Civ. Rights Under Law, Inc. v. Craigslist, Inc.*, No. 07- 1101,

519 F.3d 666, 2008 U.S. App. LEXIS 5472, slip op. at 6 (7th Cir. Mar. 14, 2008) (quoting *Doe v. GTE Corp.*, 347 F.3d 655, 659-60 (7th Cir. 2003)).

12 While the Conference Report refers to this as "[o]ne of the specific purposes" of *section 230*, it seems to be the principal or perhaps the only purpose. The report doesn't describe any other purposes, beyond supporting "the important federal policy of empowering parents to determine the content of communications their children receive through interactive computer services." H.R. Rep. No. 104-458, at 194 (1996) (Conf. Rep.), as reprinted in 1996 U.S.C.C.A.N. 10, 207-08.

With this backdrop in mind, we examine three specific functions performed [**11] by Roommate that are alleged to violate the Fair Housing Act and California law.

1. Councils first argue that the questions Roommate poses to prospective subscribers during the registration process violate the Fair Housing Act and the analogous California law. Councils allege that requiring subscribers to disclose their sex, family status and sexual orientation "indicates" an intent to discriminate against them, and thus runs afoul of both the FHA and state law.¹³

13 The Fair Housing Act prohibits any "statement . . . with respect to the sale or rental of a dwelling that *indicates . . . an intention* to make [a] preference, limitation, or discrimination" on the basis of a protected category. 42 U.S.C. § 3604(c) (emphasis added). California law prohibits "any written or oral inquiry concerning the" protected status of a housing seeker. *Cal. Gov. Code* § 12955(b).

Roommate created the questions and choice of answers, and designed its website registration process around them. Therefore, Roommate is undoubtedly the "information content provider" as to the questions and can claim no immunity for posting them on its website, or for forcing subscribers to answer them as a condition of using its [**12] services.

Here03221+60510, we must determine whether Roommate has immunity under the CDA because Councils have at least a plausible claim that5199 Roommate violated state and federal law by merely

posing the questions. We need not decide whether any of Roommate's questions actually violate the Fair Housing Act or California law, or whether they are protected by the *First Amendment* or other constitutional guarantees, see *craigslist*, 2008 U.S. App. LEXIS 5472, *11; we leave those issues for the district court on remand. Rather, we examine the scope of plaintiffs' substantive claims only insofar as necessary to determine whether *section 230* immunity applies. However, we note that asking questions certainly *can* violate the Fair Housing Act and analogous laws in the physical world.¹⁴ For example, a real estate broker may not inquire as to the race of a prospective buyer, and an employer may not inquire as to the religion of a prospective employee. If such questions are unlawful when posed face-to-face or by telephone, they don't magically become lawful when asked electronically online. The Communications Decency Act was not meant to create a lawless no-man's-land on the Internet.¹⁵

14 The Seventh Circuit has expressly [**13] held that inquiring into the race and family status of housing applicants is unlawful. See, e.g., *Jancik v. HUD*, 44 F.3d 553, 557 (7th Cir. 1995).

15 The dissent stresses the importance of the Internet to modern life and commerce, Dissent at 3476, and we, of course, agree: The Internet is no longer a fragile new means of communication that could easily be smothered in the cradle by overzealous enforcement of laws and regulations applicable to brick-and-mortar businesses. Rather, it has become a dominant--perhaps the preeminent--means through which commerce is conducted. And its vast reach into the lives of millions is exactly why we must be careful not to exceed the scope of the immunity provided by Congress and thus give online businesses an unfair advantage over their real-world counterparts, which must comply with laws of general applicability.

[*1165] Councils also claim that requiring subscribers to answer the questions as a condition of using Roommate's services unlawfully "cause[s]" subscribers to make a "statement . . . with respect to the sale or rental of a dwelling that indicates [a] preference, limitation, or discrimination," in violation of 42 U.S.C. § 3604(c). The CDA does not [**14] grant immunity for inducing third parties to express illegal preferences. Roommate's own acts--posting the questionnaire and

requiring answers to it--are entirely its doing and thus *section 230 of the CDA* does not apply to them. Roommate is entitled to no immunity.¹⁶

16 Roommate argues that Councils waived the argument that the questionnaire violated the FHA by failing to properly raise it in the district court. But, under our liberal pleading standard, it was sufficient for Councils in their First Amended Complaint to allege that Roommate "encourages" subscribers to state discriminatory preferences. *See Johnson v. Barker*, 799 F.2d 1396, 1401 (9th Cir. 1986).

2. Councils also charge that Roommate's development and display of subscribers' discriminatory preferences is unlawful. Roommate publishes a "profile page" for each subscriber on its website. The page describes the client's personal information--such as his sex, sexual orientation and whether he has children--as well as the attributes of the housing situation he seeks. The content of these pages is drawn directly from the registration process: For example, Roommate requires subscribers to specify, using a drop-down menu¹⁷ provided [**15] by Roommate, whether they are "Male" or "Female" and then displays that information on the profile page. Roommate also requires subscribers who are listing available housing to disclose whether there are currently "Straight male(s)," "Gay male(s)," "Straight female(s)" or "Lesbian(s)" living in the dwelling. Subscribers who are seeking housing must make a selection from a drop-down menu, again provided by Roommate, to indicate whether they are willing to live with "Straight or gay" males, only with "Straight" males, only with "Gay" males or with "No males." Similarly, Roommate requires subscribers listing housing to disclose whether there are "Children present" or "Children not present" and requires housing seekers to say "I will live with children" or "I will not live with children." Roommate then displays these answers, along with other information, on the subscriber's profile page. This information is obviously included to help subscribers decide which housing opportunities to pursue and which to bypass. In addition, Roommate itself uses this information to channel subscribers away from listings where the individual offering housing has expressed preferences that aren't compatible [**16] with the subscriber's answers.

17 A drop-down menu allows a subscriber to

select answers only from among options provided by the website.

The dissent tilts at windmills when it shows, quite convincingly, that Roommate's *subscribers* are information content providers who create the profiles by picking among options and providing their own answers. Dissent at 3485-88. There is no disagreement on this point. But, the fact that users are information content providers does not preclude Roommate from *also* being an information content provider by helping "develop" at least "in part" the information in the profiles. As we explained in *Batzel*, the party responsible for putting information online may be subject to liability, even if the information originated with a user. *See Batzel v. Smith*, 333 F.3d 1018, 1033 (9th Cir. 2003).¹⁸

18 *See also* discussion of *Batzel* pp. 3466-67 *infra*.

[*1166] Here, the part of the profile that is alleged to offend the Fair Housing Act and state housing discrimination laws--the information about sex, family status and sexual orientation--is provided by subscribers in response to Roommate's questions, which they cannot refuse to answer if they want to use defendant's services. [**17] By requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers, Roommate becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information. And *section 230* provides immunity only if the interactive computer service does not "creat[e] or develop[]" the information "in whole or in part." *See 47 U.S.C. § 230(f)(3)*.

Our dissenting colleague takes a much narrower view of what it means to "develop" information online, and concludes that Roommate does not develop the information because "[a]ll Roommate does is to provide a form with options for standardized answers." Dissent at 3487. But Roommate does much more than provide options. To begin with, it asks discriminatory questions that even the dissent grudgingly admits are not entitled to CDA immunity. Dissent at 3480 n.5. The FHA makes it unlawful to ask certain discriminatory questions for a very good reason: Unlawful questions solicit (a.k.a. "develop") unlawful answers. Not only does Roommate ask these questions, Roommate makes answering the discriminatory questions a condition [**18] of doing

business. This is no different from a real estate broker in real life saying, "Tell me whether you're Jewish or you can find yourself another broker." When a business enterprise extracts such information from potential customers as a condition of accepting them as clients, it is no stretch to say that the enterprise is responsible, at least in part, for developing that information. For the dissent to claim that the information in such circumstances is "created solely by" the customer, and that the business has not helped in the least to develop it, Dissent at 3487-88, strains both credulity and English.¹⁹

19 The dissent may be laboring under a misapprehension as to how the Roommate website is alleged to operate. For example, the dissent spends some time explaining that certain portions of the user profile application are voluntary. Dissent at 3485-87. We do not discuss these because plaintiffs do not base their claims on the voluntary portions of the application, except the "Additional Comments" portion, discussed below, *see pp.* 3471-75 *infra*. The dissent also soft-pedals Roommate's influence on the mandatory portions of the applications by referring to it with such words [***19*] as "encourage" or "encouragement" or "solicitation." Dissent at 3493; *see id.* at 3499. Roommate, of course, does much more than encourage or solicit; it forces users to answer certain questions and thereby provide information that other clients can use to discriminate unlawfully.

Roommate also argues that it is not responsible for the information on the profile page because it is each subscriber's action that leads to publication of his particular profile--in other words, the user pushes the last button or takes the last act before publication. We are not convinced that this is even true,²⁰ but don't see why it matters anyway. The projectionist in the theater may push the last button before a film is displayed on the screen, but surely this doesn't make him the sole producer of [**1167*] the movie. By any reasonable use of the English language, Roommate is "responsible" at least "in part" for each subscriber's profile page, because every such page is a collaborative effort between Roommate and the subscriber.

20 When a prospective subscriber submits his application, Roommate's server presumably checks it to ensure that all required fields are

complete, and that any credit card information is [***20*] not fraudulent or erroneous. Moreover, some algorithm developed by Roommate then decodes the input, transforms it into a profile page and notifies other subscribers of a new applicant or individual offering housing matching their preferences.

Similarly, Roommate is not entitled to CDA immunity for the operation of its search system, which filters listings, or of its email notification system, which directs emails to subscribers according to discriminatory criteria.²¹ Roommate designed its search system so it would steer users based on the preferences and personal characteristics that Roommate itself forces subscribers to disclose. If Roommate has no immunity for asking the discriminatory questions, as we concluded above, *see pp.* 3455-57 *supra*, it can certainly have no immunity for using the answers to the unlawful questions to limit who has access to housing.

21 Other circuits have held that it is unlawful for housing intermediaries to "screen" prospective housing applicants on the basis of race, even if the preferences arise with landlords. *See Jeanty v. McKey & Poague, Inc.*, 496 F.2d 1119, 1120-21 (7th Cir. 1974).

For example, a subscriber who self-identifies as a "Gay male" will [***21*] not receive email notifications of new housing opportunities supplied by owners who limit the universe of acceptable tenants to "Straight male(s)," "Straight female(s)" and "Lesbian(s)." Similarly, subscribers with children will not be notified of new listings where the owner specifies "no children." Councils charge that limiting the information a subscriber can access based on that subscriber's protected status violates the Fair Housing Act and state housing discrimination laws. It is, Councils allege, no different from a real estate broker saying to a client: "Sorry, sir, but I can't show you any listings on this block because you are [gay/female/black/a parent]." If such screening is prohibited when practiced in person or by telephone, we see no reason why Congress would have wanted to make it lawful to profit from it online.

Roommate's search function is similarly designed to steer users based on discriminatory criteria. Roommate's search engine thus differs materially from generic search engines such as Google, Yahoo! and MSN Live Search, in that Roommate designed its system to use allegedly

unlawful criteria so as to limit the results of each search, and to force users to participate [**22] in its discriminatory process. In other words, Councils allege that Roommate's search is designed to make it more difficult or impossible for individuals with certain protected characteristics to find housing--something the law prohibits. By contrast, ordinary search engines do not use unlawful criteria to limit the scope of searches conducted on them, nor are they designed to achieve illegal ends--as Roommate's search function is alleged to do here. Therefore, such search engines play no part in the "development" of any unlawful searches. *See* 47 U.S.C. § 230(f)(3).

It's true that the broadest sense of the term "develop" could include the functions of an ordinary search engine--indeed, just about any function performed by a website. But to read the term so broadly would defeat the purposes of *section 230* by swallowing up every bit of the immunity that the section otherwise provides. At the same time, reading the exception for co-developers as applying only to content that originates entirely with the website--as the dissent would seem to suggest--ignores the words "development . . . in part" in the statutory passage "creation or development in whole or in part." 47 U.S.C. § 230(f)(3) [**23] (emphasis added). We believe that both the immunity for passive conduits and the exception for co-developers must be given their proper scope and, to that end, we interpret the term "development" as referring not merely [1168] to augmenting the content generally, but to materially contributing to its alleged unlawfulness. In other words, a website helps to develop unlawful content, and thus falls within the exception to *section 230*, if it contributes materially to the alleged illegality of the conduct.

The dissent accuses us of "rac[ing] past the plain language of the statute," dissent at 3493, but we clearly do pay close attention to the statutory language, particularly the word "develop," which we spend many pages exploring. The dissent may disagree with our definition of the term, which is entirely fair, but surely our dissenting colleague is mistaken in suggesting we ignore the term. Nor is the statutory language quite as plain as the dissent would have it. Dissent at 3491-93. Quoting selectively from the dictionary, the dissent comes up with an exceedingly narrow definition of this rather complex and multi faceted term.²² Dissent at 3491 (defining development as "gradual advance or growth [**24] through progressive changes") (quoting *Webster's*

Third New International Dictionary 618 (2002)). The dissent does not pause to consider how such a definition could apply to website content at all, as it excludes the kinds of swift and disorderly changes that are the hallmark of growth on the Internet. Had our dissenting colleague looked just a few lines lower on the same page of the same edition of the same dictionary, she would have found another definition of "development" that is far more suitable to the context in which we operate: "making usable or available." *Id.* The dissent does not explain why the definition it has chosen reflects the statute's "plain meaning," while the ones it bypasses do not.

22 Development, it will be recalled, has many meanings, which differ materially depending on context. Thus, "development" when used as part of the phrase "research and development" means something quite different than when referring to "mental development," and something else again when referring to "real estate development," "musical development" or "economic development."

More fundamentally, the dissent does nothing at all to grapple with the difficult statutory problem posed by the [**25] fact that *section 230(c)* uses both "create" and "develop" as separate bases for loss of immunity. Everything that the dissent includes within its cramped definition of "development" fits just as easily within the definition of "creation"--which renders the term "development" superfluous. The dissent makes no attempt to explain or offer examples as to how its interpretation of the statute leaves room for "development" as a separate basis for a website to lose its immunity, yet we are advised by the Supreme Court that we must give meaning to all statutory terms, avoiding redundancy or duplication wherever possible. *See Park 'N Fly, Inc. v. Dollar Park & Fly, Inc.*, 469 U.S. 189, 197, 105 S. Ct. 658, 83 L. Ed. 2d 582 (1985).

While content to pluck the "plain meaning" of the statute from a dictionary definition that predates the Internet by decades, *compare Webster's Third New International Dictionary* 618 (1963) with *Webster's Third New International Dictionary* 618 (2002) (both containing "gradual advance or growth through progressive changes"), the dissent overlooks the far more relevant definition of "[web] content development" in Wikipedia: "the process of researching, writing,

gathering, organizing and editing information [**26] for publication on web sites." Wikipedia, Content Development (Web), http://en.wikipedia.org/w/index.php?title=Content_development_%28web%29&oldid=18844503 (last visited Mar. 19, 2008). Our interpretation of "development" is entirely in line with the context-appropriate meaning of the term, [*1169] and easily fits the activities Roommate engages in.

In an abundance of caution, and to avoid the kind of misunderstanding the dissent seems to encourage, we offer a few examples to elucidate what does and does not amount to "development" under *section 230* of the Communications Decency Act: If an individual uses an ordinary search engine to query for a "white roommate," the search engine has not contributed to any alleged unlawfulness in the individual's conduct; providing *neutral* tools to carry out what may be unlawful or illicit searches does not amount to "development" for purposes of the immunity exception. A dating website that requires users to enter their sex, race, religion and marital status through drop-down menus, and that provides means for users to search along the same lines, retains its CDA immunity insofar as it does not contribute to any alleged illegality;²³ this immunity is retained [**27] even if the website is sued for libel based on these characteristics because the website would not have contributed materially to any alleged defamation. Similarly, a housing website that allows users to specify whether they will or will not receive emails by means of *user-defined* criteria might help some users exclude email from other users of a particular race or sex. However, that website would be immune, so long as it does not require the use of discriminatory criteria. A website operator who edits user-created content--such as by correcting spelling, removing obscenity or trimming for length--retains his immunity for any illegality in the user-created content, provided that the edits are unrelated to the illegality. However, a website operator who edits in a manner that contributes to the alleged illegality--such as by removing the word "not" from a user's message reading "[Name] did *not* steal the artwork" in order to transform an innocent message into a libelous one--is directly involved in the alleged illegality and thus not immune.²⁴

23 It is perfectly legal to discriminate along those lines in dating, and thus there can be no claim based solely on the content of these questions. [**28]

24 Requiring website owners to refrain from

taking affirmative acts that are unlawful does not strike us as an undue burden. These are, after all, businesses that are being held responsible only for their own conduct, not for the no vicarious liability for the misconduct of their customers. Compliance with laws of general applicability seems like an entirely justified burden for all businesses, whether they operate online or through quaint brick-and-mortar facilities. Insofar, however, as a plaintiff would bring a claim under state or federal law based on a website operator's passive acquiescence in the misconduct of its users, the website operator would likely be entitled to CDA immunity. This is true even if the users committed their misconduct using electronic tools of general applicability provided by the website operator.

Here, Roommate's connection to the discriminatory filtering process is direct and palpable: Roommate designed its search and email systems to limit the listings available to subscribers based on sex, sexual orientation and presence of children.²⁵ Roommate selected the criteria used to hide listings, and Councils allege that the act of hiding certain listings is [**29] itself unlawful under the Fair Housing Act, which prohibits brokers from steering clients in accordance with discriminatory [*1170] preferences.²⁶ We need not decide the merits of Councils' claim to hold that Roommate is sufficiently involved with the design and operation of the search and email systems--which are engineered to limit access to housing on the basis of the protected characteristics elicited by the registration process--so as to forfeit any immunity to which it was otherwise entitled under *section 230*.

25 Of course, the logic of Roommate's argument is not limited to discrimination based on these particular criteria. If Roommate were free to discriminate in providing housing services based on sex, there is no reason another website could not discriminate based on race, religion or national origin. Nor is its logic limited to housing; it would apply equally to websites providing employment or educational opportunities--or anything else, for that matter.

26 The dissent argues that Roommate is not liable because the decision to discriminate on these grounds does not originate with Roommate; instead, "users have chosen to select

characteristics that they find desirable." Dissent at 3493. [**30] But, it is Roommate that *forces* users to express a preference and Roommate that forces users to disclose the information that can form the basis of discrimination by others. Thus, Roommate makes discrimination both possible and respectable.

Roommate's situation stands in stark contrast to *Stratton Oakmont*, the case Congress sought to reverse through passage of *section 230*. There, defendant Prodigy was held liable for a user's unsolicited message because it attempted to *remove* some problematic content from its website, but didn't remove enough. Here, Roommate is not being sued for removing some harmful messages while failing to remove others; instead, it is being sued for the predictable consequences of creating a website designed to solicit and enforce housing preferences that are alleged to be illegal.

We take this opportunity to clarify two of our previous rulings regarding the scope of *section 230* immunity. Today's holding sheds additional light on *Batzel v. Smith*, 333 F.3d 1018 (9th Cir. 2003). There, the editor of an email newsletter received a tip about some artwork, which the tipster falsely alleged to be stolen. The newsletter editor incorporated the tipster's email into the [**31] next issue of his newsletter and added a short headnote, which he then emailed to his subscribers.²⁷ The art owner sued for libel and a split panel held the newsletter editor to be immune under *section 230 of the CDA*.²⁸

27 Apparently, it was common practice for this editor to receive and forward tips from his subscribers. In effect, the newsletter served as a heavily moderated discussion list.

28 As an initial matter, the *Batzel* panel held that the defendant newsletter editor was a "user" of an interactive computer service within the definition provided by *section 230*. While we have our doubts, we express no view on this issue because it is not presented to us. See p. 3452 n.7 *supra*. Thus, we assume that the editor fell within the scope of *section 230's* coverage without endorsing *Batzel's* analysis on this point.

Our opinion is entirely consistent with that part of *Batzel* which holds that an editor's minor changes to the spelling, grammar and length of third-party content do not strip him of *section 230* immunity. None of those

changes contributed to the libelousness of the message, so they do not add up to "development" as we interpret the term. See pp. 3461-64 *supra*. *Batzel* went on [**32] to hold that the editor *could* be liable for selecting the tipster's email for inclusion in the newsletter, depending on whether or not the tipster had tendered the piece to the editor for posting online, and remanded for a determination of that issue. *Batzel*, 333 F.3d at 1035.

The distinction drawn by *Batzel* anticipated the approach we take today. As *Batzel* explained, if the tipster tendered the material for posting online, then the editor's job was, essentially, to determine whether or not to prevent its posting--precisely the kind of activity for which *section 230* was meant to provide immunity.²⁹ And any activity that can be boiled [**1171] down to deciding whether to exclude material that third parties seek to post online is perforce immune under *section 230*. See p. 3468-69 & n.32 *infra*. But if the editor publishes material that he does not believe was tendered to him for posting online, then he is the one making the affirmative decision to publish, and so he contributes materially to its allegedly unlawful dissemination. He is thus properly deemed a developer and not entitled to CDA immunity. See *Batzel*, 333 F.3d at 1033.³⁰

29 As *Batzel* pointed out, there can be no meaningful difference [**33] between an editor starting with a default rule of publishing all submissions and then manually selecting material to be removed from publication, and a default rule of publishing no submissions and manually selecting material to be published--they are flip sides of precisely the same coin. *Batzel*, 333 F.3d at 1032 ("The scope of [section 230] immunity cannot turn on whether the publisher approaches the selection process as one of inclusion or removal, as the difference is one of method or degree, not substance.").

30 The dissent scores a debater's point by noting that the same activity might amount to "development" or not, depending on whether it contributes materially to the illegality of the content. Dissent at 3489. But we are not defining "development" for all purposes; we are defining the term only for purposes of determining whether the defendant is entitled to immunity for a particular act. This definition does not depend on finding substantive liability, but merely requires analyzing the context in which a claim is brought.

A finding that a defendant is not immune is quite distinct from finding liability: On remand, Roommate may still assert other defenses to liability under [*34] the Fair Housing Act, or argue that its actions do not violate the Fair Housing Act at all. Our holding is limited to a determination that the CDA provides no immunity to Roommate's actions in soliciting and developing the content of its website; whether that content is in fact illegal is a question we leave to the district court.

We must also clarify the reasoning undergirding our holding in *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119 (9th Cir. 2003), as we used language there that was unduly broad. In *Carafano*, an unknown prankster impersonating actress Christianne Carafano created a profile for her on an online dating site. The profile included Carafano's home address and suggested that she was looking for an unconventional liaison. When Carafano received threatening phone calls, she sued the dating site for publishing the unauthorized profile. The site asserted immunity under section 230. We correctly held that the website was immune, but incorrectly suggested that it could never be liable because "no [dating] profile has any content until a user actively creates it." *Id.* at 1124. As we explain above, see pp. 3458-64 *supra*, even if the data are supplied by third parties, a [*35] website operator may still contribute to the content's illegality and thus be liable as a developer.³¹ Providing immunity every time a website uses data initially obtained from third parties would eviscerate the exception to section 230 for "develop[ing]" unlawful content "in whole or in part." 47 U.S.C. § 230(f)(3).

31 We disavow any suggestion that *Carafano* holds an information content provider automatically immune so long as the content originated with another information content provider. 339 F.3d at 1125.

We believe a more plausible rationale for the unquestionably correct result in *Carafano* is this: The allegedly libelous content there--the false implication that Carafano was unchaste--was created and developed entirely by the malevolent user, without prompting or help from the website operator. To be sure, the website provided neutral tools, which the anonymous dastard used to publish the libel, but the website did absolutely nothing to encourage the posting of defamatory

content--indeed, the defamatory posting was contrary to the website's express policies. The claim against the website was, in effect, that it failed to review each user-created profile to ensure that it wasn't [*36] defamatory. That is precisely the kind of [*1172] activity for which Congress intended to grant absolution with the passage of section 230. With respect to the defamatory content, the website operator was merely a passive conduit and thus could not be held liable for failing to detect and remove it.³²

32 Section 230 requires us to scrutinize particularly closely any claim that can be boiled down to the failure of an interactive computer service to edit or block user-generated content that it believes was tendered for posting online, see pp. 3466-67 *supra*, as that is the very activity Congress sought to immunize by passing the section. See pp. 3453-55 *supra*.

By contrast, Roommate both elicits the allegedly illegal content and makes aggressive use of it in conducting its business. Roommate does not merely provide a framework that could be utilized for proper or improper purposes; rather, Roommate's work in developing the discriminatory questions, discriminatory answers and discriminatory search mechanism is directly related to the alleged illegality of the site. Unlike *Carafano*, where the website operator had nothing to do with the user's decision to enter a celebrity's name and personal information [*37] in an otherwise licit dating service, here, Roommate is directly involved with developing and enforcing a system that subjects subscribers to allegedly discriminatory housing practices.

Our ruling today also dovetails with another facet of *Carafano*: The mere fact that an interactive computer service "classifies user characteristics . . . does not transform [it] into a 'developer' of the 'underlying misinformation.'" *Carafano*, 339 F.3d at 1124. *Carafano*, like *Batzel*, correctly anticipated our common-sense interpretation of the term "develop[]" in section 230. Of course, any classification of information, like the sorting of dating profiles by the type of relationship sought in *Carafano*, could be construed as "develop[ment]" under an unduly broad reading of the term. But, once again, such a broad reading would sap section 230 of all meaning.

The salient fact in *Carafano* was that the website's classifications of user characteristics did absolutely

nothing to enhance the defamatory sting of the message, to encourage defamation or to make defamation easier: The site provided neutral tools specifically designed to match romantic partners depending on their voluntary inputs. By sharp contrast, [**38] Roommate's website is designed to force subscribers to divulge protected characteristics and discriminatory preferences, and to match those who have rooms with those who are looking for rooms based on criteria that appear to be prohibited by the FHA.³³

33 The dissent coyly suggests that our opinion "sets us apart from" other circuits, Dissent at 3479, 3483-84, carefully avoiding the phrase "inter-circuit conflict." And with good reason: No other circuit has considered a case like ours and none has a case that even arguably conflicts with our holding today. No case cited by the dissent involves active participation by the defendant in the creation or development of the allegedly unlawful content; in each, the interactive computer service provider passively relayed content generated by third parties, just as in *Stratton Oakmont*, and did not design its system around the dissemination of unlawful content.

In *Chi. Lawyers' Comm. for Civ. Rights Under Law, Inc. v. Craigslist, Inc.*, No. 07-1101, 2008 U.S. App. LEXIS 5472 (7th Cir. Mar. 14, 2008), the Seventh Circuit held the online classified website craigslist immune from liability for discriminatory housing advertisements submitted by users. Craigslist's service [**39] works very much like the "Additional Comments" section of Roommate's website, in that users are given an open text prompt in which to enter any description of the rental property without any structure imposed on their content or any requirement to enter discriminatory information: Nothing in the service craigslist offers induces anyone to post any particular listing or express a preference for discrimination" 2008 U.S. App. LEXIS 5472, *Slip op.* at 9. We similarly hold the "Additional Comments" section of Roommate's site immune, *see pp.* 3471-75 *infra*. Consistent with our opinion, the Seventh Circuit explained the limited scope of *section 230(c)* immunity. *Craigslist*, 2008 U.S. App. LEXIS 5472, *slip op.* at 5-7. More directly, the Seventh Circuit noted in dicta that "causing a particular

statement to be made, or perhaps [causing] the *discriminatory content of a statement*" might be sufficient to create liability for a website. 2008 U.S. App. LEXIS 5472, *Slip op.* at 9 (emphasis added). Despite the dissent's attempt to imply the contrary, the Seventh Circuit's opinion is actually in line with our own.

In *Universal Communications Systems v. Lycos, Inc.*, the First Circuit held a message board owner immune under the CDA for defamatory comments posted on a message [**40] board. 478 F.3d 413 (1st Cir. 2007). The allegedly defamatory comments were made without any prompting or encouragement by defendant: "[T]here is not even a colorable argument that any misinformation was prompted by Lycos's registration process or its link structure." *Id.* at 420.

Green v. America Online, 318 F.3d 465 (3d Cir. 2003), falls yet farther from the mark. There, AOL was held immune for derogatory comments and malicious software transmitted by other defendants through AOL's "Romance over 30" "chat room." There was no allegation that AOL solicited the content, encouraged users to post harmful content or otherwise had any involvement whatsoever with the harmful content, other than through providing "chat rooms" for general use.

In *Ben Ezra, Weinstein, and Co. v. America Online Inc.*, 206 F.3d 980 (10th Cir. 2000), the Tenth Circuit held AOL immune for relaying inaccurate stock price information it received from other vendors. While AOL undoubtedly participated in the decision to make stock quotations available to members, it did not cause the errors in the stock data, nor did it encourage or solicit others to provide inaccurate data. AOL was immune because "Plaintiff could not [**41] identify any evidence indicating Defendant [AOL] developed or created the stock quotation information." *Id.* at 985 n.5.

And, finally, in *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997), the Fourth Circuit held AOL immune for yet another set of defamatory and harassing message board postings. Again, AOL did not solicit the harassing content, did not encourage others to post it, and

had nothing to do with its creation other than through AOL's role as the provider of a generic message board for general discussions.

[*1173] 3. Councils finally argue that Roommate should be held liable for the discriminatory statements displayed in the "Additional Comments" section of profile pages. At the end of the registration process, on a separate page from the other registration steps, Roommate prompts subscribers to "tak[e] a moment to personalize your profile by writing a paragraph or two describing yourself and what you are looking for in a roommate." The subscriber is presented with a blank text box, in which he can type as much or as little about himself as he wishes. Such essays are visible only to paying subscribers.

Subscribers provide a variety of provocative, and often very revealing, [**42] answers. The contents range from subscribers who "[p]ref[er] white Male roommates" or require that "[t]he person applying for the room MUST be a BLACK GAY MALE" to those who are "NOT looking for black muslims." Some common themes are a desire to live without "drugs, kids or animals" or "smokers, kids or druggies," while a few subscribers express more particular preferences, such as preferring to live in a home free of "psychos or anyone on mental medication." Some subscribers are just looking for someone who will get along with their significant other³⁴ or with their most significant Other.³⁵

34 "The female we are looking for hopefully wont [sic] mind having a little sexual incounter [sic] with my boyfriend and I [very sic]."

35 "We are 3 Christian females who Love our Lord Jesus Christ We have weekly bible studies and bi-weekly times of fellowship."

Roommate publishes these comments as written.³⁶ It does not provide any specific guidance as to what the essay should contain, nor does it urge subscribers to input [*1174] discriminatory preferences. Roommate is not responsible, in whole or in part, for the development of this content, which comes entirely from subscribers and is passively [**43] displayed by Roommate. Without reviewing every essay, Roommate would have no way to distinguish unlawful discriminatory preferences from perfectly legitimate statements. Nor can there be any doubt that this information was tendered to Roommate for publication online. *See* pp. 3466-67 *supra*. This is precisely the kind of situation for which *section 230* was

designed to provide immunity. *See* pp. 3453-3455 *supra*.

36 It is unclear whether Roommate performs any filtering for obscenity or "spam," but even if it were to perform this kind of minor editing and selection, the outcome would not change. *See Batzel*, 333 F.3d at 1031.

The fact that Roommate encourages subscribers to provide *something* in response to the prompt is not enough to make it a "develop[er]" of the information under the common-sense interpretation of the term we adopt today. It is entirely consistent with Roommate's business model to have subscribers disclose as much about themselves and their preferences as they are willing to provide. But Roommate does not tell subscribers what kind of information they should or must include as "Additional Comments," and certainly does not encourage or enhance any discriminatory content created [**44] by users. Its simple, generic prompt does not make it a developer of the information posted.³⁷

37 Nor would Roommate be the developer of discriminatory content if it provided a free-text search that enabled users to find keywords in the "Additional Comments" of others, even if users utilized it to search for discriminatory keywords. Providing neutral tools for navigating websites is fully protected by CDA immunity, absent substantial affirmative conduct on the part of the website creator promoting the use of such tools for unlawful purposes.

Councils argue that--given the context of the discriminatory questions presented earlier in the registration process--the "Additional Comments" prompt impliedly suggests that subscribers should make statements expressing a desire to discriminate on the basis of protected classifications; in other words, Councils allege that, by encouraging *some* discriminatory preferences, Roommate encourages other discriminatory preferences when it gives subscribers a chance to describe themselves. But the encouragement that bleeds over from one part of the registration process to another is extremely weak, if it exists at all. Such weak encouragement cannot strip [**45] a website of its *section 230* immunity, lest that immunity be rendered meaningless as a practical matter.³⁸

38 It's true that, under a pedantic interpretation of the term "develop," any action by the

website--including the mere act of making a text box available to write in--could be seen as "develop[ing]" content. However, we have already rejected such a broad reading of the term "develop" because it would defeat the purpose of *section 230*. See pp. 3461-64 *supra*.

We must keep firmly in mind that this is an immunity statute we are expounding, a provision enacted to protect websites against the evil of liability for failure to remove offensive content. See pp. 3453-3455 *supra*. Websites are complicated enterprises, and there will always be close cases where a clever lawyer could argue that *something* the website operator did encouraged the illegality. Such close cases, we believe, must be resolved in favor of immunity, lest we cut the heart out of *section 230* by forcing websites to face death by ten thousand duck-bites, fighting off claims that they promoted or encouraged--or at least tacitly assented to--the illegality of third parties. Where it is very clear that the website directly [**46] participates in developing the alleged illegality--as it is clear here with respect to Roommate's questions, answers and the resulting profile pages--immunity will be lost. But in cases of enhancement by implication or [**1175] development by inference--such as with respect to the "Additional Comments" here--*section 230* must be interpreted to protect websites not merely from ultimate liability, but from having to fight costly and protracted legal battles.

The dissent prophesies doom and gloom for countless Internet services, Dissent at 3490-91, but fails to recognize that we hold part of Roommate's service entirely immune from liability. The search engines the dissent worries about, *id.*, closely resemble the "Additional Comments" section of Roommate's website. Both involve a generic text prompt with no direct encouragement to perform illegal searches or to publish illegal content. We hold Roommate immune and there is no reason to believe that future courts will have any difficulty applying this principle.³⁹ The message to website operators is clear: If you don't encourage illegal content, or design your website to require users to input illegal content, you will be immune.

39 The dissent also [**47] accuses us of creating uncertainty that will chill the continued growth of commerce on the Internet. Dissent at 3496. Even looking beyond the fact that the Internet has outgrown its swaddling clothes and

no longer needs to be so gently coddled, *see* p. 3456 n.15 *supra*, some degree of uncertainty is inevitable at the edge of any rule of law. Any immunity provision, including *section 230*, has its limits and there will always be close cases. Our opinion extensively clarifies where that edge lies, and gives far more guidance than our previous cases. While the dissent disagrees about the scope of the immunity, there can be little doubt that website operators today know more about how to conform their conduct to the law than they did yesterday.

However, a larger point remains about the scope of immunity provisions. It's no surprise that defendants want to extend immunity as broadly as possible. We have long dealt with immunity in different, and arguably far more important, contexts--such as qualified immunity for police officers in the line of duty, *see Clement v. City of Glendale*, No. 05-56692, 518 F.3d 1090, 2008 U.S. App. LEXIS 5140, slip op. at 2347 (9th Cir. Mar. 11, 2008)--and observed many defendants argue that the risk of [**48] getting a close case wrong is a justification for broader immunity. Accepting such an argument would inevitably lead to an endless broadening of immunity, as every new holding creates its own borderline cases.

We believe that this distinction is consistent with the intent of Congress to preserve the free-flowing nature of Internet speech and commerce without unduly prejudicing the enforcement of other important state and federal laws. When Congress passed *section 230* it didn't intend to prevent the enforcement of all laws online; rather, it sought to encourage interactive computer services that provide users *neutral* tools to post content online to police that content without fear that through their "good samaritan . . . screening of offensive material," 47 U.S.C. § 230(c), they would become liable for every single message posted by third parties on their website.

* * *

In light of our determination that the CDA does not provide immunity to Roommate for all of the content of its website and email newsletters, we remand for the district court to determine in the first instance whether the alleged actions for which Roommate is not immune

violate the Fair Housing Act, 42 U.S.C. § 3604(c). [**49] ⁴⁰ We vacate the dismissal of the state law claims so that the district court may reconsider whether to exercise its supplemental jurisdiction in light of our ruling on the federal claims. *Fredenburg v. Contra Costa County Dep't of Health Servs.*, 172 F.3d 1176, 1183 (9th Cir. 1999). We deny Roommate's [*1176] cross-appeal of the denial of attorneys' fees and costs; Councils prevail on some of their arguments before us so their case is performe not frivolous.

40 We do not address Roommate's claim that its activities are protected by the *First Amendment*. The district court based its decision entirely on the CDA and we refrain from deciding an issue that the district court has not had the opportunity to evaluate. See *Mukherjee v. INS*, 793 F.2d 1006, 1010 (9th Cir. 1986).

REVERSED in part, VACATED in part, AFFIRMED in part and REMANDED. NO COSTS.

CONCUR BY: M. Margaret McKeown (In Part)

DISSENT BY: M. Margaret McKeown (In Part)

DISSENT

McKEOWN, Circuit Judge, with whom RYMER and BEA, Circuit Judges, join, concurring in part and dissenting in part:

The ubiquity of the Internet is undisputed. With more than 1.3 billion Internet users and over 158 million websites in existence, ¹ a vast number of them interactive like Google, Yahoo!, [**50] Craigslist, MySpace, YouTube, and Facebook, the question of webhost liability is a significant one. On a daily basis, we rely on the tools of cyberspace to help us make, maintain, and rekindle friendships; find places to live, work, eat, and travel; exchange views on topics ranging from terrorism to patriotism; and enlighten ourselves on subjects from "aardvarks to Zoroastrianism." ²

1 Internet World Stats, World Internet Users: December 2007, <http://www.internetworldstats.com/stats.htm> (last visited Mar. 14, 2008); Netcraft, February 2008 Web Server Survey, http://news.netcraft.com/archives/web_server_survey.html (last visited Mar. 14, 2008).

2 *Ashcroft v. ACLU*, 535 U.S. 564, 566, 122 S. Ct. 1700, 152 L. Ed. 2d 771 (2002).

The majority's unprecedented expansion of liability for Internet service providers threatens to chill the robust development of the Internet that Congress envisioned. The majority condemns Roommate's "search system," a function that is the heart of interactive service providers. My concern is not an empty Chicken Little "sky is falling" alert. By exposing every interactive service provider to liability for sorting, searching, and utilizing the all too familiar drop-down menus, the majority has dramatically [**51] altered the landscape of Internet liability. Instead of the "robust" ³ immunity envisioned by Congress, interactive service providers are left scratching their heads and wondering where immunity ends and liability begins.

3 *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1123 (9th Cir. 2003).

To promote the unfettered development of the Internet, Congress adopted the Communications Decency Act of 1996 ("CDA"), which provides that interactive computer service providers will not be held legally responsible for publishing information provided by third parties. 47 U.S.C. § 230(c)(1). Even though traditional publishers retain liability for performing essentially equivalent acts in the "non-virtual world," Congress chose to treat interactive service providers differently by immunizing them from liability stemming from sorting, searching, and publishing third-party information. As we explained in *Batzel v. Smith*:

[Section] 230(c)(1)[] overrides the traditional treatment of publishers, distributors, and speakers under statutory and common law. As a matter of policy, "Congress decided not to treat providers of interactive computer services like other information providers such as newspapers, [**52] magazines or television and radio stations" Congress . . . has chosen to treat cyberspace differently.

333 F.3d 1018, 1026-1027 (9th Cir. 2003) (quoting *Blumenthal v. Drudge*, 992 F. Supp. 44, 49 (D.D.C. 1998) (footnote omitted)).

Now, with the stroke of a pen or, more accurately, a few strokes of the keyboard, the majority upends the

settled view that interactive service providers enjoy broad immunity when publishing information provided by third parties. Instead, interactive [*1177] service providers are now joined at the hip with third-party users, and they rise and fall together in liability for Internet sortings and postings.

To be sure, the statute, which was adopted just as the Internet was beginning a surge of popular currency,⁴ is not a perfect match against today's technology. The Web 2.0 version is a far cry from web technology in the mid-1990s. Nonetheless, the basic message from Congress has retained its traction, and there should be a high bar to liability for organizing and searching third-party information. The bipartisan view in Congress was that the Internet, as a new form of communication, should not be impeded by the transference of regulations and principles developed [**53] from traditional modes of communication. The majority repeatedly harps that if something is prohibited in the physical world, Congress could not have intended it to be legal in cyberspace. Yet that is precisely the path Congress took with the CDA: the anomaly that a webhost may be immunized for conducting activities in cyberspace that would traditionally be cause for liability is exactly what Congress intended by enacting the CDA.

4 According to one commentator, in 1985, there were approximately 1,000 host computers connected to the Internet; by 1995, that number had exploded to 4,000,000. Paul H. Arne, *New Wine in Old Bottles: The Developing Law of the Internet*, 416 PLI/Pat 9, 15 (Sept. 1995).

In the end, the majority offers interactive computer service providers no bright lines and little comfort in finding a home within § 230(c)(1). The result in this case is driven by the distaste for housing discrimination, a laudable endgame where housing the real focus of this appeal. But it is not. I share the majority's view that housing discrimination is a troubling issue. Nevertheless, we should be looking at the housing issue through the lens of the Internet, not from the perspective of traditional [**54] publisher liability. Whether § 230(c)(1) trumps the Fair Housing Act ("FHA") is a policy decision for Congress, not us. Congress has spoken: third-party content on the Internet should not be burdened with the traditional legal framework.

I respectfully part company with the majority as to Part 2⁵ of the opinion because the majority has

misconstrued the statutory protection under the CDA for Roommate's publishing and sorting of user profiles. The plain language and structure of the CDA unambiguously demonstrate that Congress intended these activities--the collection, organizing, analyzing, searching, and transmitting of third-party content--to be beyond the scope of traditional publisher liability. The majority's decision, which sets us apart from five circuits, contravenes congressional intent and violates the spirit and serendipity of the Internet.

5 The complaint centers on the responses and profiles generated by the users. To the extent that the inquiry in isolation is part of the claims, then I agree with Part 1 of the majority's opinion that § 230(c)(1) would not protect Roommate. However, I cannot join the majority insofar as it eviscerates the distinction between traditional publishers [**55] and webhosts. *See, e.g.*, Maj. Op. at 3456 (ignoring the Congressional carve-out for interactive service providers and concluding that if a face-to-face transaction were illegal, it could not be legal in cyberspace).

Specifically, the majority's analysis is flawed for three reasons: (1) the opinion conflates the questions of liability under the FHA and immunity under the CDA; (2) the majority rewrites the statute with its definition of "information content provider," labels the search function "information development," and strips interactive service providers of immunity; and (3) the majority's approach undermines the purpose [*1178] of § 230(c)(1) and has far-reaching practical consequences in the Internet world.

To begin, it is important to recognize what this appeal is not about. At this stage, there has been no determination of liability under the FHA, nor has there been any determination that the questions, answers or even the existence of Roommate's website violate the FHA. The FHA is a complicated statute and there may well be room for potential roommates to select who they want to live with, e.g., a tidy accountant wanting a tidy professional roommate, a collegiate male requesting a [**56] male roommate, an observant Jew needing a house with a kosher kitchen, or a devout, single, religious female preferring not to have a male housemate. It also bears noting that even if Roommate is immune under the CDA, the issue of user liability for allegedly discriminatory preferences is a separate question. *See Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir.

1997) (stating that "the original culpable party" does not "escape accountability").

By offering up inflammatory examples, the majority's opinion screams "discrimination." The hazard is, of course, that the question of discrimination has not yet been litigated. In dissenting, I do not condone housing discrimination or endorse unlawful discriminatory roommate selection practices; I simply underscore that the merits of the FHA claim are not before us. However, one would not divine this posture from the majority's opinion, which is infused with condemnation of Roommate's users' practices. To mix and match, as does the majority, the alleged unlawfulness of the information with the question of webhost immunity is to rewrite the statute.

Examples from the opinion highlight that the majority's conclusion rests on the premise that [*57] Roommate's questions and matching function violate the FHA:

. "Unlawful questions solicit (a.k.a. 'develop') unlawful answers." Maj. Op. at 3459.

. "If such questions are unlawful when posed face-to-face or by telephone, they don't magically become lawful when asked electronically online." *Id.* at 3456.

. "If such screening is prohibited when practiced in person or by telephone, we see no reason why Congress would have wanted to make it lawful to profit from it online." *Id.* at 3461.

. "Roommate's search function thus differs materially from generic search engines such as Google, Yahoo! and MSN Live Search, in that Roommate designed its system to use allegedly unlawful criteria so as to limit the results of each search, and to force users to participate in its discriminatory process." *Id.*

. "By contrast, ordinary search engines do not use unlawful criteria to limit the scope of searches conducted on them, nor are they designed to achieve illegal ends--as Roommate's search

function is alleged to do here." *Id.*

. "Roommate's website is designed to force subscribers to divulge protected characteristics and discriminatory preferences." *Id.* at 3470.

The entire opinion links Roommate's ostensibly [*58] reprehensible conduct (and that of its users) with an unprecedented interpretation of the CDA's immunity provision. The majority condemns Roommate for soliciting illegal content, but there has been no determination that Roommate's questions or standardized answers are illegal. Instead of foreshadowing a ruling on the FHA, the opinion should be confined to the issue before us--application of § 230(c)(1) to Roommate. The district court has not yet ruled on the merits of the FHA claim and neither should we.

[*1179] The Statute

With this background in mind, I first turn to the text of the statute. *Section 230* begins with a detailed recitation of findings and policy reasons for the statute. Congress expressly found that the "Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity," and that "[i]ncreasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services." 47 U.S.C. § 230(a)(3), (5). Congress declared that "[i]t is the policy of the United States to . . . promote the continued development [*59] of the Internet and other interactive computer services and other interactive media." § 230(b)(1).⁶

6 The statute also seeks to "remove disincentives for the development and utilization of blocking and filtering technologies" and "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer." § 230(b)(4), (5).

Unlike some statutes, *subsections (a) and (b)* set out in clear terms the congressional findings and policies underlying the statute. For this reason, it strikes me as odd that the majority begins, not with the statute and these express findings, but with legislative history.

Granted, Congress was prompted by several cases, particularly the *Prodigy* case, to take action to protect interactive service providers. See *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 24, 1995). But that case does not cabin the scope of the statute, and the background leading up to enactment of the CDA is no substitute for the language of the statute itself. See *Chi. Lawyers' Comm. for Civ. Rights Under Law, Inc. v. Craigslist, Inc.*, No. 07-1101, 2008 U.S. App. LEXIS 5472, slip op. at 8 (7th Cir. Mar. 14, 2008) [**60] (concluding that, as enacted, "Section 230(c)(1) is general[,] despite its 'genesis' in *Prodigy*).

Section 230(c), the heart of this case, is entitled "Protection for 'good samaritan' blocking and screening of offensive material[.]" The substantive language of the statute itself is not so limited. Section 230(c)(1) provides:

(1) Treatment of publisher or speaker

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

§ 230(c)(1). Since it was first addressed in 1997 in *Zeran*, this section has been interpreted by the courts as providing webhost "immunity," although to be more precise, it provides a safe haven for interactive computer service providers by removing them from the traditional liabilities attached to speakers and publishers.⁷ See *Zeran*, 129 F.3d at 330 ("By its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.").

⁷ The second part of this subsection, § 230(c)(2), is more accurately characterized as an immunity provision, but is not relevant [**61] to our discussion here. Compare 47 U.S.C. § 230(c)(2) (stating that "[n]o provider or user of an interactive computer service shall be held liable . . .") (emphasis added).

We have characterized this immunity under § 230(c)(1) as "quite robust." *Carafano*, 339 F.3d at 1123. Five of our sister circuits have similarly embraced this robust view of immunity by providing differential treatment to interactive service providers. *Chi. Lawyers' Comm. for Civ. Rights Under Law, Inc. v. Craigslist, Inc.*

, No. 07-1101, 2008 U.S. Dist. App. LEXIS 5472, slip op. at 7-8 (7th Cir. Mar. 14, 2008); *Universal Commc'n Sys. v. Lycos, Inc.*, [*1180] 478 F.3d 413, 415 (1st Cir. 2007); *Green v. Am. Online*, 318 F.3d 465, 470 (3d Cir. 2003); *Ben Ezra, Weinstein, & Co., Inc. v. Am. Online Inc.*, 206 F.3d 980, 986 (10th Cir. 2000); *Zeran*, 129 F.3d at 330; see also *Whitney Info. Network, Inc. v. Xcentric Ventures, LLC*, No. 2:04-cv-47-FtM-34SPC, 2008 U.S. Dist. LEXIS 11632 (M.D. Fla. Feb. 15, 2008); *Doe v. MySpace, Inc.*, 474 F. Supp. 2d 843, 849 (W.D. Tex. 2007); *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1118 (W.D. Wash. 2004); *Blumenthal*, 992 F. Supp. at 50-53; *Barrett v. Rosenthal*, 40 Cal. 4th 33, 51 Cal. Rptr. 3d 55, 146 P.3d 510, 529 (Cal. 2006); *Gentry v. eBay, Inc.*, 121 Cal. Rptr.2d 703, 717-18 (Cal. Ct. App. 2002); [**62] *Schneider v. Amazon.com, Inc.*, 108 Wn. App. 454, 31 P.3d 37, 42-43 (Wash. Ct. App. 2001).

Key to this immunity provision are the terms "interactive computer service" provider and "information content provider." The CDA defines an "interactive computer service" as any "information service, system, or access software provider that provides or enables computer access by multiple users to a computer server." § 230(f)(2). An interactive computer service provider is not liable as a "publisher" or "speaker" of information if the "information" is "provided by another information content provider." § 230(c)(1). The statute then defines an "information content provider" as a "person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." § 230(f)(3). If the provider of an interactive computer service is an information content provider of the information at issue, it cannot claim immunity as a publisher or speaker. *Carafano*, 339 F.3d at 1123.

Courts deciding the question of § 230(c)(1) immunity "do not write on a blank slate." *Universal Commc'n*, 478 F.3d at 418. Even though rapid developments in technology [**63] have made webhosts increasingly adept at searching and displaying third-party information, reviewing courts have, in the twelve years since the CDA's enactment, "adopt[ed] a relatively expansive definition of 'interactive computer service' and a relatively restrictive definition of 'information content provider.'" See *Carafano*, 339 F.3d at 1123 (footnotes omitted). As long as information is provided by a third party, webhosts are immune from liability for publishing "ads for housing, auctions of paintings that may have

been stolen by Nazis, biting comments about steroids in baseball, efforts to verify the truth of politicians' promises, and everything else that third parties may post on a web site." *Craigslist, No. 07-1101, 2008 U.S. Dist. App. LEXIS 5472, slip op. at 9*. We have underscored that this broad grant of webhost immunity gives effect to Congress's stated goals "to promote the continued development of the Internet and other interactive computer services" and "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services." *Carafano, 339 F.3d at 1123* (discussing § 230(b)(1), (2)).

Application of § 230(c)(1) to Roommate's Website

Because our [**64] focus is on the term "information content provider," and what it means to create or develop information, it is worth detailing exactly how the website operates, what information is at issue and who provides it. The roommate matching process involves three categories of data: About Me or Household Description; Roommate Preferences; and Comments.

To become a member of Roommates.com, a user must complete a personal profile by selecting answers from dropdown menus or checking off boxes on the screen. The profile includes "location" information [**1181] (e.g., city and state, region of the city, and data about the surrounding neighborhood); details about the residence (e.g., the total number of bedrooms and bathrooms in the home, and amenities such as air conditioning, wheelchair access, high-speed Internet, or parking), and the "rental details" (e.g., monthly rent charged, lease period, and availability). The last section of the profile is the "Household Description" section,⁸ which includes the total number of occupants in the home, their age range, gender, occupation, level of cleanliness, whether they are smokers, and whether children or pets are present.

⁸ A user who is a room-seeker fills out [**65] an equivalent section named "About Me."

The remaining sections of the registration process are completely optional; a user who skips them has created a profile based on the information already provided. At his option, the user may select an emoticon to describe the "household character," and may upload images of the room or residence. Next, users may, at their option, specify characteristics desired in a potential roommate,

such as a preferred age range, gender, and level of cleanliness. If nothing is selected, all options are included.⁹ The final step in the registration process, which is also optional, is the "Comments" section, in which users are presented with a blank text box in which they may write whatever they like, to be published with their member profiles.

⁹ The following is an example of a member profile:

The Basics

Rent: \$ 800 per month + \$ 800 deposit

Lease: 6 month

Date available: 09/01/04 (14 days)

Utilities included: N/A

Features: Private bedroom, Private bathroom

Residence & Vicinity

Building: House, 2 bed, 1.5 bath

Features: N/A

Location: (Central) Long Beach, CA

Household

Occupant: 1, Age 26, Male (straight)

Occupation: Student

Smoking habits: Outside smoker

Cleanliness: [**66] About average

Children: Children will not be living with us

Pets: Dog(s)

Preferences

Age group: 18-99

Gender: Male (straight or gay), Female (straight or lesbian)

Smoking: Smoking okay

Cleanliness level: Clean, Average, Messy

Pets: Dog okay, Cat okay, Caged pet okay

Children: Children okay

Comments

LOOKING FOR CHILL
ROOMMATE [sic] TO SHARE 2
BR HOUSE WITH DOG AND
FERRET - RENT
800/MO+utill.6mo.lease.

Users may choose an optional "custom search" of user profiles based on criteria that they specify, like the amount of monthly rent or distance from a preferred city. Based on the information provided by users during the registration process, Roommate's automated system then searches and matches potential roommates. Roommate's Terms of Service provide in part, "You understand that we do not provide the information on the site and that all publicly posted or privately transmitted information, data, text, photographs, graphics, messages, or other materials ('Content') are the sole responsibility of the person from which such Content originated."

Roommate's users are "information content providers" because they are responsible for creating the information in their user profiles and, at their [*67] option -- not the website's choice -- in expressing preferences as to roommate characteristics. § 230(f)(3). The critical question is whether Roommate is itself an "information content provider," such that it cannot claim that the information at issue was "provided [*1182] by another information content provider." A close reading of the statute leads to the conclusion that Roommate is not an information content provider for two reasons: (1) providing a drop-down menu does not constitute "creating" or "developing" information; and (2) the

structure and text of the statute make plain that Congress intended to immunize Roommate's sorting, displaying, and transmitting of third-party information.

Roommate neither "creates" nor "develops" the information that is challenged by the Councils, i.e., the information provided by the users as to their protected characteristics and the preferences expressed as to roommate characteristics. All Roommate does is to provide a form with options for standardized answers. Listing categories such as geographic location, cleanliness, gender and number of occupants, and transmitting to users profiles of other users whose expressed information matches their expressed [*68] preferences, can hardly be said to be creating or developing information. Even adding standardized options does not "develop" information. Roommate, with its prompts, is merely "selecting material for publication," which we have stated does not constitute the "development" of information. *Batzel*, 333 F.3d at 1031. The profile is created solely by the user, not the provider of the interactive website. Indeed, without user participation, there is no information at all. The drop-down menu is simply a precategorization of user information before the electronic sorting and displaying that takes place via an algorithm. If a user has identified herself as a non-smoker and another has expressed a preference for a non-smoking roommate, Roommate's sorting and matching of user information are no different than that performed by a generic search engine.

Displaying the prompt "Gender" and offering the list of choices, "Straight male; Gay male; Straight female; Gay female" does not develop the information, "I am a Gay male." The user has identified himself as such and provided that information to Roommate to publish. Thus, the user is the sole creator of that information; no "development" has occurred. [*69] In the same vein, presenting the user with a "Preferences" section and drop-down menus of options does not "develop" a user's preference for a non-smoking roommate. As we stated in *Carafano*, the "actual profile 'information' consist[s] of the particular options chosen" by the user, such that Roommate is not "responsible, even in part, for associating certain multiple choice responses with a set of [] characteristics." 339 F.3d at 1124.

The thrust of the majority's proclamation that Roommate is "developing" the information that it publishes, sorts, and transmits is as follows: "[W]e

interpret the term 'development' as referring not merely to augmenting the content generally, but to materially contributing to its unlawfulness." Maj. Op. at 3462. This definition is original to say the least and springs forth untethered to anything in the statute.

The majority's definition of "development" epitomizes its consistent collapse of substantive liability with the issue of immunity. Where in the statute does Congress say anything about unlawfulness? Whether Roommate is entitled to immunity for publishing and sorting profiles is wholly distinct from whether Roommate may be liable for violations [**70] of the FHA. Immunity has meaning only when there is something to be immune *from*, whether a disease or the violation of a law. It would be nonsense to claim to be immune only from the innocuous. But the majority's immunity analysis is built on substantive liability: to the majority, CDA immunity depends on whether a webhost materially [*1183] contributed to the unlawfulness of the information. Whether the information at issue is unlawful and whether the webhost has contributed to its unlawfulness are issues analytically independent of the determination of immunity. Grasping at straws to distinguish Roommate from other interactive websites such as Google and Yahoo!, the majority repeatedly gestures to Roommate's potential substantive liability as sufficient reason to disturb its immunity. But our task is to determine whether the question of substantive liability may be reached in the first place.

Keep in mind that "unlawfulness" would include not only purported statutory violations but also potential defamatory statements. The irony is that the majority would have us determine "guilt" or liability in order to decide whether immunity is available. This upside-down approach would knock out even [**71] the narrowest immunity offered under § 230(c) -- immunity for defamation as a publisher or speaker.

Another flaw in the majority's approach is that it fails to account for all of the other information allegedly developed by the webhost. For purposes of determining whether Roommate is an information content provider vis-a-vis the profiles, the inquiry about geography and the inquiry about gender should stand on the same footing. Both are single word prompts followed by a drop-down menu of options. If a prompt about gender constitutes development, then so too does the prompt about geography. And therein lies the rub.

Millions of websites use prompts and drop-down menus. Inquiries range from what credit card you want to use and consumer satisfaction surveys asking about age, sex and household income, to dating sites, e.g., match.com, sites lambasting corporate practices, e.g., ripoffreports.com, and sites that allow truckers to link up with available loads, e.g., getloaded.com. Some of these sites are innocuous while others may not be. Some may solicit illegal information; others may not. But that is not the point. The majority's definition of "development" would transform every interactive [**72] site into an information content provider and the result would render illusory any immunity under § 230(c). Virtually every site could be responsible in part for developing content.

For example, the majority purports to carve out a place for Google and other search engines. Maj. Op. at 3461. But the modern Google is more than a match engine: it ranks search results, provides prompts beyond what the user enters, and answers questions. In contrast, Roommate is a straight match service that searches information and criteria provided by the user, not Roommate. It should be afforded no less protection than Google, Yahoo!, or other search engines.

The majority then argues that "providing *neutral* tools to carry out what may be unlawful or illicit searches does not amount to 'development.'" Maj. Op. at 3464. But this effort to distinguish Google, Yahoo!, and other search engines from Roommate is unavailing. Under the majority's definition of "development," these search engines are equivalent to Roommate. Google "encourages" or "contributes" (the majority's catch phrases) to the unlawfulness by offering search tools that allow the user to perform an allegedly unlawful match. If a user types into [**73] Google's search box, "looking for a single, Christian, female roommate," and Google displays responsive listings, Google is surely "materially contributing to the alleged unlawfulness" of information created by third parties, by publishing their intention to discriminate on the basis of protected characteristics. In the defamation arena, a webhost's publication of a defamatory statement "materially contributes" to its [*1184] unlawfulness, as publication to third parties is an element of the offense. At bottom, the majority's definition of "development" can be tucked in, let out, or hemmed up to fit almost any search engine, creating tremendous uncertainty in an area where Congress expected predictability.

"Development" is not without meaning. In *Batzel*, we hinted that the "development of information" that transforms one into an "information content provider" is "something more substantial than merely editing portions of an email and selecting material for publication." 333 F.3d at 1031. We did not flesh out further the meaning of "development" because the editor's alterations of an email message and decision to publish it did not constitute "development." *Id.*

Because the statute does not define [**74] "development," we should give the term its ordinary meaning. *See San Jose Christian Coll. v. City of Morgan Hill*, 360 F.3d 1024, 1034 (9th Cir. 2004) (stating that dictionaries may be used to determine the "'plain meaning' of a term undefined by a statute"). "Development" is defined in Webster's Dictionary as a "gradual advance or growth through progressive changes." *Webster's Third New International Dictionary* 618 (2002). The multiple uses of "development" and "develop" in other provisions of § 230 give texture to the definition of "development," and further expose the folly of the majority's ungrounded definition. *See, e.g.,* § 230(b)(3) (stating that "[i]t is the policy of the United States to encourage the *development* of technologies which maximize user control over what information is received by individuals, families, and schools") (emphasis added).¹⁰ Defining "development" in this way keeps intact the settled rule that the CDA immunizes a webhost who exercises a publisher's "traditional editorial functions -- such as deciding whether to publish, withdraw, post-pone, or alter content." *Batzel*, 333 F.3d at 1031 n.18.¹¹

¹⁰ Congress also stated in the CDA that "[i]t is the policy [**75] of the United States to--(1) to promote the continued *development* of the Internet and other interactive computer services and other interactive media," and "(4) to remove disincentives for the *development* and utilization of blocking and filtering technologies . . ." § 230(b)(1), (4) (emphasis added).

¹¹ The majority's notion of using a different definition of "development" digs the majority into a deeper hole. *See* Maj. Op. at 3461-63. For example, adopting the Wikipedia definition of "content development"--"the process of researching, writing, gathering, organizing and editing information for publication on web sites"--would run us smack into the sphere of

Congressionally conferred immunity. Wikipedia, Content Development (Web), [http://en.wikipedia.org/w/index.php?title=Content_development_](http://en.wikipedia.org/w/index.php?title=Content_development_%) (last visited Mar. 24, 2008). Both our circuit and others have steadfastly maintained that activities such as organizing or editing information are traditional editorial functions that fall within the scope of CDA immunity. *See, e.g., Carafano*, 339 F.3d at 1124-25; *Zeran*, 129 F.3d at 330. Likewise, an alternative definition of "development" from Webster's such as "a making [**76] usable or available" sweeps too broadly, as "making usable or available" is precisely what Google and Craigslist do. In an effort to cabin the reach of the opinion, the majority again goes back to whether the content is legal, i.e., a dating website that requires sex, race, religion, or marital status is legal because it is legal to discriminate in dating. *See* Maj. Op. at 3464. Of course this approach ignores whether the claim may be one in tort, such as defamation, rather than a statutory discrimination claim. And, this circularity also circumvents the plain language of the statute. Interestingly, the majority has no problem offering up potentially suitable definitions of "development" by turning to dictionaries, but it fails to explain why, and from where, it plucked its definition of "development" as "materially contributing to [the] alleged unlawfulness" of content. *See* Maj. Op. at 3462.

Applying the plain meaning of "development" to Roommate's sorting and transmitting of third-party information demonstrates [**1185] that it was not transformed into an "information content provider." In searching, sorting, and transmitting information, Roommate made no changes to the information provided [**77] to it by users. Even having notice that users may be using its site to make discriminatory statements is not sufficient to invade Roommate's immunity. *See Zeran*, 129 F.3d at 333 (stating that "liability upon notice has a chilling effect on the freedom of Internet speech.").

The majority blusters that Roommate develops information, because it "requir[es] subscribers to provide the information as a condition of accessing its services," and "designed its search system so it would steer users based on the preferences and personal characteristics that Roommate itself forces subscribers to disclose." Maj. Op. at 3458, 3460.¹² But the majority, without looking back,

paces past the plain language of the statute. That Roommate requires users to answer a set of prompts to identify characteristics about themselves does not change the fact that the users have furnished this information to Roommate for Roommate to publish in their profiles. Nor do Roommate's prompts alter the fact that users have chosen to select characteristics that they find desirable in potential roommates, and have directed Roommate to search and compile results responsive to their requests. Moreover, tagging Roommate with [**78] liability for the design of its search system is dangerous precedent for analyzing future Internet cases.

12 Again, Roommate does not force users to disclose preferences as to roommate characteristics.

Even if Roommate's prompts and drop-down menus could be construed to seek out, or encourage, information from users, the CDA does not withhold immunity for the encouragement or solicitation of information.¹³ See *Blumenthal*, 992 F. Supp. at 52 (stating that "Congress has made a different policy choice by providing immunity even where the interactive service provider has an *active, even aggressive role* in making available content prepared by others.") (emphasis added); *Gentry*, 121 Cal.Rptr.2d at 718 (noting that "enforcing appellants' negligence claim would place liability on eBay for simply compiling false and/or misleading content created by the individual defendants and other coconspirators."). The CDA does not countenance an exception for the solicitation or encouragement of information provided by users.

13 The First Circuit has noted that "[i]t is not at all clear that there is a culpable assistance exception to *Section 230* immunity[,]" similar to the notion of secondary liability [**79] under the Electronic Communications Privacy Act of 1986. *Universal Commc'n*, 478 F.3d at 421. But it also stated that it "need not decide whether a claim premised on active inducement might be consistent with *Section 230* in the absence of a specific exception." *Id.*

A number of district courts have recently encountered the claim that an interactive website's solicitation of information, by requiring user selection of content from drop-down menus, transformed it into an information content provider. Unsurprisingly, these courts reached the same commonsense solution that I

reach here: § 230(c)(1) immunizes the interactive service provider. See *Whitney Info. Network, Inc. v. Xcentric Ventures, LLC*, No. 2:04-cv-47-FtM-34SPC, 2008 U.S. Dist. LEXIS 11632, at *36 (M.D. Fla. Feb. 15, 2008) (stating that the "mere fact that Xcentric provides categories from which a poster must make a selection in order to submit a report on the [] website is not sufficient to treat Defendants as information content providers of the reports"); *Global Royalties, Ltd. v. Xcentric Ventures, LLC*, No. 07-956-PHX-FJM, [*1186] 2007 U.S. Dist. LEXIS 77551 (D. Ariz. Oct. 10, 2007). Simply supplying a list of options from which [**80] a user must select options "is minor and passive participation" that does not defeat CDA immunity. *Global Royalties*, 2007 U.S. Dist. LEXIS 77551, at *9; see also *Corbis*, 351 F. Supp. 2d at 1118 (holding that even though Amazon.com "may have encouraged third parties to use the Zshops platform and provided the tools to assist them, that does not disqualify it from immunity under § 230 because the Zshops vendor ultimately decided what information to put on its site.").

Carafano presented circumstances virtually indistinguishable from those before us, yet the majority comes to the exact opposite conclusion here in denying immunity for sorting and matching third-party information provided in response to webhost prompts. The website in *Carafano*, an online dating service named Matchmaker.com, asked its users sixty-two detailed questions and matched users according to their responses. We held that § 230(c)(1) immunized the dating service, and flatly rejected the proposition that matching, sorting, and publishing user information in response to webhost prompts abrogated CDA immunity. *Carafano*, 339 F.3d at 1124-25. A provider's "decision to structure the information provided by users," which [**81] enables the provider to "offer additional features, such as 'matching' profiles with similar characteristics or highly structured searches based on combinations of multiple choice questions," ultimately "promotes the expressed Congressional policy 'to promote the continued development of the Internet and other interactive computer services.'" *Id.* (quoting § 230(b)(1)). Now the majority narrows *Carafano* on the basis that Matchmaker did not prompt the allegedly libelous information that was provided by a third party. Maj. Op. at 3468. But the majority makes this distinction without *any* language in the statute supporting the consideration of the webhost's prompting or solicitation.

The structure of the statute also supports my view

that Congress intended to immunize Roommate's sorting and publishing of user profiles. An "interactive computer service" is defined to include an "access software provider." § 230(f)(2). The statute defines an "access software provider" as one that provides "enabling tools" to "filter," "screen," "pick," "choose," "analyze," "digest," "search," "forward," "organize," and "reorganize" content. § 230(f)(4)(A)-(C).

By providing a definition for "access software [**82] provider" that is distinct from the definition of an "information content provider," and withholding immunity for "information content providers," the statute makes resoundingly clear that packaging, sorting, or publishing third-party information are not the kind of activities that Congress associated with "information content providers." Yet these activities describe exactly what Roommate does through the publication and distribution of user profiles: Roommate "receives," "filters," "digests," and "analyzes" the information provided by users in response to its registration prompts, and then "transmits," "organizes," and "forwards" that information to users in the form of uniformly organized profiles. Roommate is performing tasks that Congress recognized as typical of entities that it intended to immunize.

Finally, consider the logical disconnect of the majority's opinion. The majority writes--and I agree--that the open-ended Comments section contains only third-party content. Maj. Op. at 3471-75. But if Roommate's search function permits sorting by key words such as children or gender, the majority would label Roommate's use of such criteria as a "discriminatory filtering process." [**83] *Id.* at 3465.

[*1187] At a minimum, the CDA protects the search criteria employed by websites and does not equate tools that "filter," "screen," "pick," "choose," "analyze," "digest," "search," "forward," "organize," and "reorganize" with the "creation or development" of information. § 230(f)(4)(A)-(C).

Ramifications of the Majority Opinion

I am troubled by the consequences that the majority's conclusion poses for the ever-expanding Internet community. The unwise narrowing of our precedent, coupled with the mixing and matching of CDA immunity with substantive liability, make it exceedingly difficult for website providers to know whether their activities will

be considered immune under the CDA. We got it right in *Carafano*, that "[u]nder § 230(c) . . . so long as a third party willingly provides the essential published content, the interactive service provider receives full immunity regardless of the specific editing or selection process." 339 F.3d at 1124 (quoted in *Doe*, 474 F. Supp. 2d at 847; *Chicago Lawyers' Comm. for Civil Rights Under the Law, Inc. v. Craigslist, Inc.*, 461 F. Supp. 2d 681, 690 n.7 (N.D. Ill. 2006); *Dimeo v. Max*, 433 F. Supp. 2d 523, 530 n.12 (E.D. Pa. 2006); *Prickett v. Infousa*, [**84] *Inc.*, No. 04:05-CV-10, 561 F. Supp. 2d 646, 2006 U.S. Dist. LEXIS 21867, at *4 (E.D. Tex. Mar. 30, 2006)).

Significantly, § 230(e) expressly exempts from its scope certain areas of law, such as intellectual property law and federal criminal laws. § 230(e)(1) ("Nothing in this section shall be construed to impair the enforcement of [selected obscenity statutes] or any other Federal criminal statute."); § 230(e)(2) ("Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property."). See also *Perfect 10, Inc. v. CCBILL LLC*, 488 F.3d 1102, 1118 (9th Cir. 2007). Thus, for example, a webhost may still be liable as a publisher or speaker of third-party information that is alleged to infringe a copyright. Notably, the CDA does not exempt the FHA and a host of other federal statutes from its scope. See § 230(e). The FHA existed at the time of the CDA's enactment, yet Congress did not add it to the list of specifically enumerated laws for which publisher and speaker liability was left intact. The absence of a statutory exemption suggests that Congress did not intend to provide special case status to the FHA in connection with immunity under the CDA. See *TRW Inc. v. Andrews*, 534 U.S. 19, 28, 122 S. Ct. 441, 151 L. Ed. 2d 339 (2001) [**85] (stating that "[w]here Congress explicitly enumerates certain exceptions to a general prohibition, additional exceptions are not to be implied, in the absence of evidence of a contrary legislative intent.") (citation omitted); see also *Craigslist*, No. 07-1101, 2008 U.S. App. LEXIS 5472, slip op. at 8 (stating that "[t]he question is not whether Congress gave any thought to the Fair Housing Act, but whether it excluded § 3604(c) from the reach of § 230(c)(1)").

Anticipating the morphing of the Internet and the limits of creative genius and entrepreneurship that fuel its development is virtually impossible. However, Congress explicitly drafted the law to permit this unfettered development of the Internet. Had Congress discovered that, over time, courts across the country have created

more expansive immunity than it originally envisioned under the CDA, Congress could have amended the law. But it has not. In fact, just six years ago, Congress approved of the broad immunity that courts have uniformly accorded interactive webhosts under § 230(c).

In 2002, Congress passed the "Dot Kids Implementation and Efficiency Act," which established a new "kids.us" domain for material that is safe for children. Pub. L. No. 107- 317, 116 Stat. 2766. [**86] Congress stated that the statutory protections of [*1188] § 230(c) were extended to certain entities that operated within the new domain. 47 U.S.C. § 941 (stating that certain entities "are deemed to be interactive computer services for purposes of § 230(c)"). The Committee Report that accompanied the statute declared:

The Committee notes that ISPs have successfully defended many lawsuits using section 230(c). The courts have correctly interpreted section 230(c), which was aimed at protecting against liability for such claims as negligence (See, e.g., *Doe v. America Online*, 783 So. 2d 1010 (Fla. 2001)) and defamation (*Ben Ezra, Weinstein, and Co. v. America Online*, 206 F.3d 980 (2000); *Zeran v. America Online*, 129 F.3d 327 (1997)). The Committee intends these interpretations of section 230(c) to be equally applicable to those entities covered by H.R. 3833.

H.R. REP. No. 107-449 (emphasis added). These statements "reflect the Committee's intent that the existing statutory construction," i.e., broad immunity for interactive webhosts, "be maintained in a new legislative context." *Barrett*, 146 P.3d at 523 n.17 (discussing H.R. Rep. No. 107-449); see also *Heckler v. Turner*, 470 U.S. 184, 209, 105 S. Ct. 1138, 84 L. Ed. 2d 138 (1985) [**87] (noting that subsequent legislative history can shed useful light on Congressional intent). This express Congressional approval of the courts' interpretation of § 230(c)(1), six years after its enactment, advises us to stay the course of "robust" webhost immunity.

The consequences of the majority's interpretation are far-reaching. Its position will chill speech on the Internet and impede "the continued development of the Internet and other interactive computer services and other interactive media." § 230(b)(1). To the extent the

majority strips immunity because of sorting, channeling, and categorizing functions, it guts the heart of § 230(c)(1) immunity. Countless websites operate just like Roommate: they organize information provided by their users into a standardized format, and provide structured searches to help users find information. These sites, and their attendant display, search, and inquiry tools, are an indispensable part of the Internet tool box. Putting a lid on the sorting and searching functions of interactive websites stifles the core of their services.

To the extent the majority strips immunity because the information or query may be illegal under some statute or federal [**88] law, this circumstance puts the webhost in the role of a policeman for the laws of the fifty states and the federal system. There are not enough Net Nannies in cyberspace to implement this restriction, and the burden of filtering content would be unfathomable.

To the extent the majority strips immunity because a site solicits or actively encourages content, the result is a direct restriction on the free exchange of ideas and information on the Internet. As noted in the amici curiae brief of the news organizations, online news organization routinely solicit third-party information. Were the websites to face host liability for this content, they "would have no choice but to severely limit its use" and "[s]heer economics would dictate that vast quantities of valuable information be eliminated from websites." Brief of Amici Curiae News Organizations in Support of Roommate.com, LLC 22.

To the extent the majority strips immunity because a website "materially contributed" to the content or output of a website by "specialization" of content, this approach would essentially swallow the immunity provision. The combination of solicitation, sorting, and potential for liability would put virtually [**89] every interactive website in this category. Having a website directed to Christians, Muslims, gays, disabled [*1189] veterans, or childless couples could land the website provider in hot water.¹⁴

14 It is no surprise that there are countless specialized roommate sites. See, e.g., <http://islam.tc/housing/index.php>, <http://christian-roommates.com>, and <http://prideroommates.com>.

Because the statute itself is cumbersome to interpret

3 of 4 DOCUMENTS

Barnes v. Yahoo!, Inc.

No. 05-36189

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

570 F.3d 1096; 2009 U.S. App. LEXIS 20053; 37 Media L. Rep. 1705; 47 Comm. Reg. (P & F) 1028

**October 14, 2008, Argued and Submitted, Portland, Oregon
June 22, 2009, Amended**

SUBSEQUENT HISTORY: Amended by *Barnes v. Yahoo, Inc.*, 2009 U.S. App. LEXIS 21308 (9th Cir. Or., Sept. 28, 2009)

PRIOR HISTORY: [**1]

Appeal from the United States District Court for the District of Oregon. D.C. No. CV-05-00926-AA. Ann L. Aiken, District Judge, Presiding.
Barnes v. Yahoo!, Inc., 565 F.3d 560, 2009 U.S. App. LEXIS 10940 (9th Cir. Or., 2009)
Barnes v. Yahoo!, Inc., 2005 U.S. Dist. LEXIS 28061 (D. Or., Nov. 8, 2005)

COUNSEL: Thomas R. Rask, III, Kell, Alterman & Runstein LLP, Portland, Oregon, argued the cause for the appellant and filed briefs. Denise N. Gorrell, Kell, Alterman & Runstein LLP, Portland, Oregon, was also on the briefs.

Patrick J. Carome, Wilmer, Cutler, Pickering, Hale and Dorr LLP, Washington, D.C., argued the cause for the appellee and filed the brief; Samir Jain and C. Colin Rushing, Wilmer, Cutler, Pickering, Hale and Dorr LLP, Washington, D.C., and Reginald Davis and Eulonda Skyles, of Counsel for Yahoo!, Inc., Sunnyvale, California, were also on the brief.

JUDGES: Before: Diarmuid F. O'Scannlain, Susan P. Graber, and Consuelo M. Callahan, Circuit Judges. Opinion by Judge O'Scannlain.

OPINION BY: Diarmuid F. O'Scannlain

OPINION

[*1098] AMENDED OPINION

O'SCANNLAIN, Circuit Judge:

We must decide whether the Communications Decency Act of 1996 protects an internet service provider from suit where it undertook to remove from its website material harmful to the plaintiff but failed to do so.

I

This case stems from a dangerous, cruel, and highly indecent use of the internet for the apparent purpose [**2] of revenge.¹

1 The parties agree that, as this appeal comes to us on grant of a motion for dismissal under *Federal Rule of Civil Procedure 12(b)(6)*, we accept as true the facts alleged in the complaint and construe them in the light most favorable to the plaintiff. *Anderson v. Clow (In re Stac Electronics Securities Litig.)*, 89 F.3d 1399, 1403 (9th Cir. 1996) (also noting that "conclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss for failure to state a claim" (internal quotation marks omitted)). Yahoo has indicated that it would "hotly contest[]" the factual allegations of the complaint if it is not dismissed.

In late 2004, Cecilia Barnes broke off a lengthy relationship with her boyfriend. For reasons that are unclear, he responded by posting profiles of Barnes on a website run by Yahoo!, Inc. ("Yahoo"). According to Yahoo's Member Directory, "[a] public profile is a page with information about you that other Yahoo! members

can view. You[r] profile allows you to publicly post information about yourself that you want to share with the world. Many people post their age, pictures, location, and hobbies on their profiles." Through Yahoo's [**3] online service, computer users all over the country and the world can view such profiles.

Barnes did not authorize her now former boyfriend to post the profiles, which is hardly surprising considering their content. The profiles contained nude photographs of Barnes and her boyfriend, taken without her knowledge, and some kind of open solicitation, whether express or implied is unclear, to engage in sexual intercourse. The ex-boyfriend then conducted discussions in Yahoo's online "chat rooms," posing as Barnes and directing male correspondents to the fraudulent profiles he had created. The profiles also included the addresses, real and electronic, and telephone number at Barnes' place of employment. Before long, men whom Barnes did not know were peppering her office with emails, phone calls, and personal visits, all in the expectation of sex.

In accordance with Yahoo policy, Barnes mailed Yahoo a copy of her photo ID and a signed statement denying her involvement with the profiles and requesting their removal. One month later, Yahoo had not responded but the undesired advances from unknown men continued; Barnes again asked Yahoo by mail to remove the profiles. Nothing happened. The following [**4] month, Barnes sent Yahoo two more mailings. During the same period, a local news program was preparing to broadcast a report on the incident. A day before the [*1099] initial air date of the broadcast, Yahoo broke its silence; its Director of Communications, a Ms. Osako, called Barnes and asked her to fax directly the previous statements she had mailed. Ms. Osako told Barnes that she would "personally walk the statements over to the division responsible for stopping unauthorized profiles and they would take care of it." Barnes claims to have relied on this statement and took no further action regarding the profiles and the trouble they had caused. Approximately two months passed without word from Yahoo, at which point Barnes filed this lawsuit against Yahoo in Oregon state court. Shortly thereafter, the profiles disappeared from Yahoo's website, apparently never to return.

Barnes' complaint against Yahoo is somewhat unclear, but it appears to allege two causes of action under Oregon law. First, the complaint suggests a tort for

the negligent provision or non-provision of services which Yahoo undertook to provide. As Barnes pointed out in her briefs, Oregon has adopted *section 323 of the Restatement (Second) of Torts* [**5] (1965), which describes the elements of this claim. For the sake of brevity, we refer to this tort, which is really a species of negligence, as a "negligent undertaking." Barnes also refers in her complaint and in her briefs to Yahoo's "promise" to remove the indecent profiles and her reliance thereon to her detriment. We construe such references to allege a cause of action under *section 90 of the Restatement (Second) of Contracts* (1981).

After Yahoo removed the action to federal court, it moved to dismiss the complaint under *Federal Rule of Civil Procedure 12(b)(6)*. Yahoo contended that *section 230(c)(1)* of the Communications Decency Act ("the Act") renders it immune from liability in this case. *See 47 U.S.C. § 230(c)(1)*. The district court granted the motion to dismiss, finding that the Act did in fact protect Yahoo from liability as a matter of law. Barnes timely appealed, claiming that, in the first place, the so-called immunity under *section 230(c)* did not apply to the cause of action she has brought and that, even if it did, Yahoo did not fit under the terms of such immunity.

II

The district court dismissed Barnes' claim on the ground that *section 230(c)(1)* makes Yahoo "immune" [**6] against any liability for the content that Barnes' former boyfriend had posted. We begin by analyzing the structure and reach of the statute itself.

A

Section 230 of the Act, also known as the Cox-Wyden Amendment ("the Amendment"), protects certain internet-based actors from certain kinds of lawsuits. The Amendment begins with a statement of findings and a statement of policy, in *subsections 230(a)* and *(b)*, respectively. These are rather general, but they illustrate Congress' appreciation for the internet as a "forum for a true diversity of . . . myriad avenues for intellectual activity," which "ha[s] flourished . . . with a minimum of government regulation." § 230(a)(3)-(4). The statute's "policy" includes the promotion of interactive computer services and the "vibrant and competitive free market" for such services, as well as the encouragement of "blocking and filtering technologies that empower parents to restrict their children's access to

objectionable or inappropriate online material." § 230(b)(1)-(2) & (4)-(5). We have recognized in this declaration of statutory purpose two parallel goals. The statute is designed at once "to promote the free exchange of information and ideas over [**7] the Internet and to encourage voluntary monitoring for offensive or obscene [*1100] material." *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1122 (9th Cir. 2003).

Though we keep these goals, which the statutory language declares, in mind, we must closely hew to the text of the statutory bar on liability in construing its extent. The operative section of the Amendment is *section 230(c)*, which states in full:

(c) Protection for "good samaritan"
blocking and screening of offensive
material

(1) Treatment of publisher or speaker

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability

No provider or user of an interactive computer service shall be held liable on account of--

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical [**8] means to restrict access to material described in paragraph (1).

Section 230(c) has two parts. Yahoo relies exclusively on the first part, which bars courts from

treating certain internet service providers as publishers or speakers. Looking at the text, it appears clear that neither this subsection nor any other declares a general immunity from liability deriving from third-party content, as Yahoo argues it does. "*Subsection (c)(1)* does not mention 'immunity' or any synonym." *Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666, 669 (7th Cir. 2008). Our recent *en banc* decision in *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, rested not on broad statements of immunity but rather on a careful exegesis of the statutory language. 521 F.3d 1157, 1171 (9th Cir. 2008) (*en banc*) (noting that to "provid[e] immunity every time a website uses data initially obtained from third parties would eviscerate [the statute]" ²).

2 *Roommates* interpreted a different subsection of the Amendment, § 230(f)(3), but its approach remains instructive.

Following this approach, one notices that *subsection (c)(1)*, which after all is captioned "Treatment of publisher [**9] or speaker," precludes liability only by means of a definition. "No provider or user of an interactive computer service," it says, "*shall be treated as the publisher or speaker of any information provided by another information content provider.*" § 230(c)(1) (emphasis added). *Subsection 230(e)(3)* makes explicit the relevance of this definition, for it cautions that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." ³ Bringing these two subsections together, it appears that *subsection (c)(1)* only protects from liability (1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, ⁴ as a publisher or speaker [*1101] (3) of information provided by another information content provider.

3 Conversely, "[n]othing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section." § 230(e)(3).

4 We limit our restatement of *section 230(c)(1)* to state law claims because we deal in this case with state law claims only. We have held that the Amendment's protection also extends to federal law causes [**10] of action, *see, e.g., Fair Housing Council of San Fernando Valley v. Roommates.com*, 521 F.3d 1157 (9th Cir. 2008)

(en banc) (applying the Amendment to a cause of action under the Fair Housing Act, 42 U.S.C. § 3601 *et seq.*). Because no federal law cause of action is present in this case, we need not decide how or whether our discussion of *section 230(c)(1)* would change in the face of such a federal claim.

Barnes did not contest in the district court that Yahoo is a provider of an interactive computer service, and we have no trouble concluding that it qualifies as one.⁵ Nor is there any dispute that the "information content"--such as it is--at issue in this case was provided by another "information content provider."⁶ The flashpoint in this case is the meaning of the "publisher or speaker" part of *subsection (c)(1)*, and that is where we train our sights.

5 *Section 230* helpfully defines "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by [*11] libraries or educational institutions." § 230(f)(2).

6 The statute also tells us that this term "means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." § 230(f)(3). We have recently reiterated that "providing *neutral* tools to carry out what may be unlawful or illicit . . . does not amount to 'development'" for these purposes, *Roommates*, 521 F.3d at 1169; thus it is crystal clear that Yahoo is not an "information content provider" of the profiles.

B

By its terms, then, *section (c)(1)* only ensures that in certain cases an internet service provider⁷ will not be "treated" as the "publisher or speaker" of third-party content for the purposes of another cause of action. The question before us is how to determine when, for purposes of this statute, a plaintiff's theory of liability would treat a defendant as a publisher or speaker of third-party content.

7 *Subsection 230(c)(1)* also refers to interactive computer service users, which we do not mention

further because such reference is irrelevant to this case.

The cause of action most frequently associated with the [*12] cases on *section 230* is defamation. *See, e.g., Carafano*, 339 F.3d 1119; *Batzel v. Smith*, 333 F.3d 1018 (9th Cir. 2003). This is not surprising, because, as we and some of our sister circuits have recognized, Congress enacted the Amendment in part to respond to a New York state court decision, *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 N.Y. Misc. LEXIS 229, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995) (unpublished), which held that an internet service provider could be liable for defamation. *See e.g., Roommates*, 521 F.3d at 1163; *see also Zeran v. Am. Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997).

But "a law's scope often differs from its genesis," *Craigslist*, 519 F.3d at 671, and the language of the statute does not limit its application to defamation cases. Indeed, many causes of action might be premised on the publication or speaking of what one might call "information content." A provider of information services might get sued for violating anti-discrimination laws, *see, e.g., Roommates*, 521 F.3d 1157; for fraud, negligent misrepresentation, and ordinary negligence, *see, e.g., Doe v. MySpace, Inc.*, 528 F.3d 413 (5th Cir. 2008), *cert. denied*, 129 S. Ct. 600, 172 L. Ed. 2d 456; for false light, *see, e.g., Flowers v. Carville*, 310 F.3d 1118 (9th Cir. 2002); [*13] or even for negligent publication of advertisements that cause harm to third parties, *see Braun v. Soldier of Fortune Magazine, Inc.*, 968 F.2d 1110 (11th Cir. 1992). Thus, what matters is not the name of the cause of action--defamation versus negligence [*1102] versus intentional infliction of emotional distress--what matters is whether the cause of action inherently requires the court to treat the defendant as the "publisher or speaker" of content provided by another. To put it another way, courts must ask whether the duty that the plaintiff alleges the defendant violated derives from the defendant's status or conduct as a "publisher or speaker." If it does, *section 230(c)(1)* precludes liability.

We have indicated that publication involves reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content. *See Roommates*, 521 F.3d at 1170-71 ("[A]ny activity that can be boiled down to deciding whether to exclude material that third parties seek to post online is perforce immune under *section 230*"). We need not perform any

intellectual gymnastics to arrive at this result, for it is rooted in the common sense and common definition of what a publisher does. [**14] One dictionary defines "publisher," in relevant part, as "the reproducer of a work intended for public consumption" and also as "one whose business is publication." See Webster's Third New International Dictionary 1837 (Philip Babcock Gove ed., 1986). Thus, a publisher reviews material submitted for publication, perhaps edits it for style or technical fluency, and then decides whether to publish it. ⁸ See also *Zeran*, 129 F.3d at 330 (listing "deciding whether to publish, withdraw, postpone or alter content" as examples of "a publisher's traditional editorial functions").

8 As we pointed out in *Baizel*, it is immaterial whether this decision comes in the form of deciding what to publish in the first place or what to remove among the published material. 333 F.3d at 1032. This is particularly so in the context of the internet, where material can be "posted" and "unposted" with ease.

III

Which leads us to whether Barnes, in her negligent undertaking claim, seeks to treat Yahoo as a "publisher or speaker" of the indecent profiles in order to hold Yahoo liable.

A

The Oregon law tort that Barnes claims Yahoo committed derives from *section 323⁹ of the Restatement (Second) of Torts*, which states: [**15] One who undertakes, gratuitously or for consideration, to render services to another which he should recognize as necessary for the protection of the other's person or things, is subject to liability to the other for physical harm resulting from his failure to exercise reasonable care to perform his undertaking, if

(a) his failure to exercise such care increases the risk of such harm, or

(b) the harm is suffered because of the other's reliance upon the undertaking.

9 We do not decide in this appeal whether Barnes has properly alleged this cause of action

under Oregon law.

Barnes argues that this tort claim would not treat Yahoo as a publisher. She points to her complaint, which acknowledges that although Yahoo "may have had no initial responsibility to act, once [Yahoo,] through its agent, undertook to act, [it] must do so reasonably." According to Barnes, this makes the undertaking, not the publishing or failure to withdraw from publication, the source of liability. Under this theory, Barnes' cause of action would evade the reach of *section 230(c)* entirely because it treats Yahoo not as a publisher, but rather as one who undertook to perform a service and did it negligently.

We are not [**16] persuaded. As we implied above, a plaintiff cannot sue someone for publishing third-party content simply by changing the name of the theory from defamation to negligence. Nor can he or [**1103] she escape *section 230(c)* by labeling as a "negligent undertaking" an action that is quintessentially that of a publisher. The word "undertaking," after all, is meaningless without the following verb. That is, one does not merely undertake; one undertakes *to do* something. And what is the undertaking that Barnes alleges Yahoo failed to perform with due care? The removal of the indecent profiles that her former boyfriend posted on Yahoo's website. But removing content is something publishers do, and to impose liability on the basis of such conduct necessarily involves treating the liable party as a publisher of the content it failed to remove. See *Craigslis*, 519 F.3d at 671 (finding defendant protected because "only in a capacity as publisher could [the defendant] be liable under § 3604(c) [of the Fair Housing Act]"). In other words, the duty that Barnes claims Yahoo violated derives from Yahoo's conduct as a publisher--the steps it allegedly took, but later supposedly abandoned, to de-publish the offensive [**17] profiles. It is because such conduct is *publishing conduct* that we have insisted that *section 230* protects from liability "any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online." *Roommates*, 521 F.3d at 1170-71.

Although the tort of defamation is not the only form of liability for publishers to which *subsection (c)(1)* applies, its reach confirms our conclusion. Indeed, we note that Yahoo could be liable for defamation for precisely the conduct of which Barnes accuses it. Defamation law sometimes imposes "an affirmative duty

to remove a publication made by another." Prosser and Keaton on Torts § 113, at 803. Courts have applied this principle, including in a case that reads like a low-tech version of the situation before us. In *Hellar v. Bianco*, 111 Cal. App. 2d 424, 244 P.2d 757, 758 (Cal. Ct. App. 1952), a woman received a phone call from a man who sought to arrange an unconventional, but apparently amorous, liaison. *Id.* at 758. After being rebuffed, the man informed the woman that her phone number appeared on the bathroom wall of a local bar along with writing indicating that she "was an unchaste woman who indulged in illicit amatory ventures." [**18] *Id.* The woman's husband promptly called the bartender and demanded he remove the defamatory graffito, which the bartender said he would do when he got around to it. *Id.* at 758-59. Shortly thereafter, the husband marched to the bar, policeman in tow, and discovered the offending scrawl still gracing the wall. *Id.* at 759. He defended his wife's honor by suing the bar's owner.

The California Court of Appeal held that it was "a question for the jury whether, after knowledge of its existence, [the bar owner] negligently allowed the defamatory matter to remain for so long a time as to be chargeable with its republication." *Id.* at 759. This holding suggests that Yahoo could have been sued under our facts for defamation, one of the elements of which is publication, which strongly confirms our view that section 230(c)(1) bars this lawsuit.¹⁰

10 *Hellar* is not an anomaly, but of a piece with a longstanding theory of defamation liability. See *Byrne v. Dean*, (1937) 1 K.B. 818; *Tidmore v. Mills*, 33 Ala. App. 243, 32 So. 2d 769 (Ala. Ct. App. 1947). *Contra Scott v. Hull*, 22 Ohio App. 2d 141, 259 N.E.2d 160 (Ohio Ct. App. 1970) (accepting the *Byrne* line of cases but distinguishing it on the ground that the writing was on the outside of [**19] the proprietor's building and, thus, not [the tenant's] responsibility to remove).

B

Barnes argues that, even if subsection 230(c)(1) applies to this tort in a general sense, it does not cover her claim because [**1104] she is suing Yahoo as a distributor, not as a publisher. This argument asks us to join an ongoing academic debate, which has developed in response to the Fourth Circuit's *Zeran* opinion, on whether "publisher" in subsection 230(c)(1) means only

"primary publisher" or both "primary publisher" and "distributor," also known as a "secondary publisher," for purposes of defamation liability.

To understand this debate, we briefly sketch the liability of publishers and distributors in defamation law. One of the elements of the tort of defamation is "publication" of the defamatory matter, which simply means "communication intentionally or by a negligent act to one other than the person defamed." *Restatement (Second) of Torts* § 577(1) (1965). It is well established that "[e]very repetition of the defamation is a publication in itself," whether or not the person repeating the defamation attributes it to its source. Prosser & Keaton § 113, at 799. "[E]veryone who takes part in the publication, [**20] as in the case of the owner, editor, printer, vendor, or even carrier of a newspaper is charged with publication." *Id.*; see also *Cianci v. New Times Pub. Co.*, 639 F.2d 54, 60-61 (2d Cir. 1980) (noting the "black-letter rule that one who republishes a libel is subject to liability just as if he had published it originally" (internal quotation marks omitted)). However, defamation law assigns different requirements of fault in order to hold someone liable for different forms of publication. Hence, it became "necessary to classify participants into three categories: primary publishers, secondary publishers or disseminators, and those who are suppliers of equipment and facilities and are not publishers at all." Prosser & Keaton, § 113 at 803. Primary publishers were held to a strict liability standard, whereas secondary publishers were only liable for publishing defamation with actual or constructive knowledge of its defamatory character. *Id.* at 810-11. Secondary publishers came to be known as distributors, see, e.g., *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135, 139 (S.D.N.Y. 1991).

Pointing to this legal background, Barnes argues that the term "publisher" in section 230(c)(1) refers [**21] only to primary publishers and not to secondary publishers or distributors. She argues that because Congress enacted section 230 to overrule *Stratton Oakmont*, which held an internet service provider liable as a primary publisher, not a distributor, the statute does no more than overrule that decision's application of publisher liability. In *Zeran*, the Fourth Circuit rejected a similar argument, concluding that so-called distributor liability is merely a subset of publisher liability for purposes of defamation law. 129 F.3d at 332. We have taken note of this issue before, but have not yet had to

rule on it for ourselves. *See Batzel*, 333 F.3d at 1027 n.10 ("We . . . need not decide whether § 230(c)(1) encompasses both publishers and distributors.").

In our view, however, we need not resolve the dispute at all, because it has little to do with the meaning of the statutory language. As noted above, *section 230(c)(1)* precludes courts from treating internet service providers as publishers not just for the purposes of defamation law, with its particular distinction between primary and secondary publishers, but in general. The statute does not mention defamation, and we decline to read the [**22] principles of defamation law into it. In any event, if the reach of *section 230(c)(1)* were fastened so tightly to the nuances of defamation law, our *Roommates* opinion, which dealt with a lawsuit under the Fair Housing Act, would simply have declared that the provision did not apply because there was no claim of defamation. We will not engage in an analysis so contrary to [**1105] the reasoning, and even some of the holding, of our precedent.

Nor do we find particularly edifying the debate over the exact reach of *Stratton Oakmont*, the New York case Congress apparently meant to overrule. As the Seventh Circuit has recognized,

[a]lthough the impetus for the enactment of § 230(c) as a whole was a [decision] holding an information content provider liable, as a publisher, because it had exercised some selectivity with respect to the sexually oriented material it would host for customers, a law's scope often differs from its genesis. Once the legislative process gets rolling, interest groups seek (and often obtain) other provisions.

Craigslist, 519 F.3d at 671. Both parties make a lot of sound and fury on the congressional intent of the immunity under *section 230*, but such noise ultimately signifies [**23] nothing. It is the language of the statute that defines and enacts the concerns and aims of Congress; a particular concern does not rewrite the language.

C

Leaving no stone unturned, Barnes reminds us that the statutory purpose of the Amendment is to encourage

websites affirmatively to police themselves, not to provide an excuse for doing nothing. This argument from statutory purpose has more force to it, because *section 230(c)* is, after all, captioned "Protection for 'good samaritan' blocking and screening of offensive material." *Cf. Roommates*, 521 F.3d at 1163-64. It would indeed be strange for a provision so captioned to provide equal protection as between internet service providers who do nothing and those who attempt to block and screen offensive material. As the Seventh Circuit has recognized, if *section (c)* did provide equal protection, then "[internet service providers] may be expected to take the do-nothing option and enjoy immunity" because "precautions are costly." *GTE Corp.*, 347 F.3d at 660.

A closer look at the whole of *section 230(c)*, we believe, makes sense of this apparent contradiction. *Subsection (c)(1)*, by itself, shields from liability all publication decisions, whether [**24] to edit, to remove, or to post, with respect to content generated entirely by third parties. *Subsection (c)(2)*, for its part, provides an additional shield from liability, but only for "any action voluntarily taken in good faith to restrict access to or availability of material that the provider . . . considers to be obscene . . . or otherwise objectionable." § 230(c)(2)(A). Crucially, the persons who can take advantage of this liability are not merely those whom *subsection (c)(1)* already protects, but *any* provider of an interactive computer service. *See* § 230(c)(2). Thus, even those who cannot take advantage of *subsection (c)(1)*, perhaps because they developed, even in part, the content at issue, *see Roommates*, 521 F.3d at 1162-63, can take advantage of *subsection (c)(2)* if they act to restrict access to the content because they consider it obscene or otherwise objectionable. Additionally, *subsection (c)(2)* also protects Internet service providers from liability not for publishing or speaking, but rather for actions taken to restrict access to obscene or otherwise objectionable content.¹¹

¹¹ It might be more straightforward to narrow the meaning of "publisher" liability to include [**25] only affirmative acts of publication but not the refusal to remove obscene material. That path, however, is closed to us. *Batzel*, 333 F.3d at 1032.

Thus, we must reject Barnes' contention that it does violence to the statutory scheme to bar her suit for negligent undertaking. To summarize, we hold that

section 230(c)(1) bars Barnes' claim, under Oregon law, for negligent provision of services that Yahoo undertook to provide. [*1106] The district court properly granted Yahoo's motion to dismiss that cause of action.

IV

As we indicated above, Barnes' complaint could also be read to base liability on section 90 of the *Restatement (Second) of Contracts*, which describes a theory of recovery often known as promissory estoppel. At oral argument, counsel for Barnes acknowledged that its tort claim might be "recast" in terms of promissory estoppel. We think it might, and in analyzing it as such now we add that liability for breach of promise is different from, and not merely a rephrasing of, liability for negligent undertaking.

A

Oregon has accepted promissory estoppel as a theory of recovery. *Bixler v. First Nat'l Bank of Or.*, 49 Ore. App. 195, 619 P.2d 895, 898 (Or. Ct. App. 1980) (citing *Schafer v. Fraser*, 206 Ore. 446, 290 P.2d 190, 199-206 (Or. 1955)). [*26] The "principal criteria" that determine "when action renders a promise enforceable" under this doctrine are: "(1) a promise[;] (2) which the promisor, as a reasonable person, could foresee would induce conduct of the kind which occurred[;] (3) actual reliance on the promise[;] (4) resulting in a substantial change in position." *Id.* at 899.¹²

12 As we analyze here the reach of a federal statute that applies to all fifty states, we discuss the law of contracts generally. However, Oregon law applies to Barnes' contract claim. Any conflict between this discussion and Oregon law is to be resolved, on remand, in favor of Oregon law.

In most states, including Oregon, "[p]romissory estoppel" is not a 'cause of action' in itself; rather it is a subset of a theory of recovery based on a breach of contract and serves as a substitute for consideration." *Rick Franklin Corp. v. State ex rel. Dep't of Transp.*, 207 Ore. App. 183, 140 P.3d 1136, 1140 n.5 (Or. Ct. App. 2006). "A promise binding under [section 90 of the *Restatement*] is a contract" *Restatement (Second) of Contracts* § 90 cmt. d (emphasis added).

Thus, aside from consideration, ordinary contract

principles usually apply.¹³ Just as "[c]ontract law [*27] is designed to protect the expectations of the contracting parties," 1 Samuel Williston & Richard A. Lord, *A Treatise on the Law of Contracts* § 1.1 (4th ed. 2007), so is promissory estoppel. Similarly, the majority rule in this country is that "any promise which is to serve as the basis for a promissory estoppel claim or defense [] be as clear and well defined as a promise that could serve as an offer, or that otherwise might be sufficient to give rise to a traditional contract supported by consideration." 1 Williston & Lord, *supra* § 8.7; see also *id.* § 8.6 ("there must be a promise, gratuitous at least in the sense that there is no consideration to make it binding").

13 One area where promissory estoppel does vary ordinary contract principles is in the damages. Although "full-scale enforcement by normal remedies is often appropriate," *Restatement (Second) of Contracts* § 90 comment d, some courts have awarded damages to compensate the promisee for his expected benefit (ordinary contract damages), while others have awarded damages to compensate the promisee for his detrimental reliance, see *Jackson v. Morse*, 152 N.H. 48, 871 A.2d 47, 52-53 (N.H. 2005) (collecting cases).

This philosophy is reflected [*28] in the so-called "promissory nature" of contract. *Id.* It is no small thing for courts to enforce private bargains. The law justifies such intervention only because the parties manifest, ex ante, their mutual desire that each be able to call upon a judicial remedy if the other should breach. Thus the *Restatement* defines a promise as "a *manifestation of intention* to act or refrain from acting in a specified way, so made as [*1107] to justify a promisee in understanding that a commitment has been made." *Restatement (Second) of Contracts* § 2(1) (emphasis added). "A promisor manifests an intention if he believes or has reason to believe that the promisee will infer that intention from his words or conduct." *Id.* § 2 cmt. b.

Such, then, is the promise that promissory estoppel requires: one that the promisor intends, actually or constructively, to induce reliance on the part of the promisee. From such intention courts infer the intention that the promise be legally enforceable. Thus, when A sues B for breach of contract, A is alleging that B violated an obligation that B intended to be legally enforceable. In promissory estoppel cases, courts simply

infer that intention not from consideration but [**29] from a promise that B could have foreseen would induce A's reliance.

B

Against this background, we inquire whether Barnes' theory of recovery under promissory estoppel would treat Yahoo as a "publisher or speaker" under the Act.

As we explained above, *subsection 230(c)(1)* precludes liability when the duty the plaintiff alleges the defendant violated derives from the defendant's status or conduct as a publisher or speaker. In a promissory estoppel case, as in any other contract case, the duty the defendant allegedly violated springs from a contract--an enforceable promise--not from any non-contractual conduct or capacity of the defendant. *See GTE Corp.*, 347 F.3d at 662 ("Maybe [the] plaintiffs would have a better argument that, *by its contracts* . . ., [the defendant] assumed a duty to protect them."). Barnes does not seek to hold Yahoo liable as a publisher or speaker of third-party content, but rather as the counter-party to a contract, as a promisor who has breached.

How does this analysis differ from our discussion of liability for the tort of negligent undertaking? *See supra* pp. at 5323-25. After all, even if Yahoo did make a promise, it promised to take down third-party content from [**30] its website, which is quintessential publisher conduct, just as what Yahoo allegedly undertook to do consisted in publishing activity. The difference is that the various torts we referred to above each derive liability from behavior that is identical to publishing or speaking: publishing defamatory material; publishing material that inflicts emotional distress; or indeed attempting to de-publish hurtful material but doing it badly. To undertake a thing, within the meaning of the tort, *is* to do it.

Promising is different because it is not synonymous with the performance of the action promised. That is, whereas one cannot undertake to do something without simultaneously doing it, one can, and often does, promise to do something without actually doing it at the same time. Contract liability here would come not from Yahoo's publishing conduct, but from Yahoo's manifest intention to be legally obligated to do something, which happens to be removal of material from publication. Contract law treats the outwardly manifested intention to create an expectation on the part of another as a legally

significant event. That event generates a legal duty distinct from the conduct at hand, be it the [**31] conduct of a publisher, of a doctor, or of an overzealous uncle.¹⁴

14 We are aware of some potentially countervailing history. Both promissory estoppel and ordinary breach of contract actions evolved from the common law writ of assumpsit. J. B. Ames, *The History of Assumpsit*, 2 Harv. L. Rev. 1, 2-4 (1888). Assumpsit originally sounded in tort, for only formal contracts were enforceable as such until the refinement of the doctrine of consideration. *Id.* at 15-17; 1 Williston & Lord, *supra* § 1.16. The tort of negligent undertaking is the vestige of this original tort; promissory estoppel, too, retains some of the originally delictual nature of assumpsit. *Cf. Schafer v. Fraser*, 290 P.2d at 205-06; 1 Williston & Lord, *supra* § 8.1. Indeed, "it is not uncommon under modern rules of pleading for a plaintiff to assert one count based upon negligent failure to perform a gratuitous undertaking [under *Restatement (Second) of Torts section 323*] and another based upon promissory estoppel." 1 Williston & Lord, *supra* § 8.1.

All the same, we believe the distinction we draw is sound. Though promissory estoppel lurks on the sometimes blurry boundary between contract and tort, its *promissory* character distinguishes [**32] it from tort. That character drives our analysis here and places promissory estoppel beyond the reach of *subsection 230(c)(1)*.

[*1108] Furthermore, a court cannot simply infer a promise from an attempt to de-publish of the sort that might support tort liability under *section 323 of the Restatement (Second) of Torts*. For, as a matter of contract law, the promise must "be as clear and well defined as a promise that could serve as an offer, or that otherwise might be sufficient to give rise to a traditional contract supported by consideration." 1 Williston & Lord, *supra* § 8.7. "The formation of a contract," indeed, "requires a meeting of the minds of the parties, a standard that is measured by the objective manifestations of intent by both parties to bind themselves to an agreement." *Rick Franklin Corp.*, 140 P.3d at 1140; *see also Cosgrove v. Bartolotta*, 150 F.3d 729, 733 (7th Cir. 1998) (noting that

if "[a] promise [] is vague and hedged about with conditions . . . [the promisee] cannot plead promissory estoppel."). Thus a general monitoring policy, or even an attempt to help a particular person, on the part of an interactive computer service such as Yahoo does not suffice for contract liability. [**33] This makes it easy for Yahoo to avoid liability: it need only disclaim any intention to be bound. See *Workman v. United Parcel Serv. Inc.*, 234 F.3d 998, 1001 (7th Cir. 2000) ("[C]onsideration or reliance is a necessary but not a sufficient condition of the enforceability of a promise. Another necessary condition is that the promise be worded consistently with its being intended to be enforceable.").

One might also approach this question from the perspective of waiver.¹⁵ The objective intention to be bound by a promise--which, again, promissory estoppel derives from a promise that induces reasonably foreseeable, detrimental reliance--also signifies the waiver of certain defenses. A putative promisor might defend on grounds that show that the contract was never formed (the lack of acceptance or a meeting of the minds, for example) or that he could not have intended as the evidence at first suggests he did (unconscionability, duress, or incapacity, for example). Such defenses go to the integrity of the promise and the intention it signifies; they usually cannot be waived by the agreement they purport to undermine. But once a court concludes a promise is legally enforceable according to [**34] contract law, it has implicitly concluded that the promisor has manifestly intended that the court enforce his

promise. By so intending, he has agreed to depart from the baseline rules (usually derived from tort or statute) that govern the mine-run of relationships between strangers. *Subsection 230(c)(1)* creates a baseline rule: no liability for publishing or speaking the content of other information service providers. Insofar as Yahoo made a promise with the constructive intent that it be enforceable, it has implicitly [*1109] agreed to an alteration in such baseline.

15 Indeed, promissory estoppel developed in part out of cases in which "[p]romises of future action . . . relate[d] to an intended abandonment of an existing right." 1 Williston & Lord, *supra* § 8.4.

Therefore, we conclude that, insofar as Barnes alleges a breach of contract claim under the theory of promissory estoppel, *subsection 230(c)(1)* of the Act does not preclude her cause of action. Because we have only reviewed the affirmative defense that Yahoo raised in this appeal, we do not reach the question whether Barnes has a viable contract claim or whether Yahoo has an affirmative defense under *subsection 230(c)(2)* of the Act.

V

For [**35] the foregoing reasons, we AFFIRM IN PART, REVERSE IN PART, and REMAND for further proceedings. Each party shall bear its own costs.

in light of today's Internet architecture, and because the decision today will ripple through the billions of web pages already online, and the countless pages to come in the future, I would take a cautious, careful, and precise approach to the restriction of immunity, not the broad swath cut by the majority. I respectfully dissent and

would affirm the district court's judgment that Roommate is entitled to immunity under § 230(c)(1) of the CDA, subject to examination of whether the bare inquiry itself is unlawful.

1 of 1 DOCUMENT

UTAH CODE ANNOTATED

Copyright 2010 by Matthew Bender & Company, Inc. a member of the LexisNexis Group.
All rights reserved.

*** STATUTES CURRENT THROUGH THE 2010 GENERAL SESSION ***

*** ANNOTATIONS CURRENT THROUGH 2010 UT 23 (4/23/2010); 2010 UT App 70 (4/23/2010) AND APRIL
15, 2010 (FEDERAL CASES) ***

TITLE 13. COMMERCE AND TRADE
CHAPTER 40. UTAH E-COMMERCE INTEGRITY ACT
PART 1. GENERAL PROVISIONS

Go to the Utah Code Archive Directory

Utah Code Ann. § 13-40-101 (2010)

§ 13-40-101. Title

This chapter is known as the "Utah E-Commerce Integrity Act."

HISTORY: C. 1953, 13-40-101, enacted by L. 2010, ch. 200, § 1.

1 of 1 DOCUMENT

UTAH CODE ANNOTATED

Copyright 2010 by Matthew Bender & Company, Inc. a member of the LexisNexis Group.
All rights reserved.

*** STATUTES CURRENT THROUGH THE 2010 GENERAL SESSION ***

*** ANNOTATIONS CURRENT THROUGH 2010 UT 23 (4/23/2010); 2010 UT App 70 (4/23/2010) AND APRIL
15, 2010 (FEDERAL CASES) ***

TITLE 13. COMMERCE AND TRADE
CHAPTER 40. UTAH E-COMMERCE INTEGRITY ACT
PART 1. GENERAL PROVISIONS

Go to the Utah Code Archive Directory

Utah Code Ann. § 13-40-102 (2010)

§ 13-40-102. Definitions

As used in this chapter:

(1) (a) "Cause to be copied" means to distribute or transfer computer software, or any component of computer software.

(b) "Cause to be copied" does not include providing:

- (i) transmission, routing, intermediate temporary storage, or caching of software;
- (ii) a storage or hosting medium, such as a compact disk, website, or computer server through which the software was distributed by a third party; or
- (iii) an information location tool, such as a directory, index, reference, pointer, or hypertext link, through which the user of the computer located the software.

(2) (a) "Computer software" means a sequence of instructions written in any programming language that is executed on a computer.

(b) "Computer software" does not include a data component of a webpage that is not executable independently of the webpage.

(3) "Computer virus" means a computer program or other set of instructions that is designed to degrade the performance of or disable a computer or computer network and is designed to have the ability to replicate itself on another computer or computer network without the authorization of the owner of the other computer or computer network.

(4) "Damage" means any significant impairment to the:

- (a) performance of a computer; or

(b) integrity or availability of data, software, a system, or information.

(5) "Execute," when used with respect to computer software, means the performance of the functions or the carrying out of the instructions of the computer software.

(6) "False pretenses" means the representation of a fact or circumstance that is not true and is calculated to mislead.

(7) (a) "Identifying information" means any information that can be used to access a person's financial accounts or to obtain goods and services, including the person's:

- (i) address;
- (ii) birth date;
- (iii) Social Security number;
- (iv) driver license number;
- (v) non-driver governmental identification number;
- (vi) telephone number;
- (vii) bank account number;
- (viii) student identification number;
- (ix) credit or debit card number;
- (x) personal identification number;
- (xi) unique biometric data;
- (xii) employee or payroll number;
- (xiii) automated or electronic signature;
- (xiv) computer image file;
- (xv) photograph; or
- (xvi) computer screen name or password.

(b) "Identifying information" does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

(8) "Intentionally deceptive" means any of the following:

- (a) an intentionally and materially false or fraudulent statement;
- (b) a statement or description that intentionally omits or misrepresents material information in order to deceive an owner or operator of a computer; or
- (c) an intentional and material failure to provide a notice to an owner or operator concerning the installation or execution of computer software, for the purpose of deceiving the owner or operator.

(9) "Internet" means the global information system that is logically linked together by a globally unique address space based on the Internet protocol (IP), or its subsequent extensions, and that is able to support communications using the transmission control protocol/Internet protocol (TCP/IP) suite, or its subsequent extensions, or other IP-compatible protocols, and that provides, uses, or makes accessible, either publicly or privately, high-level services layered on communications and related infrastructure.

(10) "Internet service provider" means:

(a) an Internet service provider, as defined in *Section 76-10-1230*; or

(b) a hosting company, as defined in *Section 76-10-1230*.

(11) "Message" means a graphical or text communication presented to an authorized user of a computer.

(12) (a) "Owner or operator" means the owner or lessee of a computer, or a person using a computer with the owner's or lessee's authorization.

(b) "Owner or operator" does not include a person who owned a computer before the first retail sale of the computer.

(13) "Person" means any individual, partnership, corporation, limited liability company, or other organization, or any combination thereof.

(14) "Personally identifiable information" means any of the following information if it allows the entity holding the information to identify the owner or operator of a computer:

(a) the first name or first initial in combination with the last name and a home or other physical address including street name;

(b) a personal identification code in conjunction with a password required to access an identified account, other than a password, personal identification number, or other identification number transmitted by an authorized user to the issuer of the account or its agent;

(c) a Social Security number, tax identification number, driver license number, passport number, or any other government-issued identification number; or

(d) an account balance, overdraft history, or payment history that personally identifies an owner or operator of a computer.

(15) "Webpage" means a location that has a single uniform resource locator (URL) with respect to the World Wide Web or another location that can be accessed on the Internet.

HISTORY: C. 1953, 13-40-102, enacted by L. 2010, ch. 200, § 2.

1 of 1 DOCUMENT

UTAH CODE ANNOTATED

Copyright 2010 by Matthew Bender & Company, Inc. a member of the LexisNexis Group.
All rights reserved.

*** STATUTES CURRENT THROUGH THE 2010 GENERAL SESSION ***

*** ANNOTATIONS CURRENT THROUGH 2010 UT 23 (4/23/2010); 2010 UT App 70 (4/23/2010) AND APRIL
15, 2010 (FEDERAL CASES) ***

TITLE 13. COMMERCE AND TRADE
CHAPTER 40. UTAH E-COMMERCE INTEGRITY ACT
PART 1. GENERAL PROVISIONS

Go to the Utah Code Archive Directory

Utah Code Ann. § 13-40-103 (2010)

§ 13-40-103. Application of chapter

This chapter applies to conduct involving a computer, software, or an advertisement located in, sent to, or displayed in this state.

HISTORY: C. 1953, 13-40-103, enacted by L. 2010, ch. 200, § 3.

1 of 1 DOCUMENT

UTAH CODE ANNOTATED

Copyright 2010 by Matthew Bender & Company, Inc. a member of the LexisNexis Group.
All rights reserved.

*** STATUTES CURRENT THROUGH THE 2010 GENERAL SESSION ***

*** ANNOTATIONS CURRENT THROUGH 2010 UT 23 (4/23/2010); 2010 UT App 70 (4/23/2010) AND APRIL
15, 2010 (FEDERAL CASES) ***

TITLE 13. COMMERCE AND TRADE
CHAPTER 40. UTAH E-COMMERCE INTEGRITY ACT
PART 2. PHISHING AND PHARMING

Go to the Utah Code Archive Directory

Utah Code Ann. § 13-40-201 (2010)

§ 13-40-201. Phishing and pharming

(1) A person is guilty of phishing if, with intent to defraud or injure an individual, or with knowledge that the person is facilitating a fraud or injury to be perpetrated by another:

(a) the person makes a communication under false pretenses purporting to be by or on behalf of a legitimate business, without the authority or approval of the legitimate business; and

(b) the person uses the communication to induce, request, or solicit another person to provide identifying information or property.

(2) A person is guilty of pharming if, with intent to defraud or injure another, or with knowledge that the person is facilitating a fraud or injury to be perpetrated by another, the person:

(a) creates or operates a webpage that represents itself as belonging to or being associated with a legitimate business, without the authority or approval of the legitimate business, if that webpage may induce any user of the Internet to provide identifying information or property; or

(b) alters a setting on a user's computer or similar device or software program through which the user may search the Internet, causing any user of the Internet to view a communication that represents itself as belonging to or being associated with a legitimate business, if the message has been created or is operated without the authority or approval of the legitimate business and induces, requests, or solicits any user of the Internet to provide identifying information or property.

HISTORY: C. 1953, 13-40-201, enacted by L. 2010, ch. 200, § 4.

1 of 1 DOCUMENT

UTAH CODE ANNOTATED

Copyright 2010 by Matthew Bender & Company, Inc. a member of the LexisNexis Group.
All rights reserved.

*** STATUTES CURRENT THROUGH THE 2010 GENERAL SESSION ***

*** ANNOTATIONS CURRENT THROUGH 2010 UT 23 (4/23/2010); 2010 UT App 70 (4/23/2010) AND APRIL
15, 2010 (FEDERAL CASES) ***

TITLE 13. COMMERCE AND TRADE
CHAPTER 40. UTAH E-COMMERCE INTEGRITY ACT
PART 2. PHISHING AND PHARMING

Go to the Utah Code Archive Directory

Utah Code Ann. § 13-40-202 (2010)

§ 13-40-202. Removal of domain name or content -- Liability

If an Internet registrar or Internet service provider believes in good faith that an Internet domain name controlled or operated by the Internet registrar or Internet service provider, or content residing on an Internet website or other online location controlled or operated by the Internet registrar or Internet service provider, is used to engage in a violation of this part, the Internet registrar or Internet service provider is not liable under any provision of the laws of this state or of any political subdivision of the state for removing or disabling access to the Internet domain name or other content.

HISTORY: C. 1953, 13-40-202, enacted by L. 2010, ch. 200, § 5.

1 of 1 DOCUMENT

UTAH CODE ANNOTATED

Copyright 2010 by Matthew Bender & Company, Inc. a member of the LexisNexis Group.
All rights reserved.

*** STATUTES CURRENT THROUGH THE 2010 GENERAL SESSION ***

*** ANNOTATIONS CURRENT THROUGH 2010 UT 23 (4/23/2010); 2010 UT App 70 (4/23/2010) AND APRIL
15, 2010 (FEDERAL CASES) ***

TITLE 13. COMMERCE AND TRADE
CHAPTER 40. UTAH E-COMMERCE INTEGRITY ACT
PART 2. PHISHING AND PHARMING

Go to the Utah Code Archive Directory

Utah Code Ann. § 13-40-203 (2010)

§ 13-40-203. Application of part

(1) This part applies to the discovery of a phishing or pharming incident that occurs on or after July 1, 2010.

(2) This part does not apply to a telecommunications provider's or Internet service provider's good faith transmission or routing of, or intermediate temporary storing or caching of, identifying information.

HISTORY: C. 1953, 13-40-203, enacted by L. 2010, ch. 200, § 6.

1 of 1 DOCUMENT

UTAH CODE ANNOTATED

Copyright 2010 by Matthew Bender & Company, Inc. a member of the LexisNexis Group.
All rights reserved.

*** STATUTES CURRENT THROUGH THE 2010 GENERAL SESSION ***

*** ANNOTATIONS CURRENT THROUGH 2010 UT 23 (4/23/2010); 2010 UT App 70 (4/23/2010) AND APRIL
15, 2010 (FEDERAL CASES) ***

TITLE 13. COMMERCE AND TRADE
CHAPTER 40. UTAH E-COMMERCE INTEGRITY ACT
PART 2. PHISHING AND PHARMING

Go to the Utah Code Archive Directory

Utah Code Ann. § 13-40-204 (2010)

§ 13-40-204. Relation to other law

The conduct prohibited by this part is of statewide concern, and this part's provisions supersede and preempt any provision of law of a political subdivision of the state.

HISTORY: C. 1953, 13-40-204, enacted by L. 2010, ch. 200, § 7.

1 of 1 DOCUMENT

UTAH CODE ANNOTATED

Copyright 2010 by Matthew Bender & Company, Inc. a member of the LexisNexis Group.
All rights reserved.

*** STATUTES CURRENT THROUGH THE 2010 GENERAL SESSION ***

*** ANNOTATIONS CURRENT THROUGH 2010 UT 23 (4/23/2010); 2010 UT App 70 (4/23/2010) AND APRIL
15, 2010 (FEDERAL CASES) ***

TITLE 13. COMMERCE AND TRADE
CHAPTER 40. UTAH E-COMMERCE INTEGRITY ACT
PART 3. SPYWARE PROTECTION

Go to the Utah Code Archive Directory

Utah Code Ann. § 13-40-301 (2010)

§ 13-40-301. Prohibition on the use of software

A person who is not an owner or operator of a computer may not cause computer software to be copied on the computer knowingly, with conscious avoidance of actual knowledge, or willfully, if the software is used to:

(1) modify, through intentionally deceptive means, settings of a computer controlling:

(a) the webpage that appears when an owner or operator launches an Internet browser or similar computer software used to access and navigate the Internet;

(b) the default provider or web proxy that an owner or operator uses to access or search the Internet; or

(c) an owner's or an operator's list of bookmarks used to access webpages;

(2) collect, through intentionally deceptive means, personally identifiable information:

(a) through the use of a keystroke-logging function that records all or substantially all keystrokes made by an owner or operator of a computer and transfers that information from the computer to another person;

(b) in a manner that correlates personally identifiable information with data concerning all or substantially all of the webpages visited by an owner or operator, other than webpages operated by the person providing the software, if the computer software was installed in a manner designed to conceal from all authorized users of the computer the fact that the software is being installed; or

(c) by extracting from the hard drive of an owner's or an operator's computer, an owner's or an operator's Social Security number, tax identification number, driver license number, passport number, any other government-issued identification number, an account balance, or overdraft history for a purpose unrelated to any of the purposes of the software or service described to an authorized user;

(3) prevent, through intentionally deceptive means, an owner's or an operator's reasonable efforts to block or disable the installation or execution of computer software by causing computer software that the owner or operator has properly removed or disabled to automatically reinstall or reactivate on the computer without the authorization of an

authorized user;

(4) intentionally misrepresent that computer software will be uninstalled or disabled by an owner's or an operator's action;

(5) through intentionally deceptive means, remove, disable, or render inoperative security, antispyware, or antivirus computer software installed on an owner's or an operator's computer;

(6) enable use of an owner's or an operator's computer to:

(a) access or use a modem or Internet service for the purpose of causing damage to an owner's or an operator's computer or causing an owner or operator, or a third party affected by that conduct, to incur financial charges for a service that the owner or operator did not authorize;

(b) open multiple, sequential, stand-alone messages in an owner's or an operator's computer without the authorization of an owner or operator and with knowledge that a reasonable computer user could not close the messages without turning off the computer or closing the software application in which the messages appear, unless the communication originated from the computer's operating system, a software application the user activated, or a service provider that the user chose to use, or was presented for any of the purposes described in *Section 13-40-303*; or

(c) transmit or relay commercial electronic mail or a computer virus from the computer, if the transmission or relay is initiated by a person other than the authorized user without the authorization of an authorized user;

(7) modify, without the authorization of an owner or operator, any of the following settings related the computer's access to, or use of, the Internet:

(a) settings that protect information about an owner or operator for the purpose of taking personally identifiable information of the owner or operator;

(b) security settings, for the purpose of causing damage to a computer; or

(c) settings that protect the computer from the uses identified in Subsection (6); or

(8) prevent, without the authorization of an owner or operator, an owner's or an operator's reasonable efforts to block the installation of, or to disable, computer software by:

(a) presenting the owner or operator with an option to decline installation of computer software with knowledge that, when the option is selected by the authorized user, the installation nevertheless proceeds;

(b) falsely representing that computer software has been disabled;

(c) requiring in an intentionally deceptive manner the user to access the Internet to remove the software with knowledge or reckless disregard of the fact that the software frequently operates in a manner that prevents the user from accessing the Internet;

(d) changing the name, location, or other designation information of the software for the purpose of preventing an authorized user from locating the software to remove it;

(e) using randomized or intentionally deceptive filenames, directory folders, formats, or registry entries for the purpose of avoiding detection and removal of the software by an authorized user;

(f) causing the installation of software in a particular computer directory or in computer memory for the purpose of evading an authorized user's attempt to remove the software from the computer; or

(g) requiring, without the authority of the owner of the computer, that an authorized user obtain a special code or download software from a third party to uninstall the software.

HISTORY: C. 1953, 13-40-301, enacted by L. 2010, ch. 200, § 8.

1 of 1 DOCUMENT

UTAH CODE ANNOTATED

Copyright 2010 by Matthew Bender & Company, Inc. a member of the LexisNexis Group.
All rights reserved.

*** STATUTES CURRENT THROUGH THE 2010 GENERAL SESSION ***

*** ANNOTATIONS CURRENT THROUGH 2010 UT 23 (4/23/2010); 2010 UT App 70 (4/23/2010) AND APRIL
15, 2010 (FEDERAL CASES) ***

TITLE 13. COMMERCE AND TRADE
CHAPTER 40. UTAH E-COMMERCE INTEGRITY ACT
PART 3. SPYWARE PROTECTION

Go to the Utah Code Archive Directory

Utah Code Ann. § 13-40-302 (2010)

§ 13-40-302. Other prohibited conduct

A person who is not an owner or operator of a computer may not, with regard to the computer:

(1) induce an owner or operator to install a computer software component onto the owner's or the operator's computer by intentionally misrepresenting that installing the computer software is necessary for security or privacy reasons or in order to open, view, or play a particular type of content; or

(2) use intentionally deceptive means to cause the execution of a computer software component with the intent of causing the computer to use the computer software component in a manner that violates any other provision of this chapter.

HISTORY: C. 1953, 13-40-302, enacted by L. 2010, ch. 200, § 9.

1 of 1 DOCUMENT

UTAH CODE ANNOTATED

Copyright 2010 by Matthew Bender & Company, Inc. a member of the LexisNexis Group.
All rights reserved.

*** STATUTES CURRENT THROUGH THE 2010 GENERAL SESSION ***

*** ANNOTATIONS CURRENT THROUGH 2010 UT 23 (4/23/2010); 2010 UT App 70 (4/23/2010) AND APRIL
15, 2010 (FEDERAL CASES) ***

TITLE 13. COMMERCE AND TRADE
CHAPTER 40. UTAH E-COMMERCE INTEGRITY ACT
PART 3. SPYWARE PROTECTION

Go to the Utah Code Archive Directory

Utah Code Ann. § 13-40-303 (2010)

§ 13-40-303. Exceptions

Sections 13-40-301 and 13-40-302 do not apply to the monitoring of, or interaction with, an owner's or an operator's Internet or other network connection, service, or computer, by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service for network or computer security purposes, diagnostics, technical support, maintenance, repair, network management, authorized updates of computer software or system firmware, authorized remote system management, or detection or prevention of the unauthorized use of or fraudulent or other illegal activities in connection with a network, service, or computer software, including scanning for and removing computer software prescribed under this chapter.

HISTORY: C. 1953, 13-40-303, enacted by L. 2010, ch. 200, § 10.

1 of 1 DOCUMENT

UTAH CODE ANNOTATED

Copyright 2010 by Matthew Bender & Company, Inc. a member of the LexisNexis Group.
All rights reserved.

*** STATUTES CURRENT THROUGH THE 2010 GENERAL SESSION ***

*** ANNOTATIONS CURRENT THROUGH 2010 UT 23 (4/23/2010); 2010 UT App 70 (4/23/2010) AND APRIL
15, 2010 (FEDERAL CASES) ***

TITLE 13. COMMERCE AND TRADE
CHAPTER 40. UTAH E-COMMERCE INTEGRITY ACT
PART 4. ENFORCEMENT

Go to the Utah Code Archive Directory

Utah Code Ann. § 13-40-401 (2010)

§ 13-40-401. Phishing and pharming violations

(1) A civil action against a person who violates any provision of Part 2, Phishing and Pharming, may be filed by:

- (a) an Internet service provider that is adversely affected by the violation;
- (b) an owner of a webpage, computer server, or a trademark that is used without authorization in the violation; or
- (c) the attorney general.

(2) A person permitted to bring a civil action under Subsection (1) may obtain either actual damages for a violation of this chapter or a civil penalty not to exceed \$ 150,000 per violation of Part 2, Phishing and Pharming.

(3) A violation of Part 2, Phishing and Pharming, by a state-chartered or licensed financial institution is enforceable exclusively by the financial institution's primary state regulator.

HISTORY: C. 1953, 13-40-401, enacted by L. 2010, ch. 200, § 11.

1 of 1 DOCUMENT

UTAH CODE ANNOTATED

Copyright 2010 by Matthew Bender & Company, Inc. a member of the LexisNexis Group.
All rights reserved.

*** STATUTES CURRENT THROUGH THE 2010 GENERAL SESSION ***

*** ANNOTATIONS CURRENT THROUGH 2010 UT 23 (4/23/2010); 2010 UT App 70 (4/23/2010) AND APRIL
15, 2010 (FEDERAL CASES) ***

TITLE 13. COMMERCE AND TRADE
CHAPTER 40. UTAH E-COMMERCE INTEGRITY ACT
PART 4. ENFORCEMENT

Go to the Utah Code Archive Directory

Utah Code Ann. § 13-40-402 (2010)

§ 13-40-402. Spyware protection violations

(1) The attorney general, an Internet service provider, or a software company that expends resources in good faith assisting authorized users harmed by a violation of Part 3, Spyware Protection, or a trademark owner whose mark is used to deceive authorized users in violation of Part 3, Spyware Protection, may bring a civil action against a person who violates Part 3, Spyware Protection, to recover:

(a) actual damages and liquidated damages of at least \$ 1,000 per violation of Part 3, Spyware Protection, not to exceed \$ 1,000,000 for a pattern or practice of violations; and

(b) attorney fees and costs.

(2) The court may increase a damage award to an amount equal to not more than three times the amount otherwise recoverable under Subsection (1) if the court determines that the defendant committed the violation willfully and knowingly.

(3) The court may reduce liquidated damages recoverable under Subsection (1) to a minimum of \$ 100, not to exceed \$ 100,000 for each violation, if the court finds that the defendant established and implemented practices and procedures reasonably designed to prevent a violation of Part 3, Spyware Protection.

(4) In the case of a violation of *Subsection 13-40-301(6)(a)* that causes a telecommunications carrier or provider of voice over Internet protocol service to incur costs for the origination, transport, or termination of a call triggered using the modem or Internet-capable device of a customer of the telecommunications carrier or provider of voice over Internet protocol as a result of the violation, the telecommunications carrier or provider of voice over Internet protocol may bring a civil action against the violator:

(a) to recover the charges the telecommunications carrier or provider of voice over Internet protocol is required to pay to another carrier or to an information service provider as a result of the violation, including charges for the origination, transport, or termination of the call;

(b) to recover the costs of handling customer inquiries or complaints with respect to amounts billed for the calls;

(c) to recover reasonable attorney fees and costs; and

(d) for injunctive relief.

(5) For purposes of a civil action under Subsections (1), (2), and (3), a single action or conduct that violates more than one provision of Part 3, Spyware Protection, shall be considered as multiple violations based on the number of provisions violated.

HISTORY: C. 1953, 13-40-402, enacted by L. 2010, ch. 200, § 12.

1 of 1 DOCUMENT

UNITED STATES CODE SERVICE
Copyright © 2010 Matthew Bender & Company, Inc.
a member of the LexisNexis Group (TM)
All rights reserved.

*** CURRENT THROUGH PL 111-237, APPROVED 8/16/2010 ***

TITLE 15. COMMERCE AND TRADE
CHAPTER 22. TRADEMARKS
GENERAL PROVISIONS

Go to the United States Code Service Archive Directory

15 USCS § 1125

Review expert commentary from The National Institute for Trial Advocacy preceding 15 USCS § 1051.

THE CASE NOTES SEGMENT OF THIS DOCUMENT HAS BEEN SPLIT INTO 2 DOCUMENTS.
THIS IS PART 1.

USE THE BROWSE FEATURE TO REVIEW THE OTHER PART(S).

§ 1125. False designations of origin, false descriptions, and dilution forbidden

(a) Civil action.

(1) Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which--

(A) is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or

(B) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities,

shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.

(2) As used in this subsection, the term "any person" includes any State, instrumentality of a State or employee of a State or instrumentality of a State acting in his or her official capacity. Any State, and any such instrumentality, officer, or employee, shall be subject to the provisions of this Act in the same manner and to the same extent as any nongovernmental entity.

(3) In a civil action for trade dress infringement under this Act for trade dress not registered on the principal register, the person who asserts trade dress protection has the burden of proving that the matter sought to be protected is not functional.

(b) Importation. Any goods marked or labeled in contravention of the provisions of this section shall not be imported into the United States or admitted to entry at any customhouse of the United States. The owner, importer, or consignee of goods refused entry at any customhouse under this section may have any recourse by protest or appeal that is given under the customs revenue laws or may have the remedy given by this Act in cases involving goods refused entry or seized.

(c) Dilution by blurring; dilution by tarnishment.

(1) Injunctive relief. Subject to the principles of equity, the owner of a famous mark that is distinctive, inherently or through acquired distinctiveness, shall be entitled to an injunction against another person who, at any time after the owner's mark has become famous, commences use of a mark or trade name in commerce that is likely to cause dilution by blurring or dilution by tarnishment of the famous mark, regardless of the presence or absence of actual or likely confusion, of competition, or of actual economic injury.

(2) Definitions.

(A) For purposes of paragraph (1), a mark is famous if it is widely recognized by the general consuming public of the United States as a designation of source of the goods or services of the mark's owner. In determining whether a mark possesses the requisite degree of recognition, the court may consider all relevant factors, including the following:

- (i) The duration, extent, and geographic reach of advertising and publicity of the mark, whether advertised or publicized by the owner or third parties.
- (ii) The amount, volume, and geographic extent of sales of goods or services offered under the mark.
- (iii) The extent of actual recognition of the mark.
- (iv) Whether the mark was registered under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principal register.

(B) For purposes of paragraph (1), "dilution by blurring" is association arising from the similarity between a mark or trade name and a famous mark that impairs the distinctiveness of the famous mark. In determining whether a mark or trade name is likely to cause dilution by blurring, the court may consider all relevant factors, including the following:

- (i) The degree of similarity between the mark or trade name and the famous mark.
- (ii) The degree of inherent or acquired distinctiveness of the famous mark.
- (iii) The extent to which the owner of the famous mark is engaging in substantially exclusive use of the mark.
- (iv) The degree of recognition of the famous mark.
- (v) Whether the user of the mark or trade name intended to create an association with the famous mark.
- (vi) Any actual association between the mark or trade name and the famous mark.

(C) For purposes of paragraph (1), "dilution by tarnishment" is association arising from the similarity between a mark or trade name and a famous mark that harms the reputation of the famous mark.

(3) Exclusions. The following shall not be actionable as dilution by blurring or dilution by tarnishment under this subsection:

(A) Any fair use, including a nominative or descriptive fair use, or facilitation of such fair use, of a famous mark by another person other than as a designation of source for the person's own goods or services, including use in connection with--

- (i) advertising or promotion that permits consumers to compare goods or services; or
- (ii) identifying and parodying, criticizing, or commenting upon the famous mark owner or the goods or services of the famous mark owner.

(B) All forms of news reporting and news commentary.

(C) Any noncommercial use of a mark.

(4) Burden of proof. In a civil action for trade dress dilution under this Act for trade dress not registered on the principal register, the person who asserts trade dress protection has the burden of proving that--

- (A) the claimed trade dress, taken as a whole, is not functional and is famous; and
- (B) if the claimed trade dress includes any mark or marks registered on the principal register, the unregistered matter, taken as a whole, is famous separate and apart from any fame of such registered marks.

(5) Additional remedies. In an action brought under this subsection, the owner of the famous mark shall be entitled to injunctive relief as set forth in section 34. The owner of the famous mark shall also be entitled to the remedies set forth in sections 35(a) and 36 [15 USCS § 1117(a) and 1118], subject to the discretion of the court and the principles of equity if--

(A) the mark or trade name that is likely to cause dilution by blurring or dilution by tarnishment was first used in commerce by the person against whom the injunction is sought after the date of enactment of the Trademark Dilution Revision Act of 2006 [enacted Oct. 6, 2006]; and

(B) in a claim arising under this subsection--

(i) by reason of dilution by blurring, the person against whom the injunction is sought willfully intended to trade on the recognition of the famous mark; or

(ii) by reason of dilution by tarnishment, the person against whom the injunction is sought willfully intended to harm the reputation of the famous mark.

(6) Ownership of valid registration a complete bar to action. The ownership by a person of a valid registration under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principal register under this Act shall be a complete bar to an action against that person, with respect to that mark, that--

(A)

(i) is brought by another person under the common law or a statute of a State; and

(ii) seeks to prevent dilution by blurring or dilution by tarnishment; or

(B) asserts any claim of actual or likely damage or harm to the distinctiveness or reputation of a mark, label, or form of advertisement.

(7) Savings clause. Nothing in this subsection shall be construed to impair, modify, or supersede the applicability of the patent laws of the United States.

(d) Cyberpiracy prevention.

(1)

(A) A person shall be liable in a civil action by the owner of a mark, including a personal name which is protected as a mark under this section, if, without regard to the goods or services of the parties, that person--

(i) has a bad faith intent to profit from that mark, including a personal name which is protected as a mark under this section; and

(ii) registers, traffics in, or uses a domain name that--

(I) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark;

(II) in the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark; or

(III) is a trademark, word, or name protected by reason of *section 706 of title 18, United States Code*, or *section 220506 of title 36, United States Code*.

(B) (i) In determining whether a person has a bad faith intent described under subparagraph (A), a court may consider factors such as, but not limited to--

(I) the trademark or other intellectual property rights of the person, if any, in the domain name;

(II) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;

(III) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;

(IV) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;

(V) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;

(VI) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;

(VII) the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;

(VIII) the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and

(IX) the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c).

(ii) Bad faith intent described under subparagraph (A) shall not be found in any case in which the court determines that the person believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful.

(C) In any civil action involving the registration, trafficking, or use of a domain name under this paragraph, a court may order the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark.

(D) A person shall be liable for using a domain name under subparagraph (A) only if that person is the domain name registrant or that registrant's authorized licensee.

(E) As used in this paragraph, the term "traffics in" refers to transactions that include, but are not limited to, sales, purchases, loans, pledges, licenses, exchanges of currency, and any other transfer for consideration or receipt in exchange for consideration.

(2)

(A) The owner of a mark may file an in rem civil action against a domain name in the judicial district in which the domain name registrar, domain name registry, or other domain name authority that registered or assigned the domain name is located if--

(i) the domain name violates any right of the owner of a mark registered in the Patent and Trademark Office, or protected under subsection (a) or (c); and

(ii) the court finds that the owner--

(I) is not able to obtain in personam jurisdiction over a person who would have been a defendant in a civil action under paragraph (1); or

(II) through due diligence was not able to find a person who would have been a defendant in a civil action under paragraph (1) by--

(aa) sending a notice of the alleged violation and intent to proceed under this paragraph to the registrant of the domain name at the postal and e-mail address provided by the registrant to the registrar; and

(bb) publishing notice of the action as the court may direct promptly after filing the action.

(B) The actions under subparagraph (A)(ii) shall constitute service of process.

(C) In an in rem action under this paragraph, a domain name shall be deemed to have its situs in the judicial district in which--

(i) the domain name registrar, registry, or other domain name authority that registered or assigned the domain name is located; or

(ii) documents sufficient to establish control and authority regarding the disposition of the registration and use of the domain name are deposited with the court.

(D) (i) The remedies in an in rem action under this paragraph shall be limited to a court order for the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark. Upon receipt of written notification of a filed, stamped copy of a complaint filed by the owner of a mark in a United States district court under this paragraph, the domain name registrar, domain name registry, or other domain name authority shall--

(I) expeditiously deposit with the court documents sufficient to establish the court's control and authority regarding the disposition of the registration and use of the domain name to the court; and

(II) not transfer, suspend, or otherwise modify the domain name during the pendency of the action, except upon order of the court.

(ii) The domain name registrar or registry or other domain name authority shall not be liable for injunctive or monetary relief under this paragraph except in the case of bad faith or reckless disregard, which includes a willful failure to comply with any such court order.

(3) The civil action established under paragraph (1) and the in rem action established under paragraph (2), and any remedy available under either such action, shall be in addition to any other civil action or remedy otherwise applicable.

(4) The in rem jurisdiction established under paragraph (2) shall be in addition to any other jurisdiction that otherwise exists, whether in rem or in personam.

HISTORY:

(July 5, 1946, ch 540, Title VIII, § 43, 60 Stat. 441; Nov. 16, 1988, P.L. 100-667, Title I, § 132, 102 Stat. 3946; Oct. 27, 1992, P.L. 102-542, § 3(c), 106 Stat. 3568; Jan. 16, 1996, P.L. 104-98, § 3(a), 109 Stat. 985; Aug. 5, 1999, P.L. 106-43, §§ 3(a)(2), 5, 113 Stat. 219, 220; Nov. 29, 1999, P.L. 106-113, Div B, § 1000(a)(9), 113 Stat. 1536.)
(As amended Oct. 6, 2006, P.L. 109-312, § 2, 120 Stat. 1730.)

HISTORY; ANCILLARY LAWS AND DIRECTIVES

References in text:

Acts March 3, 1881 and February 20, 1905, referred to in this section, are Acts March 3, 1881, ch 130, 22 Stat. 388, and Feb. 20, 1905, ch 592, 33 Stat. 724, which were repealed insofar as inconsistent with *15 USCS §§ 1051 et seq.* by Act July 5, 1946, ch 540, § 46(a), 60 Stat. 444. Act Feb. 20, 1905, formerly appeared as *15 USCS §§ 81 et seq.*

"This Act", referred to in this section, is Act July 5, 1946, ch 540, 60 Stat. 427, which is popularly known as the Lanham Act or the Trademark Act of 1946, and which appears generally as *15 USCS §§ 1051 et seq.* For full classification of such Act, consult USCS Tables volumes.

Explanatory notes:

Similar provisions were contained in Act March 19, 1920, ch 104, § 3, 41 Stat. 534.

The amendment made by § 1000(a)(9) of Act Nov. 29, 1999, P.L. 106-113, is based on § 3002(a) of Title III of S. 1948 (113 Stat. 1501A-545), as introduced on Nov. 17, 1999, which was enacted into law by such § 1000(a)(9).

Effective date of section:

This section takes effect one year from its enactment, as provided by Act July 5, 1946, ch 540, § 46, 60 Stat. 444, which appears as *15 USCS § 1051* note.

Amendments:

1988. Act Nov. 16, 1988 (effective one year after enactment as provided by § 136 of such Act, which appears as *15 USCS § 1051* note) substituted subsec. (a) for one which read: "(a) Any person who shall affix, apply, or annex, or use in connection with any goods or services, or any container or containers for goods, a false designation of origin, or any false description or representation, including words or other symbols tending falsely to describe or represent the same, and shall cause such goods or services to enter into commerce, and any person who shall with knowledge of the falsity of such designation of origin or description or representation cause or procure the same to be transported or used in commerce or deliver the same to any carrier to be transported or used, shall be liable to a civil action by any person doing business in the locality falsely indicated as that of origin or in the region in which said locality is situated, or by any person who believes that he is or is likely to be damaged by the use of any such false description or representation."

1992. Act Oct. 27, 1992 (effective with respect to violations occurring on or after the date of enactment, as provided by § 4 of such Act, which appears as *15 USCS § 1114* note), in subsec. (a), redesignated paras. (1) and (2) as subparas. (A) and (B), respectively, redesignated the existing provisions of such subsection as para. (1), and added para. (2).

1996. Act Jan. 16, 1996 (effective on enactment, as provided by § 5 of such Act, which appears as a note to this section) added subsec. (c).

1999. Act Aug. 5, 1999, in subsec. (a), added para. (3); and, in subsec. (c)(2), inserted "as set forth in section 34".

Act Nov. 29, 1999 (applicable as provided by § 3010 of S. 1948, as enacted into law by such Act, which appears as *15 USCS § 1117* note) added subsec. (d).

2006. Act Oct. 6, 2006, substituted subsec. (c) for one which read:

"(c) Remedies for dilution of famous marks.

(1) The owner of a famous mark shall be entitled, subject to the principles of equity and upon such terms as the court deems reasonable, to an injunction against another person's commercial use in commerce of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark, and to obtain such other relief as is provided in this subsection. In determining whether a mark is distinctive and famous, a court may consider factors such as, but not limited to--

"(A) the degree of inherent or acquired distinctiveness of the mark;

"(B) the duration and extent of use of the mark in connection with the goods or services with which the mark is used;

"(C) the duration and extent of advertising and publicity of the mark;

"(D) the geographical extent of the trading area in which the mark is used;

"(E) the channels of trade for the goods or services with which the mark is used;

"(F) the degree of recognition of the mark in the trading areas and channels of trade used by the marks' owner and the person against whom the injunction is sought;

"(G) the nature and extent of use of the same or similar marks by third parties; and

"(H) whether the mark was registered under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principal register.

"(2) In an action brought under this subsection, the owner of the famous mark shall be entitled only to injunctive relief as set forth in section 34 unless the person against whom the injunction is sought willfully intended to trade on the owner's reputation or to cause dilution of the famous mark. If such willful intent is proven, the owner of the famous mark shall also be entitled to the remedies set forth in sections 35(a) and 36, subject to the discretion of the court and the principles of equity.

"(3) The ownership by a person of a valid registration under the Act of March 3, 1881, or the Act of February 20, 1905, or on the principal register shall be a complete bar to an action against that person, with respect to that mark, that is brought by another person under the common law or a statute of a State and that seeks to prevent dilution of the distinctiveness of a mark, label, or form of advertisement.

"(4) The following shall not be actionable under this section:

"(A) Fair use of a famous mark by another person in comparative commercial advertising or promotion to identify the competing goods or services of the owner of the famous mark.

"(B) Noncommercial use of a mark.

"(C) All forms of news reporting and news commentary.";

and, in subsec. (d)(1)(B)(i)(IX), substituted "(c)" for "(c)(1) of section 43".

Other provisions:

Repeal of inconsistent provisions and effect on existing rights. As to repeal of inconsistent provisions and effect of Act July 5, 1946, popularly known as the Lanham Act, on pending proceedings and existing registrations and rights under prior acts, see Other provisions notes to *15 USCS § 1051*.

Effective date of Jan. 16, 1996 amendments. Act Jan. 16, 1996, P.L. 104-98, § 5, 109 Stat. 987, provides: "This Act and the amendments made by this Act [amending this section and *15 USCS § 1127*] shall take effect on the date of the

enactment of this Act."

Study on abusive domain name registrations involving personal names. Act Nov. 29, 1999, P.L. 106-113, Div B, § 1000(a)(9), 113 Stat. 1536 (enacting into law § 3006 of Title III of S. 1948 (113 Stat. 1501A-550), as introduced on Nov. 17, 1999), provides:

"(a) In general. Not later than 180 days after the date of the enactment of this Act, the Secretary of Commerce, in consultation with the Patent and Trademark Office and the Federal Election Commission, shall conduct a study and report to Congress with recommendations on guidelines and procedures for resolving disputes involving the registration or use by a person of a domain name that includes the personal name of another person, in whole or in part, or a name confusingly similar thereto, including consideration of and recommendations for--

"(1) protecting personal names from registration by another person as a second level domain name for purposes of selling or otherwise transferring such domain name to such other person or any third party for financial gain;

"(2) protecting individuals from bad faith uses of their personal names as second level domain names by others with malicious intent to harm the reputation of the individual or the goodwill associated with that individual's name;

"(3) protecting consumers from the registration and use of domain names that include personal names in the second level domain in manners which are intended or are likely to confuse or deceive the public as to the affiliation, connection, or association of the domain name registrant, or a site accessible under the domain name, with such other person, or as to the origin, sponsorship, or approval of the goods, services, or commercial activities of the domain name registrant;

"(4) protecting the public from registration of domain names that include the personal names of government officials, official candidates, and potential official candidates for Federal, State, or local political office in the United States, and the use of such domain names in a manner that disrupts the electoral process or the public's ability to access accurate and reliable information regarding such individuals;

"(5) existing remedies, whether under State law or otherwise, and the extent to which such remedies are sufficient to address the considerations described in paragraphs (1) through (4); and

"(6) the guidelines, procedures, and policies of the Internet Corporation for Assigned Names and Numbers and the extent to which they address the considerations described in paragraphs (1) through (4).

"(b) Guidelines and procedures. The Secretary of Commerce shall, under its Memorandum of Understanding with the Internet Corporation for Assigned Names and Numbers, collaborate to develop guidelines and procedures for resolving disputes involving the registration or use by a person of a domain name that includes the personal name of another person, in whole or in part, or a name confusingly similar thereto."

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

Facebook, Inc.,

NO. C 08-05780 JW

Plaintiff,

v.

Power Ventures, Inc., et al.,

Defendants.

**ORDER DENYING FACEBOOK'S
MOTION FOR JUDGMENT ON THE
PLEADINGS; DENYING THE PARTIES'
CROSS-MOTIONS FOR SUMMARY
JUDGMENT; GRANTING FACEBOOK'S
MOTION TO DISMISS DEFENDANTS'
COUNTERCLAIMS; DENYING
FACEBOOK'S MOTION TO STRIKE
DEFENDANTS' AFFIRMATIVE
DEFENSES**

Power Ventures, Inc., et al.,

Counterclaimants,

v.

Facebook, Inc.,

Counterdefendants.

I. INTRODUCTION

Facebook, Inc. ("Plaintiff" or "Facebook") brings this action against Power Ventures, Inc. ("Defendant" or "Power") alleging, *inter alia*, violations of the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502 ("Section 502"). Facebook alleges that Power accessed the Facebook website in violation of Facebook's Terms of Use, and when Facebook tried to stop Power's unauthorized access, Power circumvented Facebook's technical barriers. Power brings counterclaims against Facebook alleging, *inter alia*, violations of the Sherman Act, 15 U.S.C. § 2.

Presently before the Court are Facebook's Motion for Judgment on the Pleadings Pursuant to Fed. R. Civ. P. 12(c) or, in the Alternative, Partial Summary Judgment of Liability Under California Penal Code § 502;¹ Defendants' Motion for Summary Judgment;² and Facebook's Motion to Dismiss Counterclaims and Strike Affirmative Defenses.³ The Court conducted a hearing on June 7, 2010. Based on the papers submitted to date and oral argument, the Court DENIES Facebook's Motion for Judgment on the Pleadings, DENIES the parties' Cross-Motions for Summary Judgment, GRANTS Facebook's Motion to Dismiss Defendants' counterclaims for violations of Section 2 of the Sherman Act, GRANTS Facebook's Motion to Dismiss Defendants' UCL counterclaim, and DENIES Facebook's Motion to Strike Defendants' Affirmative Defenses.

II. BACKGROUND

A. Factual Background

A detailed outline of the factual allegations in this case may be found in the Court's May 11, 2009 Order Denying Motion to Dismiss and Granting in Part and Denying in Part Motion for More Definite Statement.⁴ The Court will address the facts of the case, as they relate to the present Motions, in the Discussion section below.

B. Procedural History

In its May 11 Order, the Court denied Defendants' Motion to Dismiss Plaintiff's claims for copyright infringement, violation of the Digital Millennium Copyright Act ("DMCA"), trademark infringement under federal law, trademark infringement under state law, and violation of the California Unfair Competition Law ("UCL"), and granted Defendants' Motion for a More Definite Statement with respect to Plaintiff's UCL claim.

¹ (hereafter, "Facebook's Motion for Judgment on the Pleadings," Docket Item No. 56.)

² (Docket Item No. 62.)

³ (hereafter, "Facebook's Motion to Dismiss," Docket Item No. 58.)

⁴ (hereafter, "May 11 Order," Docket Item No. 38.)

On October 22, 2009, the Court issued an Order Granting Facebook's Motion to Dismiss Counter-Complaint and Strike Affirmative Defenses. (hereafter, "October 22 Order," Docket Item No. 52.) In its October 22 Order, the Court found that the counterclaims, as stated in Defendants' Answer and Counter-Complaint, were insufficient because they consisted only of conclusory recitations of the applicable legal standard and a general "reference [to] all allegations of all prior paragraphs as though fully set forth herein." (*Id.* at 3.) Similarly, the Court found Defendants' affirmative defenses deficient because they referenced the introductory section without delineating which allegations supported each affirmative defense. (*Id.* at 3-4.) The Court granted leave to amend the counterclaims and affirmative defenses. (*Id.* at 4.) On November 23, 2010, Defendants filed the Amended Answer and Counterclaims of Defendants Power Ventures, Inc. and Steve Vachani. (hereafter, "Amended Answer," Docket Item No. 54.) On February 26, 2010, Judge Fogel recused himself from the case. (*See* Docket Item No. 72.) On March 2, 2010, the case was reassigned to Judge Ware. (*See* Docket Item No. 73.)

Presently before the Court are the parties' various Motions. The Court addresses each Motion in turn.

III. STANDARDS

A. Motion for Judgment on the Pleadings

Under Federal Rule of Civil Procedure 12(c), any party may move for judgment on the pleadings at any time after the pleadings are closed but within such time as not to delay the trial. Fed. R. Civ. P. 12(c). "For the purposes of the motion, the allegations of the non-moving party must be accepted as true, while the allegations of the moving party which have been denied are assumed to be false." *Hal Roach Studios, Inc. v. Richard Feiner and Co., Inc.*, 896 F.2d 1542, 1550 (9th Cir. 1990). Judgment on the pleadings is proper when the moving party clearly establishes on the face of the pleadings that no material issue of fact remains to be resolved and that it is entitled to judgment as a matter of law." *Id.* When brought by the defendant, a motion for judgment on the pleadings under Federal Rule of Civil Procedure 12(c) is a "means to challenge the sufficiency of the complaint after an answer has been filed." *New. Net, Inc. v. Lavasoft*, 356 F. Supp. 2d 1090, 1115

(C.D. Cal. 2004). A motion for judgment on the pleadings is therefore similar to a motion to dismiss. Id. When the district court must go beyond the pleadings to resolve an issue on a motion for judgment on the pleadings, the proceeding is properly treated as a motion for summary judgment. Fed. R. Civ. P. 12(c); Bonilla v. Oakland Scavenger Co., 697 F.2d 1297, 1301 (9th Cir. 1982).

B. Motion for Summary Judgment

Summary judgment is proper “if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(c). The purpose of summary judgment “is to isolate and dispose of factually unsupported claims or defenses.” Celotex v. Catrett, 477 U.S. 317, 323-24 (1986).

The moving party “always bears the initial responsibility of informing the district court of the basis for its motion, and identifying the evidence which it believes demonstrates the absence of a genuine issue of material fact.” Celotex, 477 U.S. at 323. The non-moving party must then identify specific facts “that might affect the outcome of the suit under the governing law,” thus establishing that there is a genuine issue for trial. Fed. R. Civ. P. 56(e).

When evaluating a motion for summary judgment, the court views the evidence through the prism of the evidentiary standard of proof that would pertain at trial. Anderson v. Liberty Lobby Inc., 477 U.S. 242, 255 (1986). The court draws all reasonable inferences in favor of the non-moving party, including questions of credibility and of the weight that particular evidence is accorded. See, e.g. Masson v. New Yorker Magazine, Inc., 501 U.S. 496, 520 (1992). The court determines whether the non-moving party’s “specific facts,” coupled with disputed background or contextual facts, are such that a reasonable jury might return a verdict for the non-moving party. T.W. Elec. Serv. v. Pac. Elec. Contractors, 809 F.2d 626, 631 (9th Cir. 1987). In such a case, summary judgment is inappropriate. Anderson, 477 U.S. at 248. However, where a rational trier of fact could not find for the non-moving party based on the record as a whole, there is no “genuine issue for trial.” Matsushita Elec. Indus. Co. v. Zenith Radio, 475 U.S. 574, 587 (1986).

Although the district court has discretion to consider materials in the court file not referenced in the opposing papers, it need not do so. See Carmen v. San Francisco Unified School District, 237 F.3d 1026, 1028-29 (9th Cir. 2001). “The district court need not examine the entire file for evidence establishing a genuine issue of fact.” Id. at 1031. However, when the parties file cross-motions for summary judgment, the district court must consider all of the evidence submitted in support of both motions to evaluate whether a genuine issue of material fact exists precluding summary judgment for either party. The Fair Housing Council of Riverside County, Inc. v. Riverside Two, 249 F.3d 1132, 1135 (9th Cir. 2001).

C. Motion to Dismiss

Pursuant to Federal Rule of Civil Procedure 12(b)(6), a complaint may be dismissed against a defendant for failure to state a claim upon which relief may be granted against that defendant. Dismissal may be based on either the lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory. Balistreri v. Pacifica Police Dep’t, 901 F.2d 696, 699 (9th Cir. 1990); Robertson v. Dean Witter Reynolds, Inc., 749 F.2d 530, 533-34 (9th Cir. 1984). For purposes of evaluating a motion to dismiss, the court “must presume all factual allegations of the complaint to be true and draw all reasonable inferences in favor of the nonmoving party.” Usher v. City of Los Angeles, 828 F.2d 556, 561 (9th Cir. 1987). Any existing ambiguities must be resolved in favor of the pleading. Walling v. Beverly Enters., 476 F.2d 393, 396 (9th Cir. 1973).

However, mere conclusions couched in factual allegations are not sufficient to state a cause of action. Papasan v. Allain, 478 U.S. 265, 286 (1986); see also McGlinchy v. Shell Chem. Co., 845 F.2d 802, 810 (9th Cir. 1988). The complaint must plead “enough facts to state a claim for relief that is plausible on its face.” Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). A claim is plausible on its face “when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” Ashcroft v. Iqbal, 129 S. Ct. 1937, 1949 (2009). Thus, “for a complaint to survive a motion to dismiss, the non-conclusory ‘factual content,’ and reasonable inferences from that content, must be plausibly suggestive of a claim entitling the plaintiff to relief.” Moss v. U.S. Secret Serv., 572 F.3d 962, 969 (9th Cir. 2009).

Courts may dismiss a case without leave to amend if the plaintiff is unable to cure the defect by amendment. Lopez v. Smith, 203 F.3d 1122, 1129 (9th Cir. 2000).

IV. DISCUSSION

A. Statutory Standing

As a threshold matter, Defendants contend that Facebook does not have standing to bring its Section 502 claim because it has not made an adequate showing that it has suffered damage or loss within the meaning of the statute.⁵

Section 502(e)(1) provides:

In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. . . .

Facebook relies solely on the undisputed facts from the pleadings to support its Motion. In their Amended Answer, Defendants admit that: (1) Facebook communicated to Defendant Steven Vachani (“Vachani”), the purported CEO of Power.com, its claim that “Power.com’s access of Facebook’s website and servers was unauthorized and violated Facebook’s rights, including Facebook’s trademark, copyrights, and business expectations with its users;”⁶ (2) “Vachani offered to attempt to integrate Power.com with Facebook Connect,” a Facebook program that “permits integration with third party websites,” but “Vachani communicated concerns about Power’s ability to integrate Power.com with Facebook Connect on the schedule that Facebook was demanding;”⁷ and (3) “Facebook implemented technical measures to block users from accessing Facebook through

⁵ (Defendants’ Reply Brief in Support of Motion for Summary Judgment at 5-14, hereafter, “Defendants’ Reply re Summary Judgment,” Docket Item No. 68.)

⁶ (FAC ¶ 57, Amended Answer ¶ 57.)

⁷ (FAC ¶¶ 28, 58, 60, Amended Answer ¶¶ 58, 60.)

Power.com,” but nonetheless “Power provided users with tools necessary to access Facebook through Power.com.”⁸

In support of their contention that Plaintiff did not suffer damage or loss, Defendants provide the declaration of Vachani, in which he states that Facebook had no cause for concern over Power’s access to its website, and that “in its communications with [Vachani], Facebook never suggested any concern that its computers or data had been altered, deleted, damaged, or destroyed.”⁹ Vachani further declares that to his knowledge, “Facebook did not . . . make any expenditure to verify that its computers or data had not been altered, deleted, damaged, or destroyed.” (*Id.*)

Upon review of the pleadings and evidence presented, the Court finds that the undisputed facts show that Facebook suffered some damage or loss as a result of Power’s actions. Specifically, Defendants’ admissions that Facebook attempted to block Power’s access and that Power provided users with tools that allowed them to access the Facebook website through Power.com adequately demonstrates that Facebook expended resources to stop Power from committing acts that Facebook now contends constituted Section 502 violations. Although Defendants contend that any steps that Facebook took to block Power’s access to the Facebook website were *de minimus*, and would involve only a “a few clicks of a mouse . . . and ten keystrokes,”¹⁰ Section 502 sets no threshold level of damage or loss that must be reached to impart standing to bring suit. Under the plain language of the statute, any amount of damage or loss may be sufficient.

Moreover, Defendants provide no foundation to establish that Vachani has personal knowledge of what steps Facebook took, or would reasonably have to take, to block Power’s access to the Facebook website. Since information regarding Facebook’s technical measures, and the cost

⁸ (FAC ¶¶ 63-64, Amended Answer ¶¶ 63-64.)

⁹ (Declaration of Steve Vachani in Support of Defendants’ Opposition to Facebook Inc.’s Motion for Judgment on the Pleadings Pursuant to Fed. R. Civ. P. 12(c) or, in the Alternative, Partial Summary Judgment of Liability Under California Penal Code § 502(c) ¶ 12, hereafter, “Vachani Decl.,” Docket Item No. 65.)

¹⁰ (Vachani ¶ 9.)

1 Facebook expended implementing those measures, is likely to be in Facebook's possession and not
2 Power's, the Court finds that Vachani's declaration alone cannot defeat Plaintiff's standing.

3 Defendants further contend that to impart standing, damage or loss must amount to an
4 "injury." (Defendants' Reply re Summary Judgment at 4.) The statute defines an "injury" as "any
5 alteration, deletion, damage, or destruction of a computer system, computer network, computer
6 program, or data caused by the access, or the denial of access, to legitimate users of a computer
7 system, network, or program." Cal. Penal Code § 502(b)(8). However, Defendants provide no
8 authority for equating damage and loss with injury beyond the observation that the terms are
9 synonyms. (Defendants' Reply re Summary Judgment at 4.) In fact, the only place in Section 502
10 that the term injury appears, other than the clause defining the term itself, is in the criminal liability
11 provision, which has no bearing on the civil provision granting a private right of action. See §
12 502(d) (setting more stringent penalties for violations that result in an injury).

13 Since the undisputed facts demonstrate that Facebook has suffered some damage or loss in
14 attempting to block Power's access to the Facebook website, the Court finds that Facebook has
15 standing to bring suit pursuant to Section 502(e). The Court proceeds to examine Defendants'
16 liability under Section 502.

17 **B. Defendants' Section 502 Liability**

18 Facebook contends that the undisputed facts prove that Defendants violated Section 502.
19 (Facebook's Motion for Judgment on the Pleadings at 1.) Facebook bases its Section 502 claim
20 solely on facts that Defendants admit in their Amended Answer, which Facebook contends show
21 beyond dispute that Power accessed the Facebook website in violation of the Facebook terms of use,
22 and that when Facebook tried to stop Power, Power worked around Facebook's technical barriers.
23 (Id.) Defendants respond, *inter alia*, that there is no evidence that Power ever accessed the

Facebook website without the express permission of the user and rightful owner of the accessed data.¹¹

On May 5, 2010, the Court granted the Electronic Frontier Foundation's ("EFF") Motion to File Amicus Curiae in support of Defendants' Motion.¹² EFF contends that in order to avoid constitutional vagueness concerns, the Court must construe the statutory phrase "without permission" narrowly to exclude access to a website or computer network that merely violates a term of use.¹³ Allowing criminal liability based only on violation of contractual terms of service, EFF contends, would grant the website or network administrator essentially unlimited authority to define the scope of criminality and potentially expose millions of average internet users to criminal sanctions without any meaningful notice. (*Id.*)

The Court finds that all of the subsections of Section 502(c) that potentially apply in this case require that the defendant's actions be taken "without permission." *See* Cal. Penal Code § 502(c)(2), (3), (7). However, the statute does not expressly define the term "without permission." In interpreting any statutory language, the court looks first to the words of the statute. *Lamie v. U.S. Trustee*, 540 U.S. 526, 534 (2004). If the language is unambiguous, the statute should be interpreted according to the plain meaning of the text. *Id.* at 534. The structure and purpose of a statute can provide guidance in determining the plain meaning of its provisions. *K-Mart Corp. v. Cartier, Inc.*, 486 U.S. 281, 291 (1988). Statutory language is ambiguous if it is capable of being understood in two or more possible senses or ways. *Chickasaw Nation v. United States*, 534 U.S. 84, 90 (2001). If

¹¹ (Defendants' Corrected Opposition to Facebook Inc.'s Motion for Judgment on the Pleadings Pursuant to Fed. R. Civ. P. 12(c) or, in the Alternative, Partial Summary Judgment of Liability Under California Penal Code § 502(c) at 11, hereafter, "Defendants' Opposition re Summary Judgment," Docket Item No. 74.)

¹² (Docket Item No. 79.)

¹³ (Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendant Power Ventures' Motion for Summary Judgment on Cal. Penal Code 502(c) at 24-28, hereafter, "Amicus Brief," Docket Item No. 83.) On July 6, 2010, Facebook filed its Reply to EFF's Amicus Brief. (hereafter, "Amicus Reply," Docket Item No. 86.)

a statutory provision is ambiguous, the court turns to the legislative history for guidance. SEC v. McCarthy, 322 F.3d 650, 655 (9th Cir. 2003).

Here, the Court first looks to the plain language of the statute. However, the term “without permission” can be understood in multiple ways, especially with regard to whether access is without permission simply as a result of violating the terms of use. Thus, the Court must consider legislative intent and constitutional concerns to determine whether the conduct at issue here falls within the scope of the statute. See F.C.C. v. Fox Television Stations, Inc., 129 S. Ct. 1800, 1811 (2009) (noting that “the canon of constitutional avoidance in an interpretive tool, counseling that ambiguous statutory language be construed to avoid serious constitutional doubts”).

1. Plain Language of the Statute

Here, Facebook does not allege that Power has altered, deleted, damaged, or destroyed any data, computer, computer system, or computer network, so the subsections that require that type of action are not applicable. However, the Court finds that the following subsections of Section 502 do not require destruction of data, and thus may apply here:

- (1) Section 502(c)(2) holds liable any person who “[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network;”
- (2) Section 502(c)(3) holds liable any person who “[k]nowingly and without permission uses or causes to be used computer services;” and
- (3) Section 502(c)(7) holds liable any person who “[k]nowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.”

To support its claim that Defendants violated these provisions, Facebook relies solely on facts that Defendants admitted in their Amended Answer. Specifically, Facebook points to Defendants’ admissions that: (1) “Power permits users to enter their account information to access the Facebook site through Power.com;”¹⁴ (2) “Defendants developed computer software and other automated devices and programs to access and obtain information from the Facebook website for

¹⁴ (Amended Answer ¶¶ 18, 45, 50.)

aggregating services;”¹⁵ (3) Facebook communicated to Vachani its claims that “Power.com’s access of Facebook’s website and servers was unauthorized and violated Facebook’s rights, including Facebook’s trademark, copyrights, and business expectations with its users;”¹⁶ (4) “Facebook implemented technical measures to block users from accessing Facebook through Power.com;”¹⁷ and (5) “Power provided users with tools necessary to access Facebook through Power.com.”¹⁸ Since all three of the subsections at issue here require that Defendants’ acts with respect to the computer or computer network be taken without permission, the Court analyzes that requirement first.

Defendants and EFF contend that Power’s actions could not have been without permission because Power only accessed the Facebook website with the permission of a Facebook account holder and at that account holder’s behest. (See Defendants’ Opposition re Summary Judgment at 11; Amicus Brief at 11.) Facebook, on the other hand, contends that regardless of whatever permission an individual Facebook user may have given to Power to access a particular Facebook account, Power’s actions clearly violated the website’s terms of use, which state that a Facebook user may not “collect users’ content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without [Facebook’s] permission.”¹⁹

Since Power admits that it utilized “automated devices” to gain access to the Facebook website, the Court finds that it is beyond dispute that Power’s activities violated an express term of

¹⁵ (Id. ¶ 74; FAC ¶ 74.)

¹⁶ (Amended Answer ¶ 57; FAC ¶ 57.)

¹⁷ (Amended Answer ¶ 63.)

¹⁸ (Id. ¶ 64.)

¹⁹ (Facebook Inc.’s Reply Brief in Support of its Motion for Judgment on the Pleadings or, in the Alternative, Partial Summary Judgment of Liability Under California Penal Code Section 502 and Opposition to Defendants’ Motion for Summary Judgment at 5-6, hereafter, “Facebook’s Reply re Summary Judgment,” Docket Item No. 66.)

the Facebook terms of use.²⁰ The issue then becomes whether an access or use that involves a violation of the terms of use is “without permission” within the meaning of the statute. In the modern context, in which millions of average internet users access websites every day without ever reading, much less understanding, those websites’ terms of use, this is far from an easy or straightforward question. Without clear guidance from the statutory language itself, the Court turns to case law, legislative intent, and the canon of constitutional avoidance to assist in interpreting the statute, and then analyzes whether the acts at issue here were indeed taken without permission.

2. Caselaw

Since the California Supreme Court has not directly addressed the question of whether the violation of a term of use constitutes access or use without permission pursuant to Section 502, the Court looks to analogous state appellate court cases and federal court cases from this district for guidance as to the statute’s proper construction. The Court also considers cases interpreting the Computer Fraud and Abuse Act (“CFAA”), the federal corollary to Section 502, in evaluating how broad an application Section 502 should properly be given.

EFF relies on two state appellate cases for the proposition that Section 502 should not apply to persons who have permission to access a computer or computer system, but who use that access in a manner that violates the rules applicable to that system. Chrisman v. City of Los Angeles, 155 Cal. App. 4th 29, 32 (Cal. Ct. App. 2007); Mahru v. Superior Court, 191 Cal. App. 3d 545, 549 (Cal. Ct. App. 1987). In Chrisman, the court found that a police officer did not violate Section 502 when, while on duty, the officer “accessed the Department computer system [] for non-duty-related activities.” 155 Cal. App. 4th at 32. The court found that at essence, Section 502 is an anti-hacking statute, and “[o]ne cannot reasonably describe appellant’s improper computer inquiries about celebrities, friends, and others as hacking.” Id. at 35. The officer’s “computer queries seeking

²⁰ This, of course, assumes that Power was in fact subject to the Facebook terms of use, an issue which was not briefed by either party. However, the terms of use state, “By accessing or using our web site . . . , you (the ‘User’) signify that you have read, understand and agree to be bound by these Terms of Use . . . , whether or not you are a registered member of Facebook.” (FAC, Ex. A.) Thus, in the act of accessing or using the Facebook website alone, Power acceded to the Terms of Use and became bound by them.

1 information that the department's computer system was designed to provide to officers was
2 misconduct if he had no legitimate purpose for that information, but it was not hacking the
3 computer's 'logical, arithmetical, or memory function resources,' as [the officer] was entitled to
4 access those resources." Id. While Chrisman does not address the specific issue before the Court
5 here, and focuses on the statutory definition of "access" rather than "without permission," the Court
6 finds that the case helps to clarify that using a computer network for the purpose that it was designed
7 to serve, even if in a manner that is otherwise improper, is not the kind of behavior that the
8 legislature sought to prohibit when it enacted Section 502.

9 In Mahru, the court found that the director and part owner of a data-processing firm was not
10 liable under Section 502 when he instructed the company's chief computer operator to make
11 specified changes in the names of two files in a former customer's computer program in retaliation
12 for that customer terminating its contract with the company. 191 Cal. App. 3d at 547-48. These
13 changes had the effect of preventing the former customer's employees from being able to run their
14 computer programs without the assistance of an expert computer software technician. Id. In finding
15 that Section 502 had not been violated by the company's actions, the court stated:

16 The Legislature could not have meant, by enacting section 502, to bring the Penal Code into
17 the computer age by making annoying or spiteful acts criminal offenses whenever a
18 computer is used to accomplish them. Individuals and organizations use computers for
19 typing and other routine tasks in the conduct of their affairs, and sometimes in the course of
20 these affairs they do vexing, annoying, and injurious things. Such acts cannot all be
21 criminal.

22 Id. at 549. However, the court in Mahru based its finding of no liability in part on documentary
23 evidence establishing that the company, and not the former customer, owned the computer hardware
24 and software, which explains why the company's manipulation of files stored on that computer
25 hardware was merely vexatious and not unlawful hacking. The Court finds that Mahru is not
26 applicable to the circumstances here, where it is undisputed that Power accessed data stored on
27 Facebook's server.

28 In support of its contention that Facebook users cannot authorize Power to access Facebook's
computer systems, Facebook relies on a previous order in this case and another case from this

District. On May 11, 2009, Judge Fogel issued an order denying Defendants' Motion to Dismiss Plaintiff's copyright infringement, DMCA, and trademark infringement claims. In addressing Plaintiff's copyright infringement claim, Judge Fogel found that, "[v]iewing the allegations in the FAC as true, the utilization of Power.com by Facebook users exceeds their access rights pursuant to the Terms of Use. Moreover, when a Facebook user directs Power.com to access the Facebook website, an unauthorized copy of the user's profile page is created." (May 11 Order at 6-7.) The Court finds that whether or not Facebook users' utilization of Power.com exceeds their access rights under Facebook's terms of use is not the issue presented in these Motions. Instead, the Court must determine whether such a violation of the terms of use constitutes use "without permission" within the meaning of Section 502, a question that the May 11 Order did not directly address.

Finally, in Facebook, Inc. v. ConnectU LLC, Judge Seeborg found that a competing social networking site violated Section 502 when it accessed the Facebook website to collect "millions" of email addresses of Facebook users, and then used those email addresses to solicit business for itself. 489 F. Supp. 2d 1087, 1089 (N.D. Cal. 2007). In that case, Judge Seeborg found unavailing ConnectU's contention that it did not act without permission because it only "accessed information on the Facebook website that ordinarily would be accessible only to registered users by using log-in information voluntarily supplied by registered users." Id. at 1090-91. Judge Seeborg found that ConnectU was subject to Facebook's terms of use and rejected ConnectU's contention that "a private party cannot define what is or what is not a criminal offense by unilateral imposition of terms and conditions of use." Id. at 1091. The court held that "[t]he fact that private parties are free to set the conditions on which they will grant such permission does not mean that private parties are defining what is criminal and what is not." Id.

The Court finds that of the cases discussed so far, the holding in ConnectU is most applicable to the present case. However, the Court respectfully disagrees with ConnectU in one key respect. Contrary to the holding of ConnectU, the Court finds that allowing violations of terms of use to fall within the ambit of the statutory term "without permission" does essentially place in private hands unbridled discretion to determine the scope of criminal liability recognized under the statute. If the

1 issue of permission to access or use a website depends on adhering to unilaterally imposed
2 contractual terms, the website or computer system administrator has the power to determine which
3 actions may expose a user to criminal liability. This raises constitutional concerns that will be
4 addressed below.

5 Although cases interpreting the scope of liability under the CFAA do not govern the Court's
6 analysis of the scope of liability under Section 502, CFAA cases can be instructive. EFF points to
7 several CFAA cases for the proposition that the CFAA prohibits trespass and theft, not mere
8 violations of terms of use. See, e.g., LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130 (9th Cir.
9 2009) ("[F]or purposes of the CFAA, when an employer authorizes an employee to use a company
10 computer subject to certain limitations, the employee remains authorized to use the computer even if
11 the employee violates those limitations."); Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d
12 1322 (N.D. Ga. 2007) ("Under the more reasoned view, a violation for accessing 'without
13 authorization' occurs only where initial access is not permitted."); But see Shurgard Storage Ctrs.,
14 Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125-29 (W.D. Wash. 2000) (finding
15 employee may be held liable under CFAA for taking employer information from the company's
16 computer system to his next job on the ground that he was "without authorization" when he
17 "allegedly sent [the employer's] proprietary information to the defendant").

18 While there appears to be some disagreement in the district courts as to the scope of the term
19 "without authorization" in the CFAA context, the Court finds the Ninth Circuit's opinion in LVRC
20 Holdings to be particularly useful in construing the analogous term in Section 502. In that case, the
21 Ninth Circuit found that access to a computer may be "authorized," within the statutory meaning of
22 the term, even if that access violates an agreed upon term of using that computer. In general, the
23 Court finds that the more recent CFAA cases militate for an interpretation of Section 502 that does
24 not premise permission to access or use a computer or computer network on a violation of terms of
25 use. However, since none of the cases discussed provides a definitive definition of without
26 permission under Section 502, the Court now looks to the legislative purpose of the statute to the
27 extent that it can be discerned.

3. Legislative Purpose

Section 502 includes the following statement of statutory purpose:

It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.

The Legislature further finds that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data.

Cal. Penal Code § 502(a).

Facebook contends that this language evidences legislative intent to address conduct beyond “straightforward hacking and tampering.” (Facebook’s Reply re Summary Judgment at 2.) Specifically, Facebook contends that the legislature’s use of the phrases “protection . . . from . . . unauthorized access” and “protection of the integrity of all types and forms of computers, computer systems, and computer data” demonstrates a far-reaching legislative purpose to protect the entire commercial computer infrastructure from trespass. (*Id.* at 2-3.)

The Court declines to give the statute’s statement of legislative intent the sweeping meaning that Facebook ascribes to it. Section 502(a) speaks in general terms of a “proliferation of computer crime and other forms of unauthorized access to computers,” but does not offer any further guidance as to what specific acts would constitute such crime or unauthorized access. It is far from clear what conduct the legislature believed posed a threat to the integrity of computers and computer systems, or if the legislature could even fathom the shape that those threats would take more than twenty years after the statute was first enacted.

Thus, the Court does not assign any weight to the statute’s statement of legislative intent in construing the liability provisions of Section 502.

4. Rule of Lenity

EFF contends that interpreting Section 502 broadly to allow liability where the absence of permission is based only on the violation of a contractual term of use or failure to fully comply with a cease and desist letter would render the statute unconstitutionally vague, stripping the statute of adequate notice to citizens of what conduct is criminally prohibited. (Amicus Brief at 24-28.) EFF further contends that giving the statute the broad application that Facebook seeks could expose large numbers of average internet users to criminal liability for engaging in routine web-surfing and emailing activity. (*Id.*)

“It is a fundamental tenet of due process that ‘[n]o one may be required at peril of life, liberty or property to speculate as to the meaning of penal statutes.’ Lanzetta v. New Jersey, 306 U.S. 451, 453 (1993). Thus, a criminal statute is invalid if it “fails to give a person of ordinary intelligence fair notice that his contemplated conduct is forbidden.” United States v. Harriss, 347 U.S. 612 (1954). Where a statute has both criminal and noncriminal applications, courts must interpret the statute consistently in both contexts. Leocal v. Ashcroft, 543 U.S. 1, 11 n.8 (2004). In the Ninth Circuit, “[t]o survive vagueness review, a statute must ‘(1) define the offense with sufficient definiteness that ordinary people can understand what conduct is prohibited; and (2) 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).

The Court finds that interpreting the statutory phrase “without permission” in a manner that imposes liability for a violation of a term of use or receipt of a cease and desist letter would create a constitutionally untenable situation in which criminal penalties could be meted out on the basis of violating vague or ambiguous terms of use. In the words of one commentator, “By granting the computer owner essentially unlimited authority to define authorization, the contract standard delegates the scope of criminality to every computer owner.”²¹ Users of computer and internet services cannot have adequate notice of what actions will or will not expose them to criminal

²¹ Orin S. Kerr, *Cybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1650-51 (2003).

1 liability when a computer network or website administrator can unilaterally change the rules at any
2 time and are under no obligation to make the terms of use specific or understandable to the general
3 public. Thus, in order to avoid rendering the statute constitutionally infirm, the Court finds that a
4 user of internet services does not access or use a computer, computer network, or website without
5 permission simply because that user violated a contractual term of use.²²

6 If a violation of a term of use is by itself insufficient to support a finding that the user's
7 access was "without permission" in violation of Section 502, the issue becomes what type of action
8 would be sufficient to support such a finding. The Court finds that a distinction can be made
9 between access that violates a term of use and access that circumvents technical or code-based
10 barriers that a computer network or website administrator erects to restrict the user's privileges
11 within the system, or to bar the user from the system altogether.²³ Limiting criminal liability to
12 circumstances in which a user gains access to a computer, computer network, or website to which
13 access was restricted through technological means eliminates any constitutional notice concerns,
14 since a person applying the technical skill necessary to overcome such a barrier will almost always
15 understand that any access gained through such action is unauthorized. Thus, the Court finds that
16 accessing or using a computer, computer network, or website in a manner that overcomes technical
17 or code-based barriers is "without permission," and may subject a user to liability under Section 502.

18 Applying this construction of the statute here, the Court finds that Power did not act "without
19 permission" within the meaning of Section 502 when Facebook account holders utilized the Power
20 website to access and manipulate their user content on the Facebook website, even if such action
21 violated Facebook's Terms of Use. However, to the extent that Facebook can prove that in doing so,
22 Power circumvented Facebook's technical barriers, Power may be held liable for violation of
23 Section 502. Here, Facebook relies solely on the pleadings for its Motion. In their Answer,

24
25 ²² This is not to say that such a user would not be subject to a claim for breach of contract.
26 Where a user violates a computer or website's terms of use, the owner of that computer or website
may also take steps to remove the violating user's access privileges.

27 ²³ See generally Kerr, *supra* note 20.

Defendants do not directly admit that the tools Power provided to its users were designed to circumvent the technical barriers that Facebook put in place to block Power's access to the Facebook website. Thus, the Court finds that there is a genuine issue of material fact as to whether Power's access or use of the Facebook website was "without permission" within the meaning of Section 502.

EFF contends that even if Power evaded the technical barriers that Facebook implemented to deny it access, Power's conduct does not fall within the scope of Section 502 liability. (Amicus Brief at 19-28.) More specifically, EFF contends that it would be inconsistent to allow liability for ignoring or bypassing technical barriers whose sole purpose is to enforce contractual limits on access while denying liability for violating those same contractual limits when technological means of restricting access are not employed. (*Id.* at 19.) Thus, according to EFF, Power's efforts to circumvent Facebook's IP-blocking efforts did not violate Section 502 because Facebook was merely attempting to enforce its Terms of Use by other means.²⁴ (*Id.* at 23-24.) The Court finds EFF's contentions unpersuasive in this regard. EFF has not pointed to any meaningful distinction between IP address blocking and any other conceivable technical barrier that would adequately justify not finding Section 502 liability in one instance while finding it in the other. Moreover, the owners' underlying purpose or motivation for implementing technical barriers, whether to enforce terms of use or otherwise, is not a relevant consideration when determining the appropriate scope of liability for accessing a computer or network without authorization. There can be no ambiguity or mistake as to whether access has been authorized when one encounters a technical block, and thus

²⁴ The Court notes that although both parties discuss IP address blocking as the form of technological barrier that Facebook utilized to deny Power access, Facebook's use of IP-blocking and Power's efforts to avoid those blocks have not been established as undisputed facts in this case. However, for purposes of this Motion, the Court finds that the specific form of the technological barrier at issue or means of circumventing that barrier are not relevant. Rather, the issue before the Court is whether there are undisputed facts to establish that such avoidance of technological barriers occurred in the first instance.

1 there is no potential failure of notice to the computer user as to what conduct may be subject to
2 criminal liability, as when a violation of terms of use is the sole basis for liability.²⁵

3 Accordingly, the Court DENIES Facebook's Motion for Judgment on the Pleadings, and
4 DENIES the parties' Cross-Motions for Summary Judgment as to Facebook's Section 502 cause of
5 action.

6 **C. Defendants' Counterclaims**

7 Facebook moves to dismiss Defendants' causes of action for violation of Section 2 of the
8 Sherman Act ("Section 2") on the ground that Defendants have failed to allege sufficient facts to
9 state a claim for monopolization or attempted monopolization. (Facebook's Motion to Dismiss at 4-
10 9.)

11 To state a Section 2 claim for monopolization, the claimant must show that the alleged
12 monopolist (1) possesses monopoly power in the relevant market (2) through the willful acquisition
13 or maintenance of that power, as distinguished from growth or development as a consequence of a
14 superior product, business acumen, or historic accident, (3) that causes antitrust injury. Verizon
15 Commc'ns v. Trinko, 540 U.S. 398, 407 (2004).

16 Since the Court finds that the element of willful acquisition or maintenance of monopoly
17 power is dispositive, the Court addresses this issue first. Defendants allege, in pertinent part:

18 Facebook has acquired and maintained market power through two devices:
19 Facebook solicited (and continues to solicit) internet users to provide their account names
20 and passwords for users' email and social networking accounts, such as Google's Gmail,
21 AOL, Yahoo, Hotmail, or other third party websites. Facebook then uses the account
22 information to allow the user to access those accounts through Facebook, and to run
23 automated scripts to import their lists of friends and other contacts—i.e., to “scrape
24 data”—from those third-party sites into Facebook. This practice fueled Facebook's growth by
25 allowing Facebook to add millions of new users, and to provide users with convenient tools
26 to encourage their friends and contacts to join Facebook as well. On information and belief
27 it is estimated that at least approximately 35% to 50% of Facebook's “132 million active
28 users” . . . registered with Facebook as a result of an invitation generated using this device.

25 ²⁵ As Facebook contends in its Amicus Reply, the Court finds that evidence of Power's
26 efforts to circumvent Facebook's technical barrier is also relevant to show the necessary mental state
27 for Section 502 liability. (Amicus Reply at 10-11.) Since the facts relating to such circumvention
28 efforts are still in dispute, the Court finds that there is also a genuine issue of material fact as to
whether Defendants possessed the requisite mental state.

Facebook simultaneously prohibited (and prohibits) users from using the same type of utility to access their own user data when it is stored on the Facebook site. Thus, Facebook prohibits users from logging into Facebook through third-party sites, such as Power.com, and also restricts users from running automated scripts to retrieve their own user data from the Facebook site.

(Amended Answer ¶ 174.)

Facebook has also maintained its monopoly power by systematically threatening new entrants, such as Power.com and others, who seek to attract users through the same device . . . that Facebook itself used to fuel its own growth. On information and belief, for approximately the past 36 months, Facebook has threatened dozens of new entrants since 2006 with baseless intellectual property claims, and has engaged in systematic and widespread copyright misuse . . . to discourage market entry and to stifle competition from new entrants.

(Amended Answer ¶ 176.)

The Court finds that Defendants' allegations cannot support a Section 2 monopolization claim. Defendants cite no authority for the proposition that Facebook is somehow obligated to allow third-party websites unfettered access to its own website simply because some other third-party websites grant that privilege to Facebook. In fact, the Ninth Circuit has held that merely introducing a product that is not technologically interoperable with competing products is not violative of Section 2. See Foremost Pro Color, Inc. v. Eastman Kodak Co., 703 F.2d 534 (9th Cir. 1983).

In response to Facebook's Motion, Defendants merely assert that Facebook's actions are anticompetitive because Defendants have alleged so, and that the Court must accept this allegation as true at the motion to dismiss stage.²⁶ In maintaining this position, Defendants miss the fact that the issue of whether or not a particular practice is anticompetitive is determinative of an essential element of a monopoly claim, and is thus a question of law that may be determined by the Court. The Court is not obligated to accept as true Defendants' allegations that amount to conclusions of law, and the Court rejects Defendants' naked assertion here that Facebook's practices are predatory. Papasan, 478 U.S. at 286.

²⁶ (Defendants' Opposition to Motion of Facebook, Inc. to Dismiss Counterclaims and Strike Affirmative Defenses at 4-5, hereafter, "Defendants' Opposition re Motion to Dismiss," Docket Item No. 63.)

The Court likewise finds that Defendants' allegation that Facebook maintained monopoly power by threatening potential new entrants to the social networking market with baseless intellectual property lawsuits cannot support a Section 2 claim. If Facebook has the right to manage access to and use of its website, then there can be nothing anticompetitive about taking legal action to enforce that right. Furthermore, whether or not a particular lawsuit is "baseless" is a legal conclusion, and thus the Court need not accept Defendants' allegations as to the merits of Facebook's lawsuits as true. Again, Defendants cite no authority for the proposition that filing lawsuits against competitors for infringing on one's intellectual property rights can be deemed an anticompetitive or predatory practice.

In light of the Court's finding that Defendants do not plead sufficient facts to satisfy one of the essential elements of their Section 2 claim, the Court need not address the sufficiency of Defendants' pleadings as to the remaining elements. Since anticompetitive conduct is also an element of a claim for attempted monopolization under Section 2, the Court finds that Defendants' pleadings are deficient as to that claim as well. See Coalition for ICANN Transparency, Inc. v. VeriSign, Inc., 567 F.3d 1084, 1093 (9th Cir. 2009).

Accordingly, the Court GRANTS Facebook's Motion to Dismiss Defendants' counterclaims for violations of Section 2 of the Sherman Act. Since Defendants have already had the opportunity to amend their counterclaims once, the Court dismisses these claims with prejudice.

D. UCL Claim

Facebook moves to dismiss Defendants' UCL claim on the ground that if Facebook's conduct is not anticompetitive under Section 2 of the Sherman Act, a UCL claim cannot be premised on that same conduct. (Facebook's Motion to Dismiss at 8-9.)

The UCL prohibits "any unlawful, unfair or fraudulent business act or practice." Cal. Bus. & Prof. Code § 17200. "The broad scope of the statute encompasses both anticompetitive business practices and practices injurious to consumers. An act or practice may be actionable as 'unfair' under the unfair competition law even if it is not 'unlawful.'" Chavez v. Whirlpool Corp., 93 Cal. App. 4th 363, 375 (Cal. Ct. App. 2001).

In Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tele. Co.,²⁷ the court concluded that an act or practice is “unfair” under the UCL if that conduct “threatens an incipient violation of an antitrust law, or violates the policy or spirit of one of those laws because its effects are comparable to or the same as a violation of the law, or otherwise significantly threatens or harms competition.”

Likewise,

the determination that the conduct is not an unreasonable restraint of trade necessarily implies that the conduct is not “unfair” toward consumers. To permit a separate inquiry into essentially the same question under the unfair competition law would only invite conflict and uncertainty and could lead to the enjoining of procompetitive conduct.

Chavez, 93 Cal. App. 4th at 375.

Here, the Court has found that Facebook’s conduct is not anticompetitive. Thus, Defendants cannot premise their UCL claim on Facebook’s conduct under either the unlawful or the unfair prong. Accordingly, the Court GRANTS Facebook’s Motion to Dismiss as to Defendants’ UCL counterclaim with prejudice.

E. Affirmative Defenses

Facebook moves to strike Defendants’ affirmative defenses of misuse of copyright and fair use. (Facebook’s Motion to Dismiss at 9-11.)

Pursuant to Federal Rule of Civil Procedure 12(f), “the court may order stricken from any pleading any insufficient defense or any redundant, immaterial, impertinent, or scandalous matter.” However, “[m]otions to strike are generally regarded with disfavor because of the limited importance of pleading in federal practice, and because they are often used as a delaying tactic.” Neilson v. Union Bank of Cal., N.A., 290 F. Supp. 2d 1101, 1152 (C.D. Cal. 2003); *see, e.g., Cal. Dep’t of Toxic Substances Control v. Alco Pac., Inc.*, 217 F. Supp. 2d 1028 (C.D. Cal. 2002). Accordingly, such motions should be denied unless the matter has no logical connection to the controversy at issue and may prejudice one or more of the parties to the suit. SEC v. Sands, 902 F. Supp. 1149, 1166 (C.D. Cal. 1995); LeDuc v. Kentucky Central Life Ins. Co., 814 F. Supp. 820, 820 (N.D. Cal. 1992). When considering a motion to strike, the court “must view the pleading in a light

²⁷ 20 Cal. 4th 163, 187 (Cal. Ct. App. 1999).

most favorable to the pleading party.” In re TheMart.com, Inc. Securities Litig., 114 F. Supp. 2d 955, 965 (C.D. Cal. 2000).

Here, the Court previously struck Defendants’ affirmative defenses because they “contain[ed] no factual allegations.” (October 22 Order at 3.) Instead, the pleadings merely referred back to the “Introduction and Background” section with the phrase “conduct, as described herein.” (Id. at 4.) The Court found such barebones pleading inadequate, but gave Defendants leave to amend. In their Amended Answer, Defendants plead in much greater detail their misuse of copyright and fair use affirmative defenses. (Amended Answer ¶¶ 161-68.) The Court finds that Defendants’ amended allegations are sufficient to provide Facebook with “fair notice of the defense.” See Mag Instrument, Inc. v. JS Prods., 595 F. Supp. 1102, 1107 (C.D. Cal. 2008).

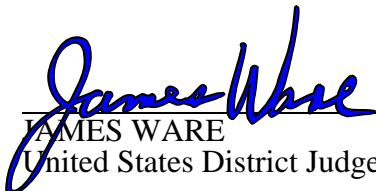
Accordingly, the Court DENIES Facebook’s Motion to Strike Defendants’ Affirmative Defenses.

V. CONCLUSION

The Court DENIES Facebook’s Motion for Judgment on the Pleadings, DENIES the parties’ Cross-Motions for Summary Judgment, GRANTS Facebook’s Motion to Dismiss Defendants’ counterclaims for violations of Section 2 of the Sherman Act with prejudice, GRANTS Facebook’s Motion to Dismiss Defendants’ UCL counterclaim with prejudice, and DENIES Facebook’s Motion to Strike Defendants’ Affirmative Defenses.

On **August 23, 2010 at 10 a.m.**, the parties shall appear for a Further Case Management Conference. On or before **August 13, 2010**, the parties shall file a Joint Case Management Statement. The Statement shall include an update on the parties’ discovery efforts and proposed schedule on how this case should proceed in light of this Order.

Dated: July 20, 2010


JAMES WARE
United States District Judge

THIS IS TO CERTIFY THAT COPIES OF THIS ORDER HAVE BEEN DELIVERED TO:

Alan R Plutzik aplutzik@bramsonplutzik.com
Cindy Ann Cohn cindy@eff.org
David P. Chiappetta david.chiappetta@corrs.com.au
Indra Neel Chatterjee nchatterjee@orrick.com
Jessica Susan Pers jpers@orrick.com
Joseph Perry Cutler JCutler@perkinscoie.com
Julio Cesar Avalos javalos@orrick.com
Lawrence Timothy Fisher ltfisher@bramsonplutzik.com
Scott A. Bursor scott@bursor.com
Thomas J. Gray tgray@orrick.com

Dated: July 20, 2010

Richard W. Wieking, Clerk

By: /s/ JW Chambers

**Elizabeth Garcia
Courtroom Deputy**

3 of 3 DOCUMENTS

Facebook, Inc. v. Power Ventures, Inc.**Case Number C 08-5780 JF (RS)****UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF
CALIFORNIA, SAN JOSE DIVISION***2009 U.S. Dist. LEXIS 42367; 91 U.S.P.Q.2D (BNA) 1430***May 11, 2009, Decided****May 11, 2009, Filed**

SUBSEQUENT HISTORY: Complaint dismissed at, Motion to strike granted by *Facebook, Inc. v. Power Ventures, Inc.*, 2009 U.S. Dist. LEXIS 103662 (N.D. Cal., Oct. 22, 2009)

COUNSEL: [*1] For Facebook, Inc., a Delaware corporation, Plaintiff: David P. Chiappetta, LEAD ATTORNEY, Perkins Coie LLP, Menlo Park, CA; Joseph Perry Cutler, LEAD ATTORNEY, PRO HAC VICE, Perkins Coie, Seattle, WA.

For Power Ventures, Inc., a California corporation, doing business as Power.com, Steven Vachani, an individual, Defendants: Alan R Plutzik, Barroway Topaz Kessler Meltzer & Check LLP, Walnut Creek, CA.

For Power Ventures, Inc., a Cayman Island Corporation, Defendant: Scott A. Bursor, LEAD ATTORNEY, PRO HAC VICE, Law Offices of Scott A. Bursor, New York, NY; Alan R Plutzik, Barroway Topaz Kessler Meltzer & Check LLP, Walnut Creek, CA.

JUDGES: JEREMY FOGEL, United States District Judge.

OPINION BY: JEREMY FOGEL

OPINION

ORDER ¹ (1) DENYING MOTION TO DISMISS AND (2) GRANTING IN PART AND DENYING IN PART MOTION FOR MORE DEFINITE STATEMENT

¹ This disposition is not designated for publication in the official reports.

[re: doc. no. 17]

Plaintiff Facebook, Inc. ("Facebook") alleges that Defendants Power Ventures, Inc. and Power.com (collectively "Power.com") and Steve Vachini ("Vachini") operate an Internet service that collects user information from Facebook's website in violation of the Controlling the Assault of Non-Solicited [*2] Pornography and Marketing ("CAN-SPAM") Act, 15 U.S.C. § 7701, *et seq.*; the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 *et seq.*; and *California Penal Code* § 502. Facebook also alleges that Defendants committed direct and indirect copyright infringement when they made copies of Facebook's website during the process of extracting user information. In addition, Facebook alleges that the means by which Power.com accessed the Facebook website constituted a violation of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201, *et seq.* Facebook also asserts claims for relief based on state and federal trademark law, as well as a claim for relief under California's Unfair Competition Law ("UCL"), *Cal. Bus. & Prof. Code* § 17200, *et seq.*

Defendants initially moved to dismiss the First Amended Complaint ("FAC") in its entirety pursuant to *Fed. R. Civ. P. 12(b)(6)* or in the alternative pursuant to *Fed. R. Civ. P. 12(e)*, but that motion was withdrawn with respect to the CAN-SPAM, CFAA, and § 502 claims in light of Facebook's opposition. Defendants now seek dismissal of Facebook's remaining claims for relief (counts 4 through 8 in the FAC). For the reasons set forth below, the motion [*3] to dismiss for failure to state a claim will be denied, and the motion for a more definite statement will be granted in part and denied in part.

I. BACKGROUND

Facebook developed and operates what is now one of the most popular social networking websites. *See* FAC P 2. The Facebook website allows users to create user profiles, join networks and "friend" other users, which creates online communities with shared interests and connections. *See id.* Every Facebook user must register before using the website, and registration requires the user to assent to Facebook's Terms of Use, which essentially is a user agreement that sets forth the acceptable terms of use. *See id.* Ex. A. Users who agree to the Terms of Use have a limited license to access and use Facebook's website and services. *See id.* P 31 and Ex. A at 3 ("Any use of the Site or the Site Content other than as specifically authorized herein, without the prior written permission of Company, is strictly prohibited and will terminate the license granted herein."). Registered users create and customize their own user profiles by adding content such as personal information, content related to their interests, and photographs, which can then [*4] be shared with other Facebook users with whom the user has a Facebook connection. *Id.* P 22. Facebook users may be contacted only by Facebook or other registered Facebook users. *Id.* P 23. Any unauthorized use of Facebook's website will result in the termination of a user's license. *See id.* P 31.

Facebook also grants third parties a limited license to create applications that interact with Facebook's proprietary network, provided that these applications adhere to a standardized set of protocols and procedures and that the third-party developers agree to Facebook's Developer Terms of Service, the Terms of Use, and any other applicable policies. FAC P 27. In addition, Facebook permits integration with third-party websites, and even permits exchange of proprietary data with third-party websites, provided that these third party websites use the "Facebook Connect" service, which enables users to "connect" their Facebook identity, friends and privacy to those third-party websites. *Id.* P 27. Facebook does not permit third-party access to Facebook user profile data unless such access is through Facebook Connect. *Id.* P 28.

The corporate Defendants are alleged to be California entities and/or organizations [*5] that do business in California. FAC PP 9-10. Defendant Vachini allegedly is the CEO of Defendant Power.com, which is a website designed to integrate various social networking

or email accounts into a single portal *Id.* PP 5, 11, 45. A user has discretion with respect to whether to use Defendants' services, and the user determines which accounts will be aggregated. *See id.* P 50. After a user provides his or her user names and passwords to Defendants, the Power.com service takes this access information to "scrape" user data from those accounts. *Id.* PP 50-52. Subsequently, the user can log on to Power.com to view the data culled from Facebook and any other social networking sites or email accounts. *See id.* at P 52.

Prior to the filing of the FAC, the parties attempted to negotiate an arrangement whereby Power.com could continue to access Facebook's website provided that it did so through the Facebook Connect application. FAC PP 58-61. Those discussions proved fruitless, however, and in late December 2008 Defendants informed Facebook that Power.com would continue to operate without using Facebook Connect. *Id.* P 62. Defendants allegedly continue to scrape Facebook's website, despite technological [*6] security measures to block such access. *Id.* PP 63-64. Defendants also have solicited Facebook users to join Power.com through promotional emails. *Id.* PP 65-66, 70.

II. LEGAL STANDARD

When considering a motion to dismiss, the plaintiff's allegations are taken as true and the Court must construe the complaint in the light most favorable to the plaintiff. *Jenkins v. McKeithen*, 395 U.S. 411, 421, 89 S. Ct. 1843, 23 L. Ed. 2d 404 (1969). For a motion to dismiss for failure to state a claim pursuant to *Fed. R. Civ. P. 12(b)(6)*, "[d]ismissal is appropriate only where the complaint lacks a cognizable legal theory or sufficient facts to support a cognizable legal theory." *Mendiondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008). "While a complaint attacked by a *Rule 12(b)(6)* motion to dismiss does not need detailed factual allegations, a plaintiff's obligation to provide the 'grounds' of his 'entitle[ment] to relief requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 127 S. Ct. 1955, 1964-65, 167 L. Ed. 2d 929 (2007) (citations omitted).

"If a pleading to which a responsive pleading is permitted is so vague or ambiguous that a party [*7] cannot reasonably be required to frame a responsive pleading, the party may move for a more definite

statement before interposing a responsive pleading." *Fed. R. Civ. P. 12(e)*. "Whether to grant a *Rule 12(e)* motion is within the discretion of the trial court." *Babb v. Bridgestone/Firestone*, 861 F. Supp. 50, 52 (M. D. Tenn., 1993). However, "[s]uch motion [is] not favored by the courts since pleadings in federal courts are only required to fairly notify the opposing party of the nature of the claim." *Resolution Trust Corp. V. Dean*, 854 F. Supp. 626, 629 (D. Ariz. 1994) (citing *A.G. Edwards & Sons, Inc. V. Smith*, 736 F. Supp. 1030, 1032 (D. Ariz. 1989)). "[The motion] should not be granted unless the defendant cannot frame a responsive pleading." *Falamore, Inc. V. Edison Bros. Stores, Inc.*, 525 F. Supp. 940 (E.D. Cal. 1981).

III. DISCUSSION

A. Copyright Infringement

To state a claim for copyright infringement, a plaintiff need only allege (1) ownership of a valid copyright and (2) copying of original elements of the work. *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 361, 111 S. Ct. 1282, 113 L. Ed. 2d 358 (1991). The FAC alleges that Defendants accessed the Facebook website and made unauthorized copies of the [*8] website or created derivative works derived from the Facebook website. *See* FAC PP 124-27.

Defendants contend that Facebook's copyright allegations are deficient because it is unclear which portions of the Facebook website are alleged to have been copied. Defendants also argue that there are significant portions of the website that are not protected by copyright because Facebook does not hold any rights to content posted by users. In response, Facebook argues that Defendants make a "cache" copy of the website on each occasion of unauthorized access. Facebook also argues that it need not define the exact contours of the protected material because copyright claims do not require particularized allegations.

The facts as pled in the instant case may be analogized to those in *Ticketmaster L.L.C. v. RMG Techs, Inc.*, 507 F. Supp. 2d 1096 (C.D. Cal. 2007), where in the context of a motion for a preliminary injunction the district court found that the defendant made a copy of Ticketmaster's website each time its automated program accessed the website. *See id. at 1106*. ("copies of webpages stored automatically in a computer's cache or random access memory ("RAM") upon a viewing of the

webpage fall [*9] within the Copyright Act's definition"). *See also MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 519 (9th Cir.1993) ("since we find that the copy created in the RAM can be 'perceived, reproduced, or otherwise communicated,' we hold that the loading of software into the RAM creates a copy under the Copyright Act."). In addition, any users that accessed the Ticketmaster website were bound its terms of use, which prohibited the use of automated programs to access content. *Id. at 1107-10*. Under those circumstances, the court found that Ticketmaster had met its burden of showing a likelihood of success on the merits with respect to its direct copyright infringement claim. *Id. at 1110*.

Facebook's user agreement prohibits, *inter alia*, the "harvest[ing] or collect[ion] [of] email addresses or other contact information of other users from the Service or the Site by electronic or other means for the purpose of sending unsolicited emails or other unsolicited communications." FAC Ex. A at 4. In addition, the user agreement broadly prohibits the downloading, scraping, or distributing of any content on the website, with the exception being that a user may download his or her own user content. [*10] *Id. at 3*. However, not even this exception allows a user to employ "data mining, robots, scraping, or similar data gathering or extraction methods." *Id.* Such actions are explicitly deemed to constitute "unauthorized use." *See id.* Accordingly, the allegations as set forth in the FAC sufficiently allege unauthorized access. Access for purposes that explicitly are prohibited by the terms of use is clearly unauthorized. *See Ticketmaster*, 507 F. Supp. 2d at 1108-1110.

In addition, Facebook need not allege the exact content that Defendants are suspected of copying at this stage of the proceedings. There is no requirement that copyright claims must be pled with particularity. *See Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 167 F. Supp. 2d 1114, 1120 (C.D. Cal. 2001) ("Copyright claims need not be pled with particularity...complaints simply alleging present ownership by plaintiff, registration in compliance with the applicable statute and infringement by defendant have been held sufficient under the rules."). Defendants' argument that Facebook's website is "huge" is irrelevant. According to the FAC, Facebook owns the copyright to any page within its system, including the material located on [*11] those pages besides user content, such as graphics, video and sound files. *See* FAC P 135 and Ex. A at 3. Defendants need only access and copy one page to

commit copyright infringement.

Defendants correctly assert that Facebook does not have a copyright on user content, which ultimately is the information that Defendants' software seeks to extract. However, if Defendants first have to make a copy of a user's entire Facebook profile page in order to collect that user content, such action may violate Facebook's proprietary rights.² Accordingly, the motion to dismiss the claim for direct copyright infringement will be denied.

2 A collection of non-copyrighted material arranged in an original way is subject to copyright protection. *See* 17 U.S.C. § 101; *Harper House, Inc. v. Thomas Nelson, Inc.*, 889 F.2d 197, 204 (9th Cir. 1989). For example, in *Ticketmaster* the factual information about concerts and tickets was not by itself copyrightable, but Ticketmaster's arrangement of that information on its website presumably was. *See id.*

The FAC also sufficiently states a claim for indirect copyright infringement. "One infringes contributorily by intentionally inducing or encouraging direct infringement, [*12] and infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it." *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 930, 125 S. Ct. 2764, 162 L. Ed. 2d 781 (2005) (citations omitted). Viewing the allegations in the FAC as true, the utilization of Power.com by Facebook users exceeds their access rights pursuant to the Terms of Use. *See* FAC Ex. A at 3-4. Moreover, when a Facebook user directs Power.com to access the Facebook website, an unauthorized copy of the user's profile page is created. *See id.* P 125. The creation of that unauthorized copy through the use of Defendants' software may constitute copyright infringement. *See Ticketmaster*, 507 F. Supp. 2d at 1110-11 ("Designing and marketing a device whose purpose is to allow unauthorized access to, and thus to infringe on, a copyrighted website is sufficient to trigger contributory liability for infringement committed by the device's immediate users."). The motion to dismiss the claim for indirect copyright infringement also will be denied.

B. Violation of the DMCA

The elements necessary to state a claim under the DMCA are (1) ownership of a valid copyright; (2)

circumvention of a technological measure [*13] designed to protect the copyrighted material; (3) unauthorized access by third parties; (4) infringement because of the circumvention; and (5) the circumvention was achieved through software that the defendant either (i) designed or produced primarily for circumvention; (ii) made available despite only limited commercial significance other than circumvention; or (iii) marketed for use in circumvention of the controlling technological measure. *See Chamberlain Group, Inc. v. Skylink Techs, Inc.*, 381 F.3d 1178, 1203 (Fed. Cir. 2004). *See also Ticketmaster*, 507 F. Supp. 2d at 1112. As with a copyright infringement claim, there is no heightened pleading requirement that mandates detailed allegations. *Perfect 10*, 167 F. Supp. 2d at 1120.

Defendants argue that Facebook's DMCA claim also is insufficient for essentially the same reasons discussed previously, except that they also argue that the unauthorized use requirement is not met because it is users who are controlling access (via Power.com) to their own content on the Facebook website. However, this argument relies on an assumption that Facebook users are authorized to use Power.com or similar services to access their user accounts. The [*14] Terms of Use negate this argument. Any user is barred from using automated programs to access the Facebook website. *See* FAC Ex. A at 3-4. Users may have the right to access their own content, but conditions have been placed on that access. *See id.* The FAC further alleges that Facebook implemented specific technical measures to block access by Power.com after Defendants informed Facebook that they intended to continue their service without using Facebook Connect, and that Defendants then attempted to circumvent those technological measures. FAC PP 63, 64. Accordingly, the motion to dismiss the DMCA claim will be denied.

C. Trademark Infringement

The Lanham Act imposes liability upon any person who (1) uses an infringing mark in interstate commerce, (2) in connection with the sale or advertising of goods or services, and (3) such use is likely to cause confusion or mislead consumers. 15 U.S.C. § 1114(1)(a). The FAC states that Facebook has been the registered owner of the FACEBOOK mark since 2004. FAC PP 38-39, 146. The FAC further alleges that Defendants use the mark in connection with their business. *See id.* P 70. At no time has Facebook authorized or consented to Defendants' use

of [*15] the mark. *Id.* P 79.

Defendants again argue that the FAC does not provide sufficient detail and that Facebook is required to provide concise information with respect to the trademark infringement allegations, including information about "each instance of such use." However, particularized pleading is not required for a trademark infringement claim. *See Perfect 10, 167 F. Supp. 2d at 1122*. The FAC incorporates a screenshot of an email sent by Defendants to Facebook users that not only incorporates the protected mark but also appears to have been originated from or been endorsed by Facebook. *See* FAC P 70. The FAC also states that Defendants' unauthorized use of the Facebook mark was likely to "confuse recipients and lead to the false impression that Facebook is affiliated with, endorses, or sponsors" Defendants' services and the Power.com website. *Id.* PP 73, 76, 78. These allegations are sufficient to state a claim for trademark infringement. *See Perfect 10, 167 F. Supp. 2d at 1122* ("Perfect 10's allegations concerning the scope of the alleged violations and Cybernet's alleged role, Cybernet is put on notice of the claims' nature and has enough information to draft its pleadings.").

"To [*16] state a claim of trademark infringement under California common law, a plaintiff need allege only 1) their prior use of the trademark and 2) the likelihood of the infringing mark being confused with their mark." *Wood v. Apodaca, 375 F. Supp. 2d 942, 947-48 (N.D. Cal. 2005)*. For the same reasons set forth above, the motion to dismiss the common law trademark claim will be denied.

D. UCL Claim

The Ninth Circuit "has consistently held that state common law claims of unfair competition and actions pursuant to *California Business and Professions Code* § 17200 are 'substantially congruent' to claims made under the Lanham Act." *Cleary v. News Corp., 30 F.3d 1255, 1263-64 (9th Cir. 1995)*. *See also Jackson v. Sturkie, 255 F. Supp. 2d 1096, 1107 (N.D. Cal. 2003)* (adequately pled Lanham Act claim meant that UCL claim also was

pled sufficiently). Facebook's UCL claim does not reference the alleged trademark violations specifically, but it does incorporate all the prior allegations in the pleading by reference. *See* FAC P 157. Otherwise, the UCL count merely alleges that Defendants have engaged in "unlawful, unfair, and/or fraudulent business acts or practices" in violation of the UCL. Accordingly, [*17] from the face of the FAC it is unclear whether Facebook's UCL claim is based on its trade dress allegations alone or whether other portions of the FAC, such as the CFAA or CAN-SPAM claims, are intended to form separate and independent bases for the UCL claim. Accordingly, the Court will grant Defendants' motion for a more definite statement pursuant to *Rule 12(e)* with respect to the UCL claim. *See Anderson v. Dist. Bd. of Trustees of Cent. Fl. Comm. Coll., 77 F.3d 364, 367(11th Cir. 1996)* ("Experience teaches that, unless cases are pled clearly and precisely, issues are not joined, discovery is not controlled, the trial court's docket becomes unmanageable, the litigants suffer, and society loses confidence in the court's ability to administer justice."). Within thirty (30) days of the date of this order, Facebook shall file a short statement clarifying the ground(s) underlying its UCL claim.

IV. ORDER

Good cause therefor appearing, IT IS HEREBY ORDERED that the motion to dismiss is DENIED and the motion for a more definite statement is GRANTED IN PART and DENIED IN PART. Defendants shall file an answer to the FAC within thirty (30) days of the date that Facebook files its supplemental [*18] statement.

IT IS SO ORDERED.

DATED: May 11, 2009

/s/ Jeremy Fogel

JEREMY FOGEL

United States District Judge

LEXSTAT 18 U.S.C. § 1030

UNITED STATES CODE SERVICE
Copyright © 2010 Matthew Bender & Company, Inc.
a member of the LexisNexis Group (TM)
All rights reserved.

*** CURRENT THROUGH PL 111-237, APPROVED 8/16/2010 ***

TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART I. CRIMES
CHAPTER 47. FRAUD AND FALSE STATEMENTS

Go to the United States Code Service Archive Directory

18 USCS § 1030

§ 1030. Fraud and related activity in connection with computers

(a) Whoever--

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y.[(y)] of section 11 of the Atomic Energy Act of 1954 [42 USCS § 2014(y)], with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$ 5,000 in any 1-year period;

(5) (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.[:]

(6) knowingly and with intent to defraud traffics (as defined in section 1029 [18 USCS § 1029]) in any password or similar information through which a computer may be accessed without authorization, if--

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States; [or]

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any--

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

(b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is--

(1)

(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section; or an attempt to commit an offense punishable under this subparagraph;

(2) (A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if--

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds \$ 5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)

(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this section;

(4) (A) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of--

(i) an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)--

(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$ 5,000 in value;

(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III) physical injury to any person;

(IV) a threat to public health or safety;

(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

(VI) damage affecting 10 or more protected computers during any 1-year period; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(B) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of--

(i) an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or

(ii) an attempt to commit an offense punishable under this subparagraph;

(C) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of--

(i) an offense or an attempt to commit an offense under subparagraphs (A) or (B) of subsection (a)(5) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(D) a fine under this title, imprisonment for not more than 10 years, or both, in the case of--

(i) an offense or an attempt to commit an offense under subsection (a)(5)(C) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(E) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;

(F) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or

(G) a fine under this title, imprisonment for not more than 1 year, or both, for--

(i) any other offense under subsection (a)(5); or

(ii) an attempt to commit an offense punishable under this subparagraph.

(5) [Deleted]

(d)

(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (*42 U.S.C. 2014(y)*)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this *title* [*18 USCS § 3056(a)*].

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section--

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated

typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer--

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means--

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934 [*15 USCS § 78o*];

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978 [*12 USCS § 3101(1)* and (3)]); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive department enumerated in section 101 of title 5;

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or

(V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection [enacted Sept. 13, 1994], concerning investigations and prosecutions under subsection (a)(5).

(i) (1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States--

(A) such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and

(B) any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j) For purposes of subsection (i), the following shall be subject to forfeiture to the United States and no property right shall exist in them:

(1) Any personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.

(2) Any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate this section.

HISTORY:

(Added Oct. 12, 1984, P.L. 98-473, Title II, Ch XXI, § 2102(a), 98 Stat. 2190; Oct. 16, 1986, P.L. 99-474, § 2, 100 Stat. 1213; Nov. 18, 1988, P.L. 100-690, Title VII, Subtitle B, § 7065, 102 Stat. 4404; Aug. 9, 1989, P.L. 101-73, Title IX, Subtitle F, § 962(a)(5), 103 Stat. 502; Nov. 29, 1990, P.L. 101-647, Title XII, § 1205(e), Title XXV, Subtitle I, § 2597(j), Title XXXV, § 3533, 104 Stat. 4831, 4910, 4925; Sept. 13, 1994, P.L. 103-322, Title XXIX, § 290001(b)-(f), 108 Stat. 2097; Oct. 11, 1996, P.L. 104-294, Title II, § 201, Title VI, § 604(b)(36), 110 Stat. 3491, 3508; Oct. 26, 2001, P.L. 107-56, Title V, § 506(a), Title VIII, § 814(a)-(e), 115 Stat. 366, 382; Nov. 2, 2002, P.L. 107-273, Div B, Title IV, §§ 4002(b)(1), (12), 4005(a)(3), (d)(3), 116 Stat. 1807, 1808, 1812, 1813; Nov. 25, 2002, P.L. 107-296, Title II, Subtitle C, § 225(g), 116 Stat. 2158.)

(As amended Sept. 26, 2008, P.L. 110-326, Title II, §§ 203, 204(a), 205-208, 122 Stat. 3561.)

HISTORY; ANCILLARY LAWS AND DIRECTIVES

References in text:

The "Farm Credit Act of 1971", referred to in subsec. (e)(4)(E), is Act Dec. 10, 1971, P.L. 92-181, 85 Stat. 583, which appears generally as 12 USCS §§ 2001 et seq. For full classification of such Act, consult USCS Tables volumes.

"Section 25 of the Federal Reserve Act", referred to in subsec. (e)(4)(I), is § 25 of Act Dec. 23, 1913, ch 6, 38 Stat. 273, which appears generally as 12 USCS §§ 601 et seq. For full classification of this section, consult USCS Tables volumes.

"Section 25(a) of the Federal Reserve Act", referred to in subsec. (e)(4)(I), was redesignated as § 25A of Act Dec. 23, 1913, ch 6, 38 Stat. 273, by Act Dec. 19, 1991, P.L. 102-242, Title I, § 142(e)(2), 105 Stat. 2281, and appears generally

LEXSEE 259 F.R.D. 449

United States v. Drew**No. CR 08-0582-GW****UNITED STATES DISTRICT COURT FOR THE CENTRAL DISTRICT OF
CALIFORNIA***259 F.R.D. 449; 2009 U.S. Dist. LEXIS 85780***August 28, 2009, Decided****August 28, 2009, Filed**

COUNSEL: [*1] For Lori Drew, Defendant (1): H Dean Steward, LEAD ATTORNEY, H Dean Steward Law Offices, San Clemente, CA; Orin S Kerr, LEAD ATTORNEY, PRO HAC VICE, Orin S Kerr Law Offices, Washington, DC.

For Electronic Frontier Foundation, et al, Amicus: Jennifer Stisa Granick, LEAD ATTORNEY, Stanford Law School, Stanford, CA.

For USA, Plaintiff: Mark Krause, LEAD ATTORNEY, AUSA - Office of US Attorney, Criminal Div - US Courthouse, Los Angeles, CA; Yvonne Leticia Garcia, LEAD ATTORNEY, AUSA - US Attorney's Office, Los Angeles, CA.

JUDGES: GEORGE H. WU, United States District Judge.

OPINION BY: GEORGE H. WU

OPINION

[*451] DECISION ON DEFENDANT'S
F.R.CRIM.P. 29(c) MOTION

I. INTRODUCTION

This case raises the issue of whether (and/or when will) violations of an Internet website's¹ terms of service constitute a crime under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. Originally, the question arose in the context of Defendant Lori Drew's motions to dismiss the Indictment on grounds of vagueness, failure

to state an offense, and unconstitutional delegation of prosecutorial power. See Case Docket Document Numbers ("Doc. Nos.") 21, 22, and 23. At that time, this Court found that the presence of the scienter element (i.e. the requirement [*2] that the intentional accessing of a computer without authorization or in excess of authorization be in furtherance of the commission of a criminal or tortious act) within the CFAA felony provision as delineated in 18 U.S.C. § 1030(c)(2)(B)(ii) overcame Defendant's constitutional challenges and arguments against the criminalization of breaches of contract involving the use of computers. See Reporter's Transcripts of Hearings on September 4 and October 30, 2008. However, Drew was subsequently acquitted by a jury of the felony CFAA counts but convicted of misdemeanor CFAA violations. Hence, the question in the present motion under Federal Rule of Criminal Procedure ("*F.R.Crim.P.*") 29(c) is whether an intentional breach of an Internet website's terms of service, without more, is sufficient to constitute a misdemeanor violation of the CFAA; and, if so, would the statute, as so interpreted, survive constitutional challenges on the grounds of vagueness and related doctrines.²

¹ There is some disagreement as to whether the words "Internet" and "website" should be capitalized and whether the latter should be two words (i.e. "web site") or one. "Internet" is capitalized as that is how the word [*3] appears most often in Supreme Court opinions. See, e.g., *Pac. Bell Tel. Co. v. linkLine Communs., Inc.*, 555 U.S. ___, 129 S. Ct. 1109, 1115, 172 L. Ed. 2d 836 (2009).

² While this case has been characterized as a

prosecution based upon purported "cyberbullying," there is nothing in the legislative history of the CFAA which suggests that Congress ever envisioned such an application of the statute. See generally, A. Hugh Scott & Kathleen Shields, *Computer and Intellectual Property Crime: Federal and State Law* (2006 Cumulative Supplement) 4-8 to 4-16 (BNA Books 2006). As observed in Charles Doyle & Alyssa Weir, *CRS Report for Congress - Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws* (Order Code 97-1025) (Updated June 28, 2005):

The federal computer fraud and abuse statute, 18 U.S.C. 1030, protects computers in which there is a federal interest -- federal computers, bank computers, and computers used in interstate and foreign commerce. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. It is not a comprehensive provision, instead it fills cracks and gaps in the protection afforded by [**4] other state and federal criminal laws.

Moreover, once Drew was acquitted by the jury of unauthorized accessing of a protected computer in furtherance of the commission of acts of intentional infliction of emotional distress, this case was no longer about "cyberbullying" (if, indeed, it was ever properly characterized as such); but, rather, it concerned the proper scope of the application of the CFAA in the context of violations of a website's terms of service.

[*452] II. BACKGROUND

A. Indictment

In the Indictment, Drew was charged with one count of conspiracy in violation of 18 U.S.C. § 371 and three counts of violating a felony portion of the CFAA, i.e., 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii), which prohibit accessing a computer without authorization or in

excess of authorization and obtaining information from a protected computer where the conduct involves an interstate or foreign communication and the offense is committed in furtherance of a crime or tortious act. See Doc. No. 1.

The Indictment included, inter alia, the following allegations (not all of which were established by the evidence at trial). Drew, a resident of O'Fallon, Missouri, entered into a conspiracy in which its members [**5] agreed to intentionally access a computer used in interstate commerce without (and/or in excess of) authorization in order to obtain information for the purpose of committing the tortious act of intentional infliction of emotional distress³ upon "M.T.M.," subsequently identified as Megan Meier ("Megan"). Megan was a 13 year old girl living in O'Fallon who had been a classmate of Drew's daughter Sarah. Id. at PP 1-2, 14. Pursuant to the conspiracy, on or about September 20, 2006, the conspirators registered and set up a profile for a fictitious 16 year old male juvenile named "Josh Evans" on the www.MySpace.com website ("MySpace"), and posted a photograph of a boy without that boy's knowledge or consent. Id. at P 16. Such conduct violated MySpace's terms of service. The conspirators contacted Megan through the MySpace network (on which she had her own profile) using the Josh Evans pseudonym and began to flirt with her over a number of days. Id. On or about October 7, 2006, the conspirators had "Josh" inform Megan that he was moving away. Id. On or about October 16, 2006, the conspirators had "Josh" tell Megan that he no longer liked her and that "the world would be a better place without [**6] her in it." Id. Later on that same day, after learning that Megan had killed herself, Drew caused the Josh Evans MySpace account to be deleted. Id.

3 The elements of the tort of intentional infliction of emotional distress are the same under both Missouri and California state laws. Those elements are: (1) the defendant must act intentionally or recklessly; (2) the defendant's conduct must be extreme or outrageous; and (3) the conduct must be the cause (4) of extreme emotional distress. See, e.g., *Thomas v. Special Olympics Missouri, Inc.*, 31 S.W.3d 442, 446 (Mo. Ct. App. 2000); *Hailey v. California Physicians' Service*, 158 Cal.App.4th 452, 473-74, 69 Cal. Rptr. 3d 789 (2007).

B. Verdict

At the trial, after consultation between counsel and the Court, the jury was instructed that, if they unanimously decided that they were not convinced beyond a reasonable doubt as to the Defendant's guilt as to the felony CFAA violations of 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii), they could then consider whether the Defendant was guilty of the "lesser included" ⁴ misdemeanor [*453] CFAA violation of 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A). ⁵

4 As provided in *F.R.Crim.P. 31(c)(1)*, a "defendant may be found guilty of . . . [*7] . an offense necessarily included in the offense charged" A "lesser included" crime is one where "the elements of the lesser offense are a subset of the elements of the charged offense." *Carter v. United States*, 530 U.S. 255, 260, 120 S. Ct. 2159, 147 L. Ed. 2d 203 (2000) (quoting *Schmuck v. United States*, 489 U.S. 705, 716, 109 S. Ct. 1443, 103 L. Ed. 2d 734 (1989)). Because the felony CFAA crime in 18 U.S.C. § 1030(c)(2)(B)(ii) consists of committing acts which constitute a violation of the misdemeanor CFAA crime in 18 U.S.C. § 1030(a)(2)(C) (as delineated in 18 U.S.C. § 1030(c)(2)(A)) plus the additional element that the acts were done "in furtherance of any crime or tortious act in violation of the Constitution or laws of the United States or any State," the misdemeanor CFAA crime is a "lesser included" offense as to the felony CFAA violation.

A defendant is entitled to a "lesser included" offense jury instruction if the evidence warrants it. *Guam v. Fejeran*, 687 F.2d 302, 305 (9th Cir. 1982).

5 Specifically, the jury was instructed that:

The crime of accessing a protected computer without authorization or in excess of authorization to obtain information, and to do so in furtherance of a tortious act in violation of the laws of any State, includes [*8] the lesser crime of accessing a protected computer without authorization or in excess

of authorization. If (1) all of you are not convinced beyond a reasonable doubt that the defendant is guilty of accessing a protected computer without authorization or in excess of authorization to obtain information, and doing so in furtherance of a tortious act in violation of the laws of any State; and (2) all of you are convinced beyond a reasonable doubt that the defendant is guilty of the lesser crime of accessing a protected computer without authorization or in excess of authorization, you may find the defendant guilty of accessing a protected computer without authorization or in excess of authorization.

See Jury Instruction No. 24, Doc. No. 107.

At the end of the trial, the jury was deadlocked and was unable to reach a verdict as to the Count 1 conspiracy charge. ⁶ See Doc. Nos. 105 and 120. As to Counts 2 through 4, the jury unanimously found the Defendant "not guilty" "of [on the dates specified in the Indictment] accessing a computer involved in interstate or foreign communication without authorization or in excess of authorization to obtain information in furtherance of the tort of intentional [*9] infliction of emotional distress in violation of Title 18, *United States Code*, Section 1030(a)(2)(C) and (c)(2)(B)(ii)" Id. The jury did find Defendant "guilty" "of [on the dates specified in the Indictment] accessing a computer involved in interstate or foreign communication without authorization or in excess of authorization to obtain information in violation of Title 18, *United States Code*, Section 1030(a)(2)(C) and (c)(2)(A), a misdemeanor." Id.

6 The conspiracy count was subsequently dismissed without prejudice at the request of the Government.

C. MySpace.com

As Jae Sung (Vice President of Customer Care at MySpace) ("Sung") testified at trial, MySpace is a "social networking" website where members can create "profiles" and interact with other members. See Reporter's Transcript of the November 21, 2008 Sung

testimony ("11/21/08 Transcript") at pages 40-41. Anyone with Internet access can go onto the MySpace website and view content which is open to the general public such as a music area, video section, and members' profiles which are not set as "private." Id. at 42. However, to create a profile, upload and display photographs, communicate with persons on the site, write "blogs," [**10] and/or utilize other services or applications on the MySpace website, one must be a "member." Id. at 42-43. Anyone can become a member of MySpace at no charge so long as they meet a minimum age requirement and register. Id.

In 2006, to become a member, one had to go to the sign-up section of the MySpace website and register by filling in personal information (such as name, email address, date of birth, country/state/postal code, and gender) and creating a password. Id. at 44-45. In addition, the individual had to check on the box indicating that "You agree to the MySpace **Terms of Service** and **Privacy Policy**." See Government's ⁷ Exhibit 1 at page 2 (emphasis in original); 11/21/08 Transcript at 45-47. The terms of service did not appear on the same registration page that contained this "check box" for users to confirm their agreement to those provisions. Id. In order to find the terms of service, one had (or would have had) to proceed to the bottom of the page where there were several "hyperlinks" including one entitled "Terms." 11/21/08 Transcript at 50; Exhibit 1 at 5. Upon clicking the "Terms" hyperlink, the screen would display the terms of service section of the website. Id. A person [**11] could become a MySpace member without ever reading or otherwise becoming aware of the provisions and conditions of the MySpace terms of service by merely clicking on the "check box" and then the "Sign Up" button without first accessing the "Terms" section. 11/21/08 Transcript at 94. ⁸

⁷ All exhibits referenced herein were proffered by the Government and admitted during the trial.

⁸ Certain websites endeavor to compel visitors to read their terms of service by requiring them to scroll down through such terms before being allowed to click on the sign-on box or by placing the box at the end of the "terms" section of the site. Id. at 93. MySpace did not have such provisions in 2006. Id. See generally *Southwest Airlines, Co. v. BoardFirst, L.L.C.*, 2007 U.S. Dist. LEXIS 96230 at *13-16 & n.4 (N.D. Tex. 2007) (discussing various methods that websites

employ to notify users of terms of service).

[*454] As used in its website, "terms of service" refers to the "MySpace.com Terms of Use Agreement" ("MSTOS"). See Government's Exhibit 3. The MSTOS in 2006 stated, inter alia:

This Terms of Use Agreement ("Agreement") sets forth the legally binding terms for your use of the Services. By using the Services, you [**12] agree to be bound by this Agreement, whether you are a "Visitor" (which means that you simply browse the Website) or you are a "Member" (which means that you have registered with Myspace.com). The term "User" refers to a Visitor or a Member. You are only authorized to use the Services (regardless of whether your access or use is intended) if you agree to abide by all applicable laws and to this Agreement. Please read this Agreement carefully and save it. If you do not agree with it, you should leave the Website and discontinue use of the Services immediately. If you wish to become a Member, communicate with other Members and make use of the Services, you must read this Agreement and indicate your acceptance at the end of this document before proceeding.

Id. at 1.

By using the Services, you represent and warrant that (a) all registration information you submit is truthful and accurate; (b) you will maintain the accuracy of such information; (c) you are 14 years of age or older; and (d) your use of the Services does not violate any applicable law or regulation.

Id. at 2.

The MSTOS prohibited the posting of a wide range of content on the website including (but not limited to) material that: [**13] a) "is potentially offensive and promotes racism, bigotry, hatred or physical harm of any kind against any group or individual"; b) "harasses or advocates harassment of another person"; c) "solicits

personal information from anyone under 18"; d) "provides information that you know is false or misleading or promotes illegal activities or conduct that is abusive, threatening, obscene, defamatory or libelous"; e) "includes a photograph of another person that you have posted without that person's consent"; f) "involves commercial activities and/or sales without our prior written consent"; g) "contains restricted or password only access pages or hidden pages or images"; or h) "provides any phone numbers, street addresses, last names, URLs or email addresses" Id. at 4. MySpace also reserved the right to take appropriate legal action (including reporting the violating conduct to law enforcement authorities) against persons who engaged in "prohibited activity" which was defined as including, inter alia: a) "criminal or tortious activity", b) "attempting to impersonate another Member or person", c) "using any information obtained from the Services in order to harass, abuse, or harm [**14] another person", d) "using the Service in a manner inconsistent with any and all applicable laws and regulations", e) "advertising to, or solicitation of, any Member to buy or sell any products or services through the Services", f) "selling or otherwise transferring your profile", or g) "covering or obscuring the banner advertisements on your personal profile page" Id. at 5. The MSTOS warned users that "information provided by other MySpace.com Members (for instance, in their Profile) may contain inaccurate, inappropriate, offensive or sexually explicit material, products or services, and MySpace.com assumes no responsibility or liability for this material." Id. at 1-2. Further, MySpace was allowed to unilaterally modify the terms of service, with such modifications taking effect upon the posting of notice on its website. Id. at 1. Thus, members would have to review the MSTOS each time they logged on to the website, to ensure that they were aware of any updates in order to avoid violating some new provision of the terms of service. Also, the MSTOS provided that "any dispute" between a visitor/member and MySpace "arising out of this Agreement must be settled by arbitration" [**15] if demanded by either party. Id. at 7.

At one point, MySpace was receiving an estimated 230,000 new accounts per day and eventually the number of profiles exceeded 400 million with over 100 million unique visitors [*455] worldwide. 11/21/08 Transcript at 74-75. "Generally speaking," MySpace would not monitor new accounts to determine if they complied with the terms of service except on a limited basis, mostly in regards to photographic content. Id. at 75. Sung testified

that there is no way to determine how many of the 400 million existing MySpace accounts were created in a way that violated the MSTOS. ⁹ Id. at 82-84. The MySpace website did have hyperlinks labelled "Safety Tips" (which contained advice regarding personal, private and financial security vis-a-vis the site) and "Report Abuse" (which allowed users to notify MySpace as to inappropriate content and/or behavior on the site). Id. at 51-52. MySpace attempts to maintain adherence to its terms of service. Id. at 60. It has different teams working in various areas such as "parent care" (responding to parents' questions about this site), handling "harassment/cyberbully cases, imposter profiles," removing inappropriate content, searching [**16] for underage users, etc. Id. at 60-61. As to MySpace's response to reports of harassment:

It varies depending on the situation and what's being reported. It can range from . . . letting the user know that if they feel threatened to contact law enforcement, to us removing the profile, and in rare circumstances we would actually contact law enforcement ourselves.

Id. at 61.

9 As stated in the MSTOS:

MySpace.com does not endorse and has no control over the Content. Content is not necessarily reviewed by MySpace.com prior to posting and does not necessarily reflect the opinions or policies of MySpace.com. MySpace.com makes no warranties, express or implied, as to the Content or to the accuracy and reliability of the Content or any material or information that you transmit to other Members.

Exhibit 3 at 3.

Once a member is registered and creates his or her profile, the data is housed on computer servers which are located in Los Angeles County. Id. at 53. Members can create messages which can be sent to other MySpace members, but messages cannot be sent to or from other

Internet service providers such as Yahoo!. Id. at 54. All communications among MySpace members are routed from the sender's computer [**17] through the MySpace servers in Los Angeles. Id. at 54-55.

Profiles created by adult MySpace members are by default available to any user who accesses the MySpace website. Id. at 56. The adult members can, however, place privacy settings on their accounts such that only pre-authorized "friends" are able to view the members' profile pages and contents. Id. For members over 16 but under 18, their profiles are by default set at "private" but can be changed by the member. Id. at 57. Members under 16 have a privacy setting for their profiles which cannot be altered to allow regular public access. Id. To communicate with a member whose profile has a privacy setting, one must initially send a "friend" request to that person who would have to accept the request. Id. at 57-58. To become a "friend" of a person under 16, one must not only send a "friend" request but must also know his or her email address or last name. Id. at 58.

According to Sung, MySpace owns the data contained in the profiles and the other content on the website.¹⁰ MySpace is owned by Fox Interactive Media which is part of News Corporation. Id. at 42.

10 Technically, as delineated in the MSTOS, Exhibit 3 at pages 2-3:

By displaying [**18] or publishing ("posting") any Content, messages, text, files, images, photos, video, sounds, profiles, works or authorship, or any other materials (collectively, "Content") on or through the Services, you hereby grant to MySpace.com, a non-exclusive, fully-paid and royalty-free, worldwide license (with the right to sublicense through unlimited levels of sublicensees) to use, copy, modify, adapt, translate, publicly perform, publicly display, store, reproduce, transmit, and distribute such Content on and through the Services. This license will terminate at the time you remove such Content from the

Services. Notwithstanding the foregoing, a back-up or residual copy of the Content posted by you may remain on the MySpace.com servers after you have removed the Content from the Services, and MySpace.com retains the rights to those copies.

III. APPLICABLE LAW

A. *F.R.Crim.P. 29(c)*

A motion for judgment of acquittal under *F.R.Crim.P. 29(c)* may be made by a [*456] defendant seeking to challenge a conviction on the basis of the sufficiency of the evidence, see, e.g., *United States v. Freter*, 31 F.3d 783, 785 (9th Cir. 1994), or on other grounds including ones involving issues of law for the court to decide, [**19] see, e.g. *United States v. Pardue*, 983 F.2d 843, 847 (8th Cir. 1993) (issue as to whether a defendant is entitled to a judgment of acquittal based on outrageous government conduct is "one of law for the court"). Where the *Rule 29(c)* motion rests in whole or in part on the sufficiency of the evidence, the evidence must be viewed "in the light most favorable to the government" (see *Freter*, 31 F.3d at 785), with circumstantial evidence and inferences drawn in support of the jury's verdict. See *United States v. Lewis*, 787 F.2d 1318, 1323 (9th Cir. 1986).

B. The CFAA

In 2006, the CFAA (18 U.S.C. § 1030) provided in relevant part that:

(a) Whoever --

* * * *

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains --

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in *section 1602(n)* of title 15, or contained in a file of a consumer reporting agency on a

consumer, as such terms are defined in the Fair Credit Reporting Act (*15 U.S.C. 1681 et seq.*);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an [**20] interstate or foreign communication;¹¹

* * * *

shall be punished as provided in subsection (c) of this section.

* * * *

(c) The punishment for an offense under subsection (a) or (b) of this section is --

* * * *

(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; . . .

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if --

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds \$ 5,000

11 On September 26, 2008, the Identity Theft Enforcement and Restitution Act of 2008 was [**21] passed which amended *18 U.S.C. § 1030(a)(2)(C)* by inter alia striking the words "if the conduct involved an interstate or foreign communication" after "protected computer." See 110 P.L. 326, Title II, § 203, 112 Stat. 3560-65.

As used in the CFAA, the term "computer" "includes any data storage facility or communication facility directly related to or operating in conjunction with such device" *18 U.S.C. § 1030(e)(1)*. The term "protected computer" "means a computer - (A) exclusively for the use of a financial institution or the United States Government . . . ; or (B) which is used in interstate or foreign commerce or communication" *Id. § 1030(e)(2)*. The term "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter" *Id. § 1030(e)(6)*.

In addition to providing criminal penalties for computer fraud and abuse, the CFAA also states that "[A]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other [**22] equitable relief." *18 U.S.C. § 1030(g)*. Because of the availability of civil remedies, much of the law as to the meaning and scope of the [*457] CFAA has been developed in the context of civil cases.

IV. DISCUSSION

A. The Misdemeanor *18 U.S.C. § 1030(a)(2)(C)* Crime Based on Violation of a Website's Terms of Service

During the relevant time period herein,¹² the misdemeanor *18 U.S.C. § 1030(a)(2)(C)* crime consisted of the following three elements:

First, the defendant intentionally
[accessed without authorization]
[exceeded authorized access of] a

computer;

Second, the defendant's access of the computer involved an interstate or foreign communication; and

Third, by [accessing without authorization] [exceeding authorized access to] a computer, the defendant obtained information from a computer . . . [used in interstate or foreign commerce or communication] . . .

Ninth Circuit Model Criminal Jury Instruction 8.79 (2003 Ed.) (brackets in original).

12 See footnote 11, *supra*.

In this case, a central question is whether a computer user's intentional violation of one or more provisions in an Internet website's terms of services (where those terms condition access to and/or use of the website's services [**23] upon agreement to and compliance with the terms) satisfies the first element of *section 1030(a)(2)(C)*. If the answer to that question is "yes," then seemingly, any and every conscious violation of that website's terms of service will constitute a CFAA misdemeanor.

Initially, it is noted that the latter two elements of the *section 1030(a)(2)(C)* crime will always be met when an individual using a computer contacts or communicates with an Internet website. Addressing them in reverse order, the third element requires "obtain[ing] information" from a "protected computer" - which is defined in *18 U.S.C. § 1030(e)(2)(B)* as a computer "which is used in interstate or foreign commerce or communication" "Obtain[ing] information from a computer" has been described as "'includ[ing] mere observation of the data. Actual aspiration . . . need not be proved in order to establish a violation" S.Rep. No. 99-432, at 6-7 (1986), reprinted at 1986 U.S.C.C.A.N. 2479, 2484." Comment, Ninth Circuit Model Criminal Instructions 8.77. ¹³ As for the "interstate or foreign commerce or communication" component, the Supreme Court in *Reno v. American Civil Liberties Union*, 521 U.S. 844, 849, 117 S. Ct. 2329, 138 L. Ed. 2d 874 (1997), [**24] observed that: "The Internet is an international network of interconnected computers." See also *Brookfield Communications v. West Coast Entertainment Corp.*, 174 F.3d 1036, 1044 (9th Cir. 1999) ("The Internet is a global network of interconnected computers

which allows individuals and organizations around the world to communicate and to share information with one another."). The Ninth Circuit in *United States v. Sutcliffe*, 505 F.3d 944, 952 (9th Cir. 2007), found the Internet to be "similar to - and often using - our national network of telephone lines." It went on to conclude that:

We have previously agreed that "[i]t can not be questioned that the nation's vast network of telephone lines constitutes interstate commerce," *United States v. Holder*, 302 F.Supp. 296, 298 (D. Mont. 1969)), *aff'd* and adopted, 427 F.2d 715 (9th Cir. 1970) (per curiam), and, a fortiori, it seems clear that use of the internet is intimately related to interstate commerce. As we have noted, "[t]he Internet engenders a medium of communication that enables information to be quickly, conveniently, and inexpensively disseminated to hundreds of millions of individuals worldwide." *United States v. Pirello*, 255 F.3d 728, 729 (9th Cir. 2001). [**25] It is "comparable . . . to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services," *ACLU*, 521 U.S. at 853, and is "a valuable tool in today's commerce," *Pirello*, 255 F.3d at 730. We are therefore in agreement with the Eighth Circuit's conclusion that "[a]s both [*458] the means to engage in commerce and the method by which transactions occur, 'the Internet is an instrumentality and channel of interstate commerce.'" *United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007) (per curiam) (quoting *United States v. MacEwan*, 445 F.3d 237, 245 (3d Cir. 2006)).

Id. at 952-53. Thus, the third element is satisfied whenever a person using a computer contacts an Internet website and reads any response from that site.

13 As also stated in Senate Report No. 104-357, at 7 (1996), reprinted at 1996 WL 492169 (henceforth "S. Rep. No. 104-357"), ". . . the term 'obtaining information' includes merely reading it."

As to the second element (i.e., that the accessing of the computer involve an interstate or foreign communication),¹⁴ an initial question arises as to whether the communication itself must be interstate or foreign (i.e., [**26] it is transmitted across state lines or country borders) or whether it simply requires that the computer system, which is accessed for purposes of the communication, is interstate or foreign in nature (for example, akin to a national telephone system).¹⁵ The term "interstate or foreign communication" is not defined in the CFAA. However, as observed in *Patrick Patterson Custom Homes, Inc. v. Bach*, 586 F.Supp.2d 1026, 1033 (N.D. Ill. 2008), "[t]he plain language of section 1030(a)(2)(C) requires that the conduct of unlawfully accessing a computer, and not the obtained information, must involve an interstate or foreign communication." See also *Charles Schwab & Co. Inc. v. Carter*, 2005 U.S. Dist. LEXIS 21348 at *26 (N.D. Ill. 2005). It has been held that "[a]s a practical matter, a computer providing a 'web-based' application accessible through the internet would satisfy the 'interstate communication' requirement." *Paradigm Alliance, Inc. v. Celeritas Technologies, LLC*, 248 F.R.D. 598, 602 (D. Kan. 2008); see also *Patrick Patterson Custom Homes*, 586 F.Supp.2d at 1033-34; *Modis, Inc. v. Bardelli*, 531 F.Supp.2d 314, 318-19 (D. Conn. 2008); *Charles Schwab & Co.*, 2005 U.S. Dist. LEXIS 21348 at *26-27. [**27] This interpretation is consistent with the legislative history of the CFAA.¹⁶ Therefore, where contact is made between an individual's computer and an Internet website, the second element is per se established.

14 It is noted that, with the 2008 amendment to section 1030(a)(2)(C) which struck the provision that "the conduct involved an interstate or foreign communication" (see footnote 11, supra), the second element is no longer a requirement for the CFAA 18 U.S.C. § 1030(a)(2)(C) crime, although the interstate/foreign nexus remains as part of the third element.

15 A resolution of that question would not effect Defendant's conviction here since the undisputed evidence at trial is that MySpace's server is connected to the Internet and the communications made by the alleged conspirators in O'Fallon, Missouri to Megan would automatically be routed to MySpace's server in Beverly Hills, California where it would be stored and thereafter sent to or retrieved by Megan in O'Fallon.

16 For example, as stated in S. Rep. No.

104-357, at 13:

The bill would amend *subsection 1030(e)(2)* by replacing the term "Federal interest computer" with the new term "protected computer" and a new definition . . . [**28] The new definition also replaces the current limitation in *subsection 1030(e)(2)(B)* of "Federal interest computer" being "one of two or more computers used in committing the offense, not all of which are located in the same State." Instead, "protected computer" would include computers "used in interstate or foreign commerce or communications." Thus, hackers who steal information or computer usage from computers in their own State would be subject to this law, under amended *section 1030(a)(4)*, if the requisite damage threshold is met and the computer is used in interstate commerce or foreign commerce or communications.

As to the first element (i.e. intentionally accessing a computer without authorization or exceeding authorized access), the primary question here is whether any conscious violation of an Internet website's terms of service will cause an individual's contact with the website via computer to become "intentionally access[ing] . . . without authorization" or "exceeding authorization." Initially, it is noted that three of the key terms of the first element (i.e., "intentionally," "access a computer," and "without authorization") are undefined, and there is a considerable amount [**29] of controversy as to the meaning of the latter two phrases. See *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582 n.10 (1st Cir. 2001) ("Congress did not define the phrase 'without authorization,' perhaps assuming that the words speak for themselves. The meaning, however, has proven to be elusive."); *Southwest Airlines Co. v. BoardFirst*, [**459] L.L.C., 2007 U.S. Dist. LEXIS 96230 at *36 (N.D. Tex. 2007) ("BoardFirst") ("The CFAA does not define the term 'access.'"); Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer*

Misuse Statutes, 78 *N.Y.U. L. Rev.* 1596, 1619-21 (2003) ("Kerr, Cybercrime's Scope"); Mark A. Lemley, Place and Cyberspace, 91 *Cal. L. Rev.* 521, 528-29 (2003); Dan Hunter, Cyberspace as Place and the Tragedy of the Digital Anticommons, 91 *Cal. L. Rev.* 439, 477 (2003).

While "intentionally" is undefined, the legislative history of the CFAA clearly evinces Congress's purpose in its choice of that word. Prior to 1986, 18 U.S.C. § 1030(a)(2) utilized the phrase "knowingly accesses." See United States Code 1982 Ed. Supp. III at 16-17. In the 1986 amendments to the statute, the word "intentionally" was substituted for the word "knowingly." [**30] See 18 U.S.C.A. § 1030 "Historical and Statutory Notes" at 450 (West 2000). In Senate Report No. 99-432 at 5-6, reprinted at 1986 U.S.C.C.A.N. 2479, 2483-84, it was stated that:

Section 2(a)(1) amends 18 U.S.C. 1030(a)(2) to change the scienter requirement from "knowingly" to "intentionally," for two reasons. First, intentional acts of unauthorized access - rather than mistaken, inadvertent, or careless ones - are precisely what the Committee intends to proscribe. Second, the Committee is concerned that the "knowingly" standard in the existing statute might be inappropriate for cases involving computer technology The substitution of an "intentional" standard is designed to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another. Again, this will comport with the Senate Report on the Criminal Code, which states that "'intentional' means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective." [Footnote omitted.]

Under § 1030(a)(2)(C), the "requisite intent" is "to obtain [**31] unauthorized access of a protected computer." *United States v. Willis*, 476 F.3d 1121, 1125 (10th Cir. 2007) ("The government need not also prove that . . . the information was used to any particular ends."); see also S.Rep. No.104-357, at 7-8 ("[T]he crux of the offense

under subsection 1030(a)(2)(C) . . . is abuse of a computer to obtain the information.").

As to the term "accesses a computer," one would think that the dictionary definition of verb transitive "access" would be sufficient. That definition is "to gain or have access to; to retrieve data from, or add data to, a database" Webster's New World Dictionary, Third College Edition, 7 (1988) (henceforth "Webster's New World Dictionary"). Most courts that have actually considered the issue of the meaning of the word "access" in the CFAA have basically turned to the dictionary meaning. See e.g. *BoardFirst*, 2007 U.S. Dist. LEXIS 96230 at *36; *Role Models Am., Inc. v. Jones*, 305 F. Supp. 2d 564, 566-67 (D. Md. 2004); *Am. Online, Inc. v. Nat'l Health Care Discount, Inc.*, 121 F.Supp.2d 1255, 1272-73 (N.D. Iowa 2000). However, academic commentators have generally argued for a different interpretation of the word. For example, [**32] as stated in Patricia L. Bellia, *Defending Cyberproperty*, 79 *N.Y.U. L. Rev.* 2164, 2253-54 (2004):

We can posit two possible readings of the term "access." First, it is possible to adopt a broad reading, under which "access" means any interaction between two computers. In other words, "accessing" a computer simply means transmitting electronic signals to a computer that the computer processes in some way. A narrower understanding of "access" would focus not merely on the successful exchange of electronic signals, but rather on conduct by which one is in a position to obtain privileges or information not available to the general public. The choice between these two meanings of "access" obviously affects what qualifies as unauthorized conduct. If we adopt the broader reading of access, and any successful interaction between computers qualifies, then breach of policies or contractual terms purporting to outline permissible uses of a system can constitute unauthorized access to the system. Under the narrower reading of access, however, [460] only breach of a code-based restriction on the system would qualify.

Professor Bellia goes on to conclude that "[c]ourts would better serve both the statutory [**33] intent of the CFAA and public policy by limiting its application to unwanted uses only in connection with code-based controls on access." *Id.* at 2258. But see Kerr, *Cybercrime's Scope*, 78 *N.Y.U. L. Rev.* at 1619-21, 1643, and 1646-48 (arguing for a "broad construction of access . . . as any successful interaction with the computer"). It is simply noted that, while defining "access" in terms of a code-based restriction might arguably be a preferable approach, no case has adopted it¹⁷ and the CFAA legislative history does not support it.

17 But see *BoardFirst*, 2007 U.S. Dist. LEXIS 96230 at *43-44 ("§ 1030(a)(2)(C). However, the BoardFirst court did not adopt a "code-based" definition of "accessing without authorization" but requested further briefing on the issue.

As to the term "without authorization," the courts that have considered the phrase have taken a number of different approaches in their analysis. See generally Kerr, *Cybercrime's Scope*, 78 *N.Y.U. L. Rev.* at 1628-40. Those approaches are usually based upon analogizing the concept of "without authorization" as to computers to a more familiar and mundane predicate presented in or suggested by the specific factual situation at [**34] hand. See e.g., *United States v. Phillips*, 477 F.3d 215, 219 (5th Cir.), cert. denied, 552 U.S. 820, 128 S. Ct. 119, 169 L. Ed. 2d 27 (2007), ("Courts have therefore typically analyzed the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user."). Thus, for example, where a case arises in the context of employee misconduct, some courts have treated the issue as falling within an agency theory of authorization. See, e.g., *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006); *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F.Supp.2d 1121, 1124-25 (W.D. Wash. 2000). Likewise, the Ninth Circuit (in dealing with the issue of purported consent to access emails pursuant to a subpoena obtained in bad faith in the context of the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, and the CFAA) applied the law of trespass to determine whether a subpoenaed party had effectively authorized the defendants' access. See *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072-75, 1078 (9th Cir. 2004). Further, where the relationship between the parties [**35] is contractual in nature or resembles

such a relationship, access has been held to be unauthorized where there has been an ostensible breach of contract. See e.g., *EF Cultural Travel BV*, 274 F.3d at 583-84; *Phillips*, 477 F.3d at 221 ("[c]ourts have recognized that authorized access typically arises only out of a contractual or agency relationship."). But see *Brett Senior & Associates v. Fitzgerald*, 2007 U.S. Dist. LEXIS 50833 at *13-14 (E.D. Pa. 2007) (observing - in the context of an employee's breach of a confidentiality agreement when he copied information from his firm's computer files to give to his new employer: "It is unlikely that Congress, given its concern 'about the appropriate scope of Federal jurisdiction' in the area of computer crime, intended essentially to criminalize state-law breaches of contract.").

Within the breach of contract approach, most courts that have considered the issue have held that a conscious violation of a website's terms of service/use will render the access unauthorized and/or cause it to exceed authorization. See, e.g., *Southwest Airlines Co. v. Farechase, Inc.*, 318 F.Supp.2d 435, 439-40 (N.D. Tex. 2004); *Nat'l Health Care Disc., Inc.*, 174 F.Supp.2d at 899; [**36] *Register.com, Inc. v. Verio, Inc.*, 126 F.Supp.2d 238, 247-51 (S.D.N.Y. 2000), *aff'd*, 356 F.3d 393 (2d Cir. 2004); *Am. Online, Inc. v. LCGM, Inc.*, 46 F.Supp.2d 444, 450 (E.D. Va. 1998); see also *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 62-63 (1st Cir. 2003) ("A lack of authorization could be established by an explicit statement on the website restricting access . . . [W]e think that the public website provider can easily spell out explicitly what is forbidden . . ."). But see *BoardFirst*, 2007 U.S. Dist. LEXIS 96230 at *40 (noting that the above cases and their particular application of the law "have received their share of criticism from commentators"). [**461] The court in *BoardFirst* further stated:

[I]t is at least arguable here that BoardFirst's access of the Southwest website is not at odds with the site's intended function; after all, the site is designed to allow users to obtain boarding passes for Southwest flights via the computer. In no sense can BoardFirst be considered an "outside hacker[] who break[s] into a computer" given that southwest.com is a publicly available website that anyone can access and use. True, the Terms posted on south-west.com

do not give sanction [**37] to the particular *manner* in which BoardFirst uses the site -- to check in Southwest customers for financial gain. But then again § 1030(a)(2)(C) does not forbid the *use* of a protected computer for any prohibited *purpose*; instead it prohibits one from intentionally *accessing* a computer "without authorization". As previously explained, the term "access", while not defined by the CFAA, ordinarily means the "freedom or ability to . . . make use of" something. Here BoardFirst or any other computer user obviously has the *ability* to make use of southwest.com given the fact that it is a publicly available website the access to which is not protected by any sort of code or password. *Cf. Am. Online*, 121 F.Supp.2d at 1273 (remarking that it is unclear whether an AOL member's violation of the AOL membership agreement results in "unauthorized access").¹⁸

Id. at *43-44 (emphasis in original).

18 Subsequently, the court in *Am. Online* did conclude that violating the website's terms of service would be sufficient to constitute "exceed[ing] authorized access." 174 F.Supp.2d at 899.

In this particular case, as conceded by the Government,¹⁹ the only basis for finding that Drew intentionally accessed MySpace's [**38] computer/servers without authorization and/or in excess of authorization was her and/or her co-conspirator's violations of the MSTOS by deliberately creating the false Josh Evans profile, posting a photograph of a juvenile without his permission and pretending to be a sixteen year old O'Fallon resident for the purpose of communicating with Megan. Therefore, if conscious violations of the MySpace terms of service were not sufficient to satisfy the first element of the CFAA misdemeanor violation as per 18 U.S.C. §§ 1030(a)(2)(C) and 1030(a)(2)(A), Drew's *Rule 29(c)* motion would have to be granted on that basis alone. However, this Court concludes that an intentional breach of the MSTOS can potentially constitute accessing the MySpace computer/server without authorization and/or in excess of

authorization under the statute.

19 See Reporter's Transcript of July 2, 2009 Hearing at 3-4.

There is nothing in the way that the undefined words "authorization" and "authorized" are used in the CFAA (or from the CFAA's legislative history²⁰) which indicates that Congress intended for them to have specialized meanings.²¹ As delineated in Webster's New World Dictionary at 92, to "authorize" ordinarily [**39] means "to give official approval to or permission for . . .".

20 For example, when Congress added the term "exceeds authorized access" to the CFAA in 1986 and defined it as meaning "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter", it was observed that the definition (which includes the concept of accessing a computer with authorization) was "self-explanatory." See S.Rep. No. 99-432, at 13 (1986), reprinted at 1986 U.S.C.C.A.N. 2479, 2491.

21 Commentators have criticized the legislatures' understandings of computers and the accessing of computers as "simplistic" and based upon the technology in existence in the 1970's and 1980's (e.g. pre-Internet) rather than upon what currently exists. See, e.g., Kerr, *Cybercrime's Scope*, 78 *N.Y.U. L. Rev.* at 1640-41.

It cannot be considered a stretch of the law to hold that the owner of an Internet website has the right to establish the extent to (and the conditions under) which members of the public will be allowed access to information, services and/or applications which are available on the website. See generally *Phillips*, 477 F.3d at 219-21; [**40] *EF Cultural Travel BV*, 318 F.3d at 62; *Register.com, Inc.*, 126 F.Supp.2d at 245-46; *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F.Supp. 1015, 1023-24 (S.D. Ohio 1997). Nor can it be doubted that the owner can relay and impose [**462] those limitations/restrictions/conditions by means of written notice such as terms of service or use provisions placed on the home page of the website. See *EF Cultural Travel BV*, 318 F.3d at 62-63. While issues might be raised in particular cases as to the sufficiency of the notice and/or sufficiency of the user's assent to the terms, see generally *Specht v. Netscape Communications Corp.*, 306 F.3d 17,

30-35 (2d Cir. 2002); *BoardFirst*, 2007 U.S. Dist. LEXIS 96230 at *11-21, and while public policy considerations might in turn limit enforcement of particular restrictions, see *EF Cultural Travel BV*, 318 F.3d at 62, the vast majority of the courts (that have considered the issue) have held that a website's terms of service/use can define what is (and/or is not) authorized access vis-a-vis that website.

Here, the MSTOS defined "services" as including "the MySpace.com Website . . . , the MySpace.com instant messenger, and any other connection with the Website [**41] ." See Exhibit 3 at 1. It further notified the public that the MSTOS "sets forth the legally binding terms for your use of the services." *Id.* Visitors and members were informed that "you are only authorized to use the Services . . . if you agree to abide by all applicable laws and to this Agreement." *Id.* Moreover, to become a MySpace member and thereby be allowed to communicate with other members and fully utilize the MySpace Services, one had to click on a box to confirm that the user had agreed to the MySpace Terms of Service. *Id.*; see also Exhibit 1 at 2. Clearly, the MSTOS was capable of defining the scope of authorized access of visitors, members and/or users to the website.²²

22 MySpace utilizes what have become known as "browsewrap" and "clickwrap" agreements in regards to its terms of service. Browsewraps can take various forms but basically the website will contain a notice that - by merely using the services of, obtaining information from, or initiating applications within the website - the user is agreeing to and is bound by the site's terms of service. See *Burcham v. Expedia, Inc.*, 2009 U.S. Dist. LEXIS 17104 at *9-10 n.5 (E.D. Mo. 2009); *BoardFirst*, 2007 U.S. Dist. LEXIS 96230 at *13-15; [**42] *Ticketmaster Corp. v. Tickets.Com, Inc.*, 2003 U.S. Dist. LEXIS 6483 at *9 (C.D. Cal. 2003) ("[A] contract can be formed by proceeding into the interior web pages after knowledge (or, in some cases presumptive knowledge) of the conditions accepted when doing so."); *Specht v. Netscape Communications Corp.*, 150 F.Supp.2d 585, 594 (S.D.N.Y. 2001), *aff'd*, 306 F.3d 17 (2d Cir. 2002); *Pollstar v. Gigmania, Ltd.*, 170 F.Supp.2d 974, 981 (E.D. Cal. 2000). "Courts considering browsewrap agreements have held that 'the validity of a browsewrap license turns on whether a website

user has actual or constructive knowledge of a site's terms and conditions prior to using the site.'" *Burcham*, 2009 U.S. Dist. LEXIS 17104 at *9-10 n.5, quoting *BoardFirst*, 2007 U.S. Dist. LEXIS 96230 at *15-16.

Clickwrap agreements require a user to affirmatively click a box on the website acknowledging awareness of and agreement to the terms of service before he or she is allowed to proceed with further utilization of the website. See *Specht*, 306 F.3d at 22 n.4; *CoStar Realty Info., Inc. v. Field*, 612 F.Supp.2d 660, 669 (D. Md. 2009). Clickwrap agreements "have been routinely upheld by circuit and district courts." *Burcham*, 2009 U.S. Dist. LEXIS 17104 at *8; [**43] see also *Specht*, 306 F.3d at 22 n.4; *CoStar Realty Info.*, 612 F.Supp.2d at 669; *DeJohn v. The .TV Corp. Int'l*, 245 F.Supp.2d 913, 921 (N.D. Ill. 2003).

As a "visitor" to the MySpace website and being initially limited to the public areas of the site, one is bound by MySpace's browsewrap agreement. If one wishes further access into the site for purposes of creating a profile and contacting MySpace members (as Drew and the co-conspirators did), one would have to affirmatively acknowledge and assent to the terms of service by checking the designated box, thereby triggering the clickwrap agreement. As stated in the MSTOS, "This Agreement is accepted upon your use of the Website or any of the Services and is further affirmed by you becoming a Member." Exhibit 3 at 7; see generally, *Doe v. MySpace, Inc.*, 474 F.Supp.2d 843, 846 (W.D. Tex. 2007).

B. Contravention of the Void-for-Vagueness Doctrine

1. Applicable Law

Justice Holmes observed that, as to criminal statutes, there is a "fair warning" requirement. As he stated in *McBoyle v. United States*, 283 U.S. 25, 27, 51 S. Ct. 340, 75 L. Ed. 816 (1931):

Although it is not likely that a criminal will carefully consider the text of the law before he murders or steals, it is

reasonable [**44] that a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed. [*463] To make the warning fair, so far as possible the line should be clear.

As further elaborated by the Supreme Court in *United States v. Lanier*, 520 U.S. 259, 266, 117 S. Ct. 1219, 137 L. Ed. 2d 432 (1997):

There are three related manifestations of the fair warning requirement. First, the vagueness doctrine bars enforcement of "a statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application." *Connally v. General Constr. Co.*, 269 U.S. 385, 391, 46 S. Ct. 126, 70 L. Ed. 322 (1926) Second, as a sort of "junior version of the vagueness doctrine," H. Packer, *The Limits of the Criminal Sanction* 95 (1968), the canon of strict construction of criminal statutes, or rule of lenity, ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered Third, although clarity at the requisite level may be supplied by judicial gloss on an otherwise uncertain statute, . . . due process bars courts from applying a novel construction [**45] of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope In each of these guises, the touchstone is whether the statute, either standing alone or as construed, made it reasonably clear at the relevant time that the defendant's conduct was criminal. [Citations omitted.]

The void-for-vagueness doctrine has two prongs: 1) a definitional/notice sufficiency requirement and, more importantly, 2) a guideline setting element to govern law enforcement. In *Kolender v. Lawson*, 461 U.S. 352, 357-58, 103 S. Ct. 1855, 75 L. Ed. 2d 903 (1983), the Court explained that:

As generally stated, the void-for-vagueness doctrine requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement Although the doctrine focuses both on actual notice to citizens and arbitrary enforcement, we have recognized recently that the more important aspect of the vagueness doctrine "is not actual notice, but the other principal element of the doctrine -- the requirement that a legislature establish minimal [**46] guidelines to govern law enforcement." *Smith [v. Goguen]*, 415 U.S. [566,] 574, 94 S. Ct. 1242, 39 L. Ed. 2d 605 [1974]. Where the legislature fails to provide such minimal guidelines, a criminal statute may permit "a standardless sweep [that] allows policemen, prosecutors, and juries to pursue their personal predilections." *Id.* at 575. [Footnote and citations omitted.]

To avoid contravening the void-for-vagueness doctrine, the criminal statute must contain "relatively clear guidelines as to prohibited conduct" and provide "objective criteria" to evaluate whether a crime has been committed. *Gonzales v. Carhart*, 550 U.S. 124, 149, 127 S. Ct. 1610, 167 L. Ed. 2d 480 (2007) (quoting *Posters 'N' Things, Ltd. v. United States*, 511 U.S. 513, 525-26, 114 S. Ct. 1747, 128 L. Ed. 2d 539 (1994)). As stated in *Connally v. General Construction Co.*, 269 U.S. 385, 391-92, 46 S. Ct. 126, 70 L. Ed. 322 (1926):

The question whether given legislative enactments have been thus wanting in certainty has frequently been before this court. In some of the cases the statutes involved were upheld; in others, declared invalid. The precise point of differentiation in some instances is not easy of statement. But it will be enough for present purposes to say generally that the decisions of the court upholding statutes as sufficiently certain, rested [**47] upon the conclusion that they

employed words or phrases having a technical or other special meaning, well enough known to enable those within their reach to correctly apply them, . . . or a well-settled common law meaning, notwithstanding an element of degree in the definition as to which estimates might differ, . . . or, as broadly stated . . . in *United States v. Cohen Grocery Co.*, 255 U.S. 81, 92, 41 S. Ct. 298, 65 L. Ed. 516, "that, for reasons found to result either from the text of the statutes involved or the subjects with which they dealt, a standard of some sort was afforded." [Citations omitted.]

However, a "difficulty in determining whether certain marginal offenses are within the meaning of the language under attack as [*464] vague does not automatically render a statute unconstitutional for indefiniteness . . . Impossible standards of specificity are not required." *Jordan v. De George*, 341 U.S. 223, 231, 71 S. Ct. 703, 95 L. Ed. 886 (1951) (citation and footnote omitted). "What renders a statute vague is not the possibility that it will sometimes be difficult to determine whether the incriminating fact it establishes has been proved; but rather the indeterminacy of precisely what that fact is." *United States v. Williams*, 553 U.S. 285, 128 S.Ct. 1830, 1846, 170 L. Ed. 2d 650 (2008). [*48] In this regard, the Supreme Court "has made clear that scienter requirements alleviate vagueness concerns." *Gonzales*, 550 U.S. at 149; see also *Colautti v. Franklin*, 439 U.S. 379, 395, 99 S. Ct. 675, 58 L. Ed. 2d 596 (1979) ("This Court has long recognized that the constitutionality of a vague statutory standard is closely related to whether that standard incorporates a requirement of *mens rea*").

"It is well established that vagueness challenges to statutes which do not involve *First Amendment* freedoms must be examined in the light of the facts of the case at hand." *United States v. Mazurie*, 419 U.S. 544, 550, 95 S. Ct. 710, 42 L. Ed. 2d 706 (1975); *United States v. Purdy*, 264 F.3d 809, 811 (9th Cir. 2001). "Whether a statute is . . . unconstitutionally vague is a question of law" *United States v. Ninety-Five Firearms*, 28 F.3d 940, 941 (9th Cir. 1994).

2. Definitional/Actual Notice Deficiencies

The pivotal issue herein is whether basing a CFAA

misconduct violation as per 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A) upon the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine. This Court concludes that it does primarily because of the absence of minimal guidelines to govern law enforcement, but also [*49] because of actual notice deficiencies.

As discussed in Section IV(A) above, terms of service which are incorporated into a browsewrap or clickwrap agreement can, like any other type of contract, define the limits of authorized access as to a website and its concomitant computer/server(s). However, the question is whether individuals of "common intelligence" are on notice that a breach of a terms of service contract can become a crime under the CFAA. Arguably, they are not.

First, an initial inquiry is whether the statute, as it is written, provides sufficient notice. Here, the language of section 1030(a)(2)(C) does not explicitly state (nor does it implicitly suggest) that the CFAA has "criminalized breaches of contract" in the context of website terms of service. Normally, breaches of contract are not the subject of criminal prosecution. See generally *United States v. Handakas*, 286 F.3d 92, 107 (2d Cir. 2002), overruled on other grounds in *United States v. Rybicki*, 354 F.3d 124, 144 (2d Cir. 2003) (en banc). Thus, while "ordinary people" might expect to be exposed to civil liabilities for violating a contractual provision, they would not expect criminal penalties.²³ Id. This would [*50] especially be the case where the services provided by MySpace are in essence offered at no cost to the users and, hence, there is no specter of the users "defrauding" MySpace in any monetary sense.²⁴

²³ But see *United States v. Sorich*, 427 F.Supp.2d 820, 834 (N.D. Ill. 2006), aff'd, 531 F.3d 501 (7th Cir. 2008), cert. denied, 129 S. Ct. 1308, 173 L. Ed. 2d 645 (2009) ("[S]imply because . . . actions can be considered violations of the 'contract' . . . does not mean that those same actions do not qualify as violations of [a criminal] statute.").

²⁴ Also, it is noted here that virtually all of the decisions which have found a breach of a website's terms of service to be a sufficient basis to establish a section 1030(a)(2)(C) violation have been in civil actions, not criminal cases.

Second, if a website's terms of service controls what

is "authorized" and what is "exceeding authorization" - which in turn governs whether an individual's accessing information or services on the website is criminal or not, *section 1030(a)(2)(C)* would be unacceptably vague because it is unclear whether any or all violations of terms of service will render the access unauthorized, or whether only certain ones will. For example, in [**51] the present case, MySpace's terms of service prohibits a member from engaging in a multitude of activities on the website, including such conduct as "criminal or tortious [*465] activity," "gambling," "advertising to . . . any Member to buy or sell any products," "transmit[ing] any chain letters," "covering or obscuring the banner advertisements on your personal profile page," "disclosing your password to any third party," etc. See Exhibit 3 at 5. The MSTOS does not specify which precise terms of service, when breached, will result in a termination of MySpace's authorization for the visitor/member to access the website. If any violation of any term of service is held to make the access unauthorized, that strategy would probably resolve this particular vagueness issue; but it would, in turn, render the statute incredibly overbroad and contravene the second prong of the void-for-vagueness doctrine as to setting guidelines to govern law enforcement.²⁵

25 Another uncertainty is whether, once a user breaches a term of service, is every subsequent accessing of the website by him or her without authorization or in excess of authorization.

Third, by utilizing violations of the terms of service as [**52] the basis for the *section 1030(a)(2)(C)* crime, that approach makes the website owner - in essence - the party who ultimately defines the criminal conduct. This will lead to further vagueness problems. The owner's description of a term of service might itself be so vague as to make the visitor or member reasonably unsure of what the term of service covers. For example, the MSTOS prohibits members from posting in "band and filmmaker profiles . . . sexually suggestive imagery or any other unfair . . . [c]ontent intended to draw traffic to the profile." Exhibit 3 at 4. It is unclear what "sexually suggestive imagery" and "unfair content" ²⁶ mean. Moreover, website owners can establish terms where either the scope or the application of the provision are to be decided by them *ad hoc* and/or pursuant to undelineated standards. For example, the MSTOS provides that what constitutes "prohibited content" on the website is determined "in the sole discretion of

MySpace.com" Id. Additionally, terms of service may allow the website owner to unilaterally amend and/or add to the terms with minimal notice to users. See, e.g., *id.* at 1.

26 See *Time Warner Entm't Co., L.P. v. FCC*, 240 F.3d 1126, 1135, 345 U.S. App. D.C. 186 (D.C. Cir. 2001) [**53] ("The word 'unfair' is of course extremely vague.").

Fourth, because terms of service are essentially a contractual means for setting the scope of authorized access, a level of indefiniteness arises from the necessary application of contract law in general and/or other contractual requirements within the applicable terms of service to any criminal prosecution. For example, the MSTOS has a provision wherein "any dispute" between MySpace and a visitor/member/user arising out of the terms of service is subject to arbitration upon the demand of either party. Before a breach of a term of service can be found and/or the effect of that breach upon MySpace's ability to terminate the visitor/member/user's access to the site can be determined, the issue would be subject to arbitration.²⁷ Thus, a question arises as to whether a finding of unauthorized access or in excess of authorized access can be made without arbitration.

27 An arbitration clause is considered to be "broad" when it contains language to the effect that arbitration is required for "any" claim or dispute which "arises out of" the agreement. *Fleet Tire Service v. Oliver Rubber Co.*, 118 F.3d 619, 621 (8th Cir. 1997); see also *Schoendube Corp. v. Lucent Technologies, Inc.*, 442 F.3d 727, 729 (9th Cir. 2006). [**54] Where a broad arbitration clause is in effect, "even the question of whether the controversy relates to the agreement containing the clause is subject to arbitration." *Fleet Tire Service*, 118 F.3d at 621. Moreover, "[a]n agreement to arbitrate 'any dispute' without strong limiting or excepting language immediately following it logically includes not only the dispute, but the consequences naturally flowing from it" *Management & Tech. Consultants v. Parsons-Jurden*, 820 F.2d 1531, 1534-35 (9th Cir. 1987). Further, where the parties have agreed that an issue is to be resolved by way of arbitration, the matter must be decided by the arbitrator, and "a court is not to rule on the potential merits of the underlying claim[]

indeed even if it appears to the court to be frivolous" *AT&T Technologies, Inc. v. Communications Workers of Am.*, 475 U.S. 643, 649-50, 106 S. Ct. 1415, 89 L. Ed. 2d 648 (1986).

Furthermore, under California law, ²⁸ a material breach of the MSTOS by a user/member does not automatically discharge the contract, but merely "excuses the injured party's performance, and gives him or her the election [*466] of certain remedies." 1 Witkin, Summary of California Law (Tenth Ed.): Contracts § 853 at [*55] 940 (2008). Those remedies include rescission and restitution, damages, specific performance, injunction, declaratory relief, etc. *Id.* The contract can also specify particular remedies and consequences in the event of a breach which are in addition to or a substitution for those otherwise afforded by law. *Id.* at § 855 at 942. The MSTOS does provide that: "MySpace.com reserves the right, in its sole discretion . . . to restrict, suspend, or terminate your access to all or part of the services at any time, for any or no reason, with or without prior notice, and without liability." Exhibit 3 at 2. However, there is no provision which expressly states that a breach of the MSTOS automatically results in the termination of authorization to access the website. Indeed, the MSTOS cryptically states: "you are only authorized to use the Services . . . if you agree to abide by all applicable laws and to this Agreement." *Id.* at 1 (emphasis added).

28 According to the MSTOS, "If there is any dispute about or involving the Services, you agree that the dispute shall be governed by the laws of the State of California without regard to conflict of law provisions" Exhibit 3 at 7.

3. The Absence [*56] of Minimal Guidelines to Govern Law Enforcement

Treating a violation of a website's terms of service, without more, to be sufficient to constitute "intentionally access[ing] a computer without authorization or exceed[ing] authorized access" would result in transforming section 1030(a)(2)(C) into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanor criminals. As noted in Section IV(A) above, utilizing a computer to contact an Internet website by itself will automatically satisfy all remaining elements of the misdemeanor crime in 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A). Where the website's terms of use only

authorizes utilization of its services/applications upon agreement to abide by those terms (as, for example, the MSTOS does herein), any violation of any such provision can serve as a basis for finding access unauthorized and/or in excess of authorization.

One need only look to the MSTOS terms of service to see the expansive and elaborate scope of such provisions whose breach engenders the potential for criminal prosecution. Obvious examples of such breadth would include: 1) the lonely-heart who submits intentionally [*57] inaccurate data about his or her age, height and/or physical appearance, which contravenes the MSTOS prohibition against providing "information that you know is false or misleading"; 2) the student who posts candid photographs of classmates without their permission, which breaches the MSTOS provision covering "a photograph of another person that you have posted without that person's consent"; and/or 3) the exasperated parent who sends out a group message to neighborhood friends entreating them to purchase his or her daughter's girl scout cookies, which transgresses the MSTOS rule against "advertising to, or solicitation of, any Member to buy or sell any products or services through the Services." See Exhibit 3 at 4. However, one need not consider hypotheticals to demonstrate the problem. In this case, Megan (who was then 13 years old) had her own profile on MySpace, which was in clear violation of the MSTOS which requires that users be "14 years of age or older." *Id.* at 2. No one would seriously suggest that Megan's conduct was criminal or should be subject to criminal prosecution.

Given the incredibly broad sweep of 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A), should conscious violations [*58] of a website's terms of service be deemed sufficient by themselves to constitute accessing without authorization or exceeding authorized access, the question arises as to whether Congress has "establish[ed] minimal guidelines to govern law enforcement." *Kolender*, 461 U.S. at 358; see also *City of Chicago v. Morales*, 527 U.S. 41, 60, 119 S. Ct. 1849, 144 L. Ed. 2d 67 (1999). Section 1030(a)(2)(C) does not set forth "clear guidelines" or "objective criteria" as to the prohibited conduct in the Internet/website or similar contexts. See generally *Posters 'N' Things, Ltd.*, 511 U.S. at 525-26. For instance, section 1030(a)(2)(C) is not limited to instances where the website owner contacts law enforcement to complain about an individual's unauthorized access or exceeding permitted access on the

site.²⁹ Nor is there any [*467] requirement that there be any actual loss or damage suffered by the website or that there be a violation of privacy interests.

29 Here, the prosecution was not initiated based on a complaint or notification from MySpace to law enforcement officials.

The Government argues that *section 1030(a)(2)(C)* has a scienter requirement which dispels any definitional vagueness and/or dearth of guidelines, citing to *United States v. Sablan*, 92 F.3d 865 (9th Cir. 1996). [**59] The Court in *Sablan* did observe that:

[T]he computer fraud statute does not criminalize other-wise innocent conduct. Under the statute, the Government must prove that the defendant intentionally accessed a federal interest computer without authorization. Thus, *Sablan* must have had a wrongful intent in accessing the computer in order to be convicted under the statute. This case does not present the prospect of a defendant being convicted without any wrongful intent as was the situation in [*United States v. X-Citement Video* 513 U.S. 64, 71-73, 115 S. Ct. 464, 130 L. Ed. 2d 372 (1994)].

Id. at 869. However, *Sablan* is easily distinguishable from the present case as it: 1) did not involve the defendant's accessing an Internet website;³⁰ 2) did not consider the void-for-vagueness doctrine but rather the *mens rea* requirement; and 3) dealt with a different CFAA subsection (i.e. 18 U.S.C. § 1030(a)(5)) and in a felony situation.

30 In *Sablan*, the defendant was a bank employee who had been recently fired for circumventing its security procedures in retrieving files. Early one morning, she entered the closed bank through an unlocked door and, using an unreturned key, went to her former work site. Utilizing an old password, she [**60] logged onto the bank's mainframe where she called up several computer files. Although defendant denied any additional actions, the government charged her with changing certain files and deleting others. As a result of her conduct, several bank files were severely damaged. See 92 F.3d at 866.

The only scienter element in *section 1030(a)(2)(C)* is the requirement that the person must "intentionally" access a computer without authorization or "intentionally" exceed authorized access. It has been observed that the term "intentionally" itself can be vague in a particular statutory context. See, e.g., *American Civil Liberties Union v. Gonzales*, 478 F.Supp.2d 775, 816-17 (E.D. Pa. 2007), aff'd, 534 F.3d 181, 205 (3rd Cir. 2008), cert. denied, 129 S. Ct. 1032, 173 L. Ed. 2d 293 (2009).

Here, the Government's position is that the "intentional" requirement is met simply by a conscious violation of a website's terms of service. The problem with that view is that it basically eliminates any limiting and/or guiding effect of the scienter element. It is unclear that every intentional breach of a website's terms of service would be or should be held to be equivalent to an intent to access the site without authorization [**61] or in excess of authorization. This is especially the case with MySpace and similar Internet venues which are publically available for access and use. See generally *BoardFirst*, 2007 U.S. Dist. LEXIS 96230 at *43. However, if every such breach does qualify, then there is absolutely no limitation or criteria as to which of the breaches should merit criminal prosecution. All manner of situations will be covered from the more serious (e.g. posting child pornography) to the more trivial (e.g. posting a picture of friends without their permission). All can be prosecuted. Given the "standardless sweep" that results, federal law enforcement entities would be improperly free "to pursue their personal predilections." 31 *Kolender*, 461 U.S. at 358 (citing *Smith v. Goguen*, 415 U.S. 566, 575, 94 S. Ct. 1242, 39 L. Ed. 2d 605 (1994)).

31 In comparison, the felony violation of 18 U.S.C. § 1030(a)(2)(C) contains effective scienter elements because it not only requires the intentional accessing of a computer without authorization or in excess of authorization, but also the prerequisite that such access must be "in furtherance" of a [**62] crime or tortious act which, in turn, will normally contain additional scienter and/or wrongful intent conditions.

In sum, if any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization, the result will be that *section 1030(a)(2)(C)* becomes a law "that affords too

LEXSEE 2007 U.S.DIST. LEXIS 87951

In re Grand Jury Subpoena (Boucher)

No. 2:06-mj-91

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF VERMONT

2007 U.S. Dist. LEXIS 87951

November 29, 2007, Decided

November 29, 2007, Filed

SUBSEQUENT HISTORY: Reversed by, Motion denied by, Objection sustained by *In re Grand Jury Subpoena (Boucher)*, 2009 U.S. Dist. LEXIS 13006 (D. Vt., Feb. 19, 2009)

COUNSEL: [*1] For Sebastien D. Boucher, Defendant (1): Bradley S. Stetler, LEAD ATTORNEY, Stetler, Allen & Kampmann, Burlington, VT; James H. Budreau, LEAD ATTORNEY, Law Office of James Budreau, Boston, MA.

For USA, Plaintiff: Paul J. Van de Graaf, LEAD ATTORNEY, Office of the United States Attorney District of Vermont, Burlington, VT.

JUDGES: Jerome J. Niedermeier, United States Magistrate Judge.

OPINION BY: Jerome J. Niedermeier

OPINION

OPINION AND ORDER

(Paper 14)

On December 17, 2006, defendant Sebastien Boucher was arrested on a complaint charging him with transportation of child pornography in violation of 18 U.S.C. § 2252A(a)(1). At the time of his arrest government agents seized from him a laptop computer containing child pornography. The government has now determined that the relevant files are encrypted, password-protected, and inaccessible. The grand jury has subpoenaed Boucher to enter a password to allow access to the files on the computer. Boucher has moved to quash

the subpoena on the grounds that it violates his *Fifth Amendment* right against self-incrimination. On July 9, 2007 and November 1, 2007, the Court held evidentiary hearings on the motion.

Background

On December 17, 2006, Boucher and his father crossed the [*2] Canadian border into the United States at Derby Line, Vermont. At the border station, agents directed Boucher's car into secondary inspection. Customs and Border Protection Officer Chris Pike performed the secondary inspection.

Officer Pike found a laptop computer in the back seat of the car. He opened the computer and accessed the files without entering a password. Officer Pike conducted a search of the computer files for any images or videos. He located approximately 40,000 images, some of which appeared to be pornographic based on the names of the files.

Officer Pike asked Boucher whether any of the image files on the laptop contained child pornography. Boucher responded that he was uncertain, and Officer Pike continued investigating the contents of the computer. Officer Pike noticed several file names that appeared to reference child pornography. He then called Special Agent Mark Curtis of Immigration and Customs Enforcement who has experience and training in recognizing child pornography.

When Agent Curtis arrived, he examined the computer and found a file named "2yo getting raped during diaper change." Agent Curtis was unable to open the file to view it. However, Agent Curtis determined

[*3] that the file had been opened on December 11, 2006. He continued to investigate and found thousands of images of adult pornography and animation depicting adult and child pornography.

Agent Curtis then read Boucher his Miranda rights. Boucher waived his rights in writing and agreed to speak to Agent Curtis. Agent Curtis asked Boucher about the file "2yo getting raped during diaper change." Boucher stated that he downloads many pornographic files from online newsgroups onto a desktop computer at home and then transfers them to his laptop. Boucher also stated that he sometimes unknowingly downloads images that contain child pornography but deletes them when he realizes their contents.

Agent Curtis asked Boucher to show him where the files he downloaded from the newsgroups were located on the laptop. Boucher was allowed access to the laptop and navigated to a part of the hard drive designated as drive Z. Agent Curtis did not see Boucher enter a password to access drive Z. Agent Curtis began searching through drive Z in Boucher's presence though Boucher appeared to be uncomfortable with this.

Agent Curtis located many adult pornographic files and one video entitled "preteen bondage." Agent [*4] Curtis viewed the video and observed what appeared to be a preteen girl masturbating. He asked Boucher whether he had any similar files on his laptop, and Boucher again stated that he usually deletes files that he discovers to contain child pornography.

Agent Curtis then asked Boucher to leave the room and continued to examine drive Z. He located several images and videos of child pornography in drive Z. After consulting with the United States Attorney's office, Agent Curtis arrested Boucher. He then seized the laptop, after shutting it down.

On December 29, 2006, Mike Touchette of the Vermont Department of Corrections took custody of the laptop. Touchette created a mirror image of the contents of the laptop. When Touchette began exploring the computer, he could not access drive Z because it was protected by encryption algorithms through the use of the software Pretty Good Privacy ("PGP"), which requires a password to access drive Z. Since shutting down the laptop, the government has been unable to access drive Z to view the images and videos containing child pornography.

Secret Service Agent Matthew Fasvlo, who has experience and training in computer forensics, testified that it is nearly [*5] impossible to access these encrypted files without knowing the password. There are no "back doors" or secret entrances to access the files. The only way to get access without the password is to use an automated system which repeatedly guesses passwords. According to the government, the process to unlock drive Z could take years, based on efforts to unlock similarly encrypted files in another case. Despite its best efforts, to date the government has been unable to learn the password to access drive Z.

To gain access to drive Z and the files in question, the grand jury has subpoenaed Boucher directing him to:

provide all documents, whether in electronic or paper form, reflecting any passwords used or associated with the Alienware Notebook Computer, Model D9T, Serial No. NKD900TA5L00859, seized from Sebastien Boucher at the Port of Entry at Derby Line, Vermont on December 17, 2006.

Boucher has moved to quash the subpoena as violative of his *Fifth Amendment* right against self-incrimination. At the hearing the government suggested that Boucher could enter the password into the computer without the government, the grand jury, or the Court observing or recording the password in any way. The [*6] government also suggested that to avoid any *Fifth Amendment* issue the Court could order that the act of entering the password could not be used against Boucher. The Court must now determine whether compelling Boucher to enter the password into the laptop would violate his *Fifth Amendment* privilege against self-incrimination.

Discussion

The *Fifth Amendment* privilege against self-incrimination "protects a person ... against being incriminated by his own compelled testimonial communications." *Fisher v. United States*, 425 U.S. 391, 409, 96 S. Ct. 1569, 48 L. Ed. 2d 39 (1976). For the privilege to apply, the communication must be compelled, testimonial, and incriminating in nature. *Id.* at 408. Subpoenas require compliance and therefore constitute compulsion. *Id.* at 409 (stating that a subpoena

requiring production of evidence "without doubt involves substantial compulsion."). Because the files sought by the government allegedly contain child pornography, the entry of the password would be incriminating. Whether the privilege against self incrimination applies therefore depends on whether the subpoena seeks testimonial communication.

Both parties agree that the *contents* of the laptop do not enjoy *Fifth Amendment* protection as [*7] the contents were voluntarily prepared and are not testimonial. *See id. at 409-10* (holding previously created work documents not privileged under the *Fifth Amendment*). Also, the government concedes that it cannot compel Boucher to disclose the password to the grand jury because the disclosure would be testimonial. The question remains whether entry of the password, giving the government access to drive Z, would be testimonial and therefore privileged.

I. Entering the Password is Testimonial

Compelling Boucher to enter the password forces him to produce evidence that could be used to incriminate him. Producing the password, as if it were a key to a locked container, forces Boucher to produce the contents of his laptop.

The act of producing even unprivileged evidence can have communicative aspects itself and may be "testimonial" and entitled to *Fifth Amendment* protection. *United States v. Doe*, 465 U.S. 605, 612, 104 S. Ct. 1237, 79 L. Ed. 2d 552 (1984) [hereinafter *Doe I*] ("Although the contents of a document may not be privileged, the act of producing the document may be."). An act is testimonial when the act entails implicit statements of fact, such as admitting that evidence exists, is authentic, or is within a suspect's [*8] control. *Doe v. United States*, 487 U.S. 201, 209, 108 S. Ct. 2341, 101 L. Ed. 2d 184 (1988) [hereinafter *Doe II*]. The privilege against self-incrimination protects a suspect from being compelled to disclose any knowledge he has, or to speak his guilt. *Id. at 210-11*. The suspect may not be put in the "cruel trilemma" of choosing between self-accusation, perjury, or contempt. *Id. at 212*.

The government points to *Doe II* in support of its contention that entering the password is non-testimonial and therefore not privileged. In *Doe II*, a suspect was subpoenaed to sign a form requesting his bank records from banks in the Cayman Islands and Bermuda. *Id. at*

203. The suspect asserted his privilege against self-incrimination, arguing that signing the form would be testimonial and incriminating. *Id. at 207-09*. But the form only spoke in the hypothetical, not referencing specific accounts or banks. *Id. at 215*. The Court held that the form did not acknowledge any accounts and made no statement, implicitly or explicitly, about the existence or control over any accounts. *Id. at 215-16*. Because signing the form made no statement about the suspect's knowledge, the Court held that the act lacked testimonial significance and the privilege [*9] did not apply. *Id. at 218*.

Entering a password into the computer implicitly communicates facts. By entering the password Boucher would be disclosing the fact that he knows the password and has control over the files on drive Z. The procedure is equivalent to asking Boucher, "Do you know the password to the laptop?" If Boucher does know the password, he would be faced with the forbidden trilemma; incriminate himself, lie under oath, or find himself in contempt of court. *Id. at 212*.

Unlike the situation in *Doe II*, Boucher would be compelled to produce his thoughts and the contents of his mind. In *Doe II*, the suspect was compelled to act to obtain access without indicating that he believed himself to have access. Here, when Boucher enters a password he indicates that he believes he has access.

The Supreme Court has held some acts of production are unprivileged such as providing fingerprints, blood samples, or voice recordings. *Id. at 210*. Production of such evidence gives no indication of a person's thoughts or knowledge because it is undeniable that a person possesses his own fingerprints, blood, and voice. *Id. at 210-11*. Unlike the unprivileged production of such samples, it is not without [*10] question that Boucher possesses the password or has access to the files.

In distinguishing testimonial from non-testimonial acts, the Supreme Court has compared revealing the combination to a wall safe to surrendering the key to a strongbox. *See id. at 210, n.9; see also United States v. Hubbell*, 530 U.S. 27, 43, 120 S. Ct. 2037, 147 L. Ed. 2d 24 (2000). The combination conveys the contents of one's mind; the key does not and is therefore not testimonial.¹ *Doe II*, 487 U.S. at 210, n.9. A password, like a combination, is in the suspect's mind, and is therefore testimonial and beyond the reach of the grand jury subpoena.

1 The Supreme Court's use of the term "surrender" creates a reasonable inference that the Court assumed the government's prior knowledge of the suspect's possession of the key. If it was unknown whether the suspect had the key, compelling the production of the key would disclose the suspect's access to the strongbox contents and might therefore be a privileged testimonial act.

II. Effect of Non-Viewing

The government has offered to restrict the entering of the password so that no one views or records the password. While this would prevent the government from knowing what the password is, it would not change [*11] the testimonial significance of the act of entering the password. Boucher would still be implicitly indicating that he knows the password and that he has access to the files. The contents of Boucher's mind would still be displayed, and therefore the testimonial nature does not change merely because no one else will discover the password.

III. Effect of Exclusion from Evidence

During the hearing on the motion, the government offered not to use the production of the password against Boucher. The government argues that this would remove the testimonial aspect from the act, and that the act would therefore be unprivileged. This is the same argument the Supreme Court rejected in *United States v. Hubbell*, 530 U.S. 27, 120 S. Ct. 2037, 147 L. Ed. 2d 24 (2000).

In *Hubbell*, the Court determined the precise scope of a grant of immunity with respect to the production of subpoenaed documents. *Id.* at 34. The government subpoenaed business documents from Hubbell but granted him immunity for the production. *Id.* at 31. The government then prosecuted him for fraud based on the documents that he had produced. *Id.* The government argued that it was not making improper use of the production because it did not need the act of production itself [*12] as evidence and the documents themselves were unprivileged. *Id.* at 40-45. The government argued that the immunity granted did not preclude "derivative use", use of the fruits of the production, because the documents themselves were the fruit only of the simple physical act of production. *Id.* at 43.

The Court acknowledged that the government would

not have to use the act of production as evidence to prove the existence, authenticity, or custody of the documents, or to prove the charges against Hubbell. *Id.* at 41. However, the Court noted that Hubbell's immunity needed to extend to any derivative use in order to protect his *Fifth Amendment* privilege. *Hubbell*, 530 U.S. at 38-39 (citing *Kastigar v. United States*, 406 U.S. 441, 92 S. Ct. 1653, 32 L. Ed. 2d 212 (1972)). The Court also re-emphasized the critical importance of a suspect's protection from prosecution based on sources of information obtained from compelled testimony. *Id.* at 39.

The Court found that the act of production had testimonial aspects, because production communicated information about the existence, custody, and authenticity of the documents. *Id.* 36-37. The compelled testimony of the production became the first in a chain of evidence which led to the [*13] prosecution. *Id.* at 42. The Court refused to divorce the physical act of production from its implicit testimonial aspect to make it a legitimate, wholly independent source. *Id.* at 40. In doing so, the Court reaffirmed its holding that derivative use immunity is coextensive with the privilege against self-incrimination. *Id.* at 45. Accordingly, the Court held that Hubbell could not be prosecuted based on the documents and only evidence wholly independent of the production could be used. *Id.* at 45-46.

Here, as in *Hubbell*, the government cannot separate the non-testimonial aspect of the act of production, entering the password, from its testimonial aspect. The testimonial aspect of the entry of the password precludes the use of the files themselves as derivative of the compelled testimony. Any files the government would find based on Boucher's entry of the password could not be used against him, just as Hubbell's documents could not be used against him. Barring the use of the entry of the password is not enough to protect Boucher's privilege.

IV. Foregone Conclusion

The government also asserts that the information gained through entry of the password is a "foregone conclusion", therefore [*14] no privilege applies. The Government relies on *In re Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992*, 1 F.3d 87 (2d Cir. 1993) [hereinafter *Doe III*]. *Doe III* held that the privilege against self-incrimination does not apply to an act of production if the existence and location of the subpoenaed evidence is known to the government and the

production would not "implicitly authenticate" the evidence. *Id.* at 93.

In *Doe III*, the suspect had produced a photocopy of a personal calendar but the Government suspected that the calendar had been altered through the whiting out of incriminating entries. *Id.* at 88-90. The government subpoenaed the suspect to produce the original calendar before the grand jury. *Id.* The Second Circuit reasoned that the existence and location of the calendar was a "foregone conclusion" because it was known, through production of the photocopy, that the suspect had possession of the calendar and the original calendar added little or nothing to the sum total of the government's information. *Id.* at 93. The court also found that act of production itself was not necessary to authenticate the original calendar because the Government could authenticate it simply by comparing [*15] it to the photocopy. *Id.* Therefore, because the government had knowledge of the existence and location of the original calendar and did not need to use the act of production to authenticate the original calendar, the suspect had no act of production privilege and was required to produce the original calendar before the grand jury. *Id.* at 93-94.

Here, the subpoena can be viewed as either compelling the production of the password itself or compelling the production of the files on drive Z. Both alternatives are distinguishable from *Doe III*.

If the subpoena is requesting production of the files in drive Z, the foregone conclusion doctrine does not apply. While the government has seen some of the files on drive Z, it has not viewed all or even most of them. While the government may know of the existence and location of the files it has previously viewed, it does not know of the existence of other files on drive Z that may contain incriminating material. By compelling entry of the password the government would be compelling production of all the files on drive Z, both known and unknown. Unlike in *Doe III*, the files the government has not seen could add much to the sum total of the government's [*16] information. Therefore, the foregone conclusion doctrine does not apply and the act of

production privilege remains.

Since the government is trying to compel the production of the password itself, the foregone conclusion doctrine cannot apply. The password is not a physical thing. If Boucher knows the password, it only exists in his mind. This information is unlike a document, to which the foregone conclusion doctrine usually applies, and unlike any physical evidence the government could already know of. It is pure testimonial production rather than physical evidence having testimonial aspects. Compelling Boucher to produce the password compels him to display the contents of his mind to incriminate himself. *Doe III* did not deal with production of a suspect's thoughts and memories but only previously created documents. The foregone conclusion doctrine does not apply to the production of non-physical evidence, existing only in a suspect's mind where the act of production can be used against him.

Conclusion

For the foregoing reasons, the motion to quash the subpoena is GRANTED.

Dated at Burlington, in the District of Vermont, this 29th day of November, 2007.

/S/ Jerome J. Niedermeier

Jerome [*17] J. Niedermeier

United States Magistrate Judge

Any party may object to this Report and Recommendation within 10 days after service by filing with the clerk of the court and serving on the magistrate judge and all parties, written objections which shall specifically identify the portions of the proposed findings, recommendations or report to which objection is made and the basis for such objections. Failure to file objections within the specified time waives the right to appeal the District Court's order. *See* Local Rules 72.1, 72.3, 73.1; 28 U.S.C. § 636(b)(1) ; *Fed. R. Civ. P.* 72(b), 6(a) and 6(e).

LEXSEE 2007 U.S. DIST. LEXIS 30603

Saxton v. Sheets

CASE NO. 3: 06 CV 306

**UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF
OHIO, EASTERN DIVISION**

2007 U.S. Dist. LEXIS 30603

April 24, 2007, Decided

April 25, 2007, Filed

SUBSEQUENT HISTORY: Affirmed by *Saxton v. Sheets*, 547 F.3d 597, 2008 U.S. App. LEXIS 24041 (6th Cir.) (6th Cir. Ohio, 2008)

PRIOR HISTORY: *State v. Saxton*, 2004 Ohio 3546, 2004 Ohio App. LEXIS 3216 (Ohio Ct. App., Marion County, July 6, 2004)

COUNSEL: [*1] For Anthony L. Saxton, Petitioner: J. Banning Jasiunas, LEAD ATTORNEY, Office of the Ohio Public Defender, Columbus, OH.

For Michael Sheets, Warden, Respondent: Gregory T. Hartke, LEAD ATTORNEY, Office of the Attorney General, Cleveland, OH.

JUDGES: Donald C. Nugent, United States District Judge.

OPINION BY: Donald C. Nugent

OPINION

MEMORANDUM OPINION AND ORDER

This matter comes before the Court upon the Report and Recommendation of Magistrate Judge Patricia A. Hemann. The Report and Recommendation (ECF # 25), filed on December 6, 2006, is ADOPTED by this Court, and Petitioner's Petition for Writ of Habeas Corpus (ECF # 1), filed pursuant to 28 U.S.C. § 2254, on February 8, 2006, is denied.

Pursuant to *Local Rule* 72.2, this matter was referred to Magistrate Judge Hemann for the preparation of a

report and recommendation. On December 6, 2006, Magistrate Judge Hemann recommended that this Court deny Petitioner's Petition. After numerous extensions of time, on April 12, 2007, Petitioner filed objections to the Report and Recommendation. (ECF # 42.)

The Court has reviewed the Report and Recommendation *de novo*. See *Thomas v. Arn*, 474 U.S. 140, 106 S. Ct. 466, 88 L. Ed. 2d 435 (1985) [*2] . Moreover, it has considered all of the pleadings, affidavits, motions, and filings of the parties. Despite Petitioner's assertions to the contrary, the Court finds Magistrate Judge Hemann's Report and Recommendation to be well-written, well-supported, and correct. In addition, the Court finds Petitioner's objections to the same to be entirely lacking in merit. Therefore, the Report and Recommendation (ECF # 25) is ADOPTED in its entirety, the Petition for Writ of Habeas Corpus is DENIED (ECF # 1), and Petitioner's objections are thereby DENIED (ECF # 42).

Furthermore, the Court certifies, pursuant to 28 U.S.C. § 1915(a)(3), that an appeal from this decision could not be taken in good faith, and there is no basis upon which to issue a certificate of appealability. 28 U.S.C. § 2253(c); *FED. R. APP. P.* 22(b).

IT IS SO ORDERED.

s/ Donald C. Nugent

United States District Judge

DATED: April 24, 2007

528.010 Definitions for chapter.

The following definitions apply in this chapter unless the context otherwise requires:

- (1) "Advancing gambling activity" -- A person "advances gambling activity" when, acting other than as a player, he engages in conduct that materially aids any form of gambling activity. The conduct shall include, but is not limited to, conduct directed toward the establishment of the particular game, contest, scheme, device, or activity involved; toward the acquisition or maintenance of premises, paraphernalia, equipment, or apparatus therefor; toward the solicitation or inducement of persons to participate therein; toward the actual conduct of the playing phases thereof; toward the arrangement of any of its financial or recording phases or toward any other phase of its operation. A person who gambles at a social game of chance on equal terms with other participants does not otherwise advance gambling activity by performing acts, without remuneration or fee, directed toward the arrangement or facilitation of the game as inviting persons to play, permitting the use of premises therefor and supplying equipment used therein.
- (2) "Bookmaking" means advancing gambling activity by unlawfully accepting bets upon the outcome of future contingent events from members of the public as a business.
- (3)
 - (a) "Gambling" means staking or risking something of value upon the outcome of a contest, game, gaming scheme, or gaming device which is based upon an element of chance, in accord with an agreement or understanding that someone will receive something of value in the event of a certain outcome. A contest or game in which eligibility to participate is determined by chance and the ultimate winner is determined by skill shall not be considered to be gambling.
 - (b) Gambling shall not mean charitable gaming which is licensed and regulated under the provisions of KRS Chapter 238.
- (4) "Gambling device" means:
 - (a) Any so-called slot machine or any other machine or mechanical device an essential part of which is a drum or reel with insignia thereon, and which when operated may deliver, as a result of the application of an element of chance, any money or property, or by the operation of which a person may become entitled to receive, as the result of the application of an element of chance, any money or property; or
 - (b) Any other machine or any mechanical or other device, including but not limited to roulette wheels, gambling tables and similar devices, designed and manufactured primarily for use in connection with gambling and which when operated may deliver, as the result of the application of an element of chance, any money or property, or by the operation of which a person may become entitled to receive, as the result of the application of an element of chance, any money or property;
 - (c) But, the following shall not be considered gambling devices within this definition:

1. Devices dispensing or selling combination or French pools on licensed, regular racetracks during races on said tracks.
 2. Electro-mechanical pinball machines specially designed, constructed, set up, and kept to be played for amusement only. Any pinball machine shall be made to receive and react only to the deposit of coins during the course of a game. The ultimate and only award given directly or indirectly to any player for the attainment of a winning score or combination on any pinball machine shall be the right to play one (1) or more additional games immediately on the same device at no further cost. The maximum number of free games that can be won, registered, or accumulated at one (1) time in operation of any pinball machine shall not exceed thirty (30) free games. Any pinball machine shall be made to discharge accumulated free games only by reactivating the playing mechanism once for each game released. Any pinball machine shall be made and kept with no meter or system to preserve a record of free games played, awarded, or discharged. Nonetheless, a pinball machine shall be a gambling device if a person gives or promises to give money, tokens, merchandise, premiums, or property of any kind for scores, combinations, or free games obtained in playing the pinball machine in which the person has an interest as owner, operator, keeper, or otherwise.
 3. Devices used in the conduct of charitable gaming.
- (5) "Lottery and gift enterprise" means:
- (a) A gambling scheme in which:
 1. The players pay or agree to pay something of value for chances, represented and differentiated by numbers or by combinations of numbers or by some other media, one (1) or more of which are to be designated the winning ones; and
 2. The ultimate winner is to be determined by a drawing or by some other method based upon the element of chance; and
 3. The holders of the winning chances are to receive something of value.
 - (b) A gift enterprise or referral sales plan which meets the elements of a lottery listed in paragraph (a) of this subsection is to be considered a lottery under this chapter.
- (6) "Mutuel" or "the numbers games" means a form of lottery in which the winning chances or plays are not determined upon the basis of a drawing or other act on the part of persons conducting or connected with the scheme, but upon the basis of the outcome or outcomes of a future contingent event or events otherwise unrelated to the particular scheme.
- (7) "Player" means a person who engages in any form of gambling solely as a contestant or bettor, without receiving or becoming entitled to receive any profit therefrom other than personal gambling winnings, and without otherwise rendering any material assistance to the establishment, conduct, or operation of the particular

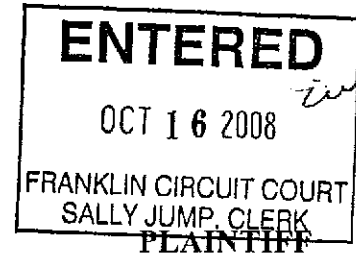
gambling activity. A person who engages in "bookmaking" as defined in subsection (2) of this section is not a "player." The status of a "player" shall be a defense to any prosecution under this chapter.

- (8) "Profiting from gambling activity" -- A person "profits from gambling activity" when, other than as a player, he accepts or receives or agrees to accept or receive money or other property pursuant to an agreement or understanding with any person whereby he participates or is to participate in the proceeds of gambling activity.
- (9) "Something of value" means any money or property, any token, object, or article exchangeable for money or property, or any form of credit or promise directly or indirectly contemplating transfer of money or property or of any interest therein, or involving extension of a service, entertainment, or a privilege of playing at a game or scheme without charge.
- (10) "Charitable gaming" means games of chance conducted by charitable organizations licensed and regulated under the provisions of KRS Chapter 238.

Effective: March 16, 1994

History: Amended 1994 Ky. Acts ch. 66, sec. 19, effective March 16, 1994. -- Amended 1992 Ky. Acts ch. 254, sec. 1, effective July 14, 1992. -- Amended 1990 Ky. Acts ch. 469, sec. 1, effective July 13, 1990. -- Amended 1988 Ky. Acts ch. 423, sec. 1, effective July 15, 1988. -- Amended 1980 Ky. Acts ch. 188, sec. 307; and ch. 267, sec. 9, effective July 15, 1980. -- Amended 1978 Ky. Acts ch. 321, sec. 5, effective June 17, 1978. -- Created 1974 Ky. Acts ch. 406, sec. 240, effective January 1, 1975.

COMMONWEALTH OF KENTUCKY
FRANKLIN CIRCUIT COURT
DIVISION II
CASE NO. 08-CI-1409



COMMONWEALTH OF KENTUCKY, ex rel.
J. MICHAEL BROWN, Secretary, Justice and
Public Safety Cabinet

vs.

OPINION AND ORDER

141 INTERNET DOMAIN NAMES

DEFENDANTS

Statement of Matters Pending

This matter is before the Court to determine if the Seizure Order entered September 18, 2008 is valid and whether the Court should proceed toward forfeiture of the 141 Internet domain names. Additionally, there are several motions filed by various Groups described in greater detail below. For purposes of brevity, the Court identifies the following common pending matters for its consideration and action, to wit: (1) the motion to dismiss the present civil action for forfeiture,¹ (2) the motion to vacate or set aside this Court's Seizure Order of September 18,² (3) the motion of Internet Gaming Association to Intervene pursuant to Kentucky Civil Rules of Procedure (CR) 24.

¹ The persons and entities who filed separate Motions to Dismiss were Atty. William E. Johnson on behalf of the Group of 7 (hereinbelow defined), Atty. Alison L. Grimes on behalf of the Group of 2 (hereinbelow defined), Interactive Gaming Council, and the Interactive Media and Entertainment Gaming Association.

² The persons and entities who filed separate motions to alter or vacate the Seizure Order of September 18, 2008 were Atty. Alison L. Grimes on behalf of the Group of 2 and Atty. William E. Johnson on behalf of the Group of 7.

After reviewing the records of this case and the arguments raised in written briefs and during oral arguments, and after having been sufficiently advised, this Court hereby renders this Opinion and Order:

Parties, Other Groups, and Lawyers

The plaintiff before this Court is the Commonwealth of Kentucky, as represented by the Secretary of the Justice and Safety Cabinet, Mr. J. Michael Brown.

The named defendants to this action are 141 Internet domain names. Some, but not all, of the 141 domain names have been identified to have counsel. Annex “1,” consisting of the list of the 141 Internet Domain Names, hereinafter collectively referred to as the “Defendants 141 Domain Names”, is attached and incorporated in this Opinion and Order.

The first group of domain names, namely, playersonly.com, pokerhost.com,³ sbglobal.com,⁴ sportsbook.com, sportsinteraction.com, mysportsbook.com, and linesmaker.com, are represented by Attorneys William E. Johnson,⁵ Kevin D. Finger,⁶ Paul D. McGrady⁷ and Patrick O’Brien.⁸ For purposes of clarity, we hereinafter refer to this group of 7 defendant domain names as the “**Group of 7.**”

³ The Court notes that in the Motions filed by Atty. William E. Johnson before the hearing of September 26, counsel included the Internet domain name pokerhost.com as one of the *res* he represented. However, in subsequent motions filed, this name was no longer included. For purposes of the present order, the Court will treat that pokerhost.com is still represented by William E. Johnson.

⁴ The Court notes that in the Motions filed by William E. Johnson before the hearing of September 26, counsel included the Internet domain name sbglobal.com as one of the *res* he represented. However, in subsequent motions filed, this name was no longer included. For purposes of the present order, the Court will treat that sbglobal.com is still represented by counsel.

⁵ Attorney William E. Johnson is local counsel in Frankfort, Kentucky, and practices with Johnson True & Guarnieri LLP in the Commonwealth.

⁶ Attorney Kevin F. Finger practices law with Greenberg Traurig LLP in Chicago LLP and was authorized by this Court to practice in Kentucky *pro hac vice* in relation to this case.

⁷ Attorney Paul D. McGrady practices law with Greenberg Traurig LLP in Chicago and was authorized by this Court to practice in Kentucky *pro hac vice* in relation to this case.

⁸ Attorney Patrick T. O’Brien also practices law with Greenberg Traurig LLP in Fort Lauderdale, Florida.

The second group of domain names, namely, goldenpalace.com and goldencasino.com, are represented by Attorneys P. Douglas Barr, Palmer G. Vance II and Alison Lundergan Grimes.⁹ The domain name goldenpalace.com is further represented by Atty. Lawrence G. Walters.¹⁰ For purposes of clarity, we hereinafter refer to this group of 2 defendant domain names as the “**Group of 2.**”

There are other groups that requested leave from this Court to intervene and/or to appear as a friend or amici curiae of the Court. These groups are as follows:

The **Interactive Gaming Council** (IGC) is an incorporated trade association organized and existing under the laws of British Columbia, Canada. IGC comes to this Court for the purpose of representing the rights of the internet gaming community and its general members, especially the owners and operators of some (but not all) of the domain names identified in the Commonwealth’s Second Amended Complaint. The Court notes that the IGC did not expressly identify which of the 141 domain names are owned by or related to the operations of its members.

The **Interactive Media Entertainment & Gaming Association, Inc.** (IMEGA), is an incorporated trade association organized and existing under the laws of the State of New Jersey. IMEGA is a voluntary association that collects and disseminates information regarding electronic and Internet-based gaming. IMEGA comes to this Court for the purpose of representing the rights of some of its members who are the owners of some (but not all) of the domain names included in the Commonwealth’s Second Amended Complaint. The Court also notes that IMEGA and its counsel did not identify the specific

⁹ Attorneys P. Douglas Barr, Palmer G. Vance, and Alison L. Grimes are local attorneys, practicing with Stoll Keenon Ogden PLLC in the Commonwealth.

¹⁰ Attorney Lawrence G. Walters practices law with Weston, Garrou Walters & Mooney in Florida and was authorized by this Court to practice in Kentucky pro hac vice in relation to this case.

domain names, which are owned or used in the business operations of IMEGA's members.

The **Poker Players Alliance** (PPA) is an incorporated association of poker players and enthusiasts, organized and existing under the laws of the State of Nevada. The PPA represented to this Court that it has at least 13,000 members residing in Kentucky. The PPA sought leave to file a Memorandum *Amicus Curiae* for the purpose of bringing to the Court's attention that some of the domain names in the Commonwealth's Second Amended Complaint merely host games of poker, which, according to the PPA, is predominantly a game of skill and not chance and therefore should not be considered illegal under Kentucky's gambling laws.

The **Internet Commerce Association** (ICA) is also an incorporated trade association composed of domain name registrants and website owners organized and existing under the laws of the District of Columbia. The ICA sought leave to file a Memorandum *Amici Curiae* in opposition to the proceedings initiated by the Commonwealth before this Court. The mission of the ICA is to promote the interests of its members in the areas of Internet governance and domain name administration. The ICA monitors for its members any judicial actions that impact its members and their Internet business activities.

The **Network Solutions, Inc.** (NSI) and Mr. Michael R. Mazzoli, by way of seeking leave to admit its counsel, Mr. Timothy B. Hyland, sought permission to allow NSI to participate in all aspects of the action, including trial and appeal, but without submitting to the jurisdiction of this Court, whether *in rem* or *in personam*.

For purposes of clarity and brevity, the Group of 7, Group of 2, IGC, IMEGA, PPA, ICA and NSI, and their lawyers and representatives will hereinafter be collectively referred to as the "Opposing Groups and Lawyers."

STATEMENT OF FACTS

On August 26, 2008, the Commonwealth filed a complaint with this Court. Together with the complaint, the Commonwealth moved that the file be sealed until such time that the Court would consider the Commonwealth's Motion for a Seizure Order. This Court granted the Commonwealth's Order on this date, thereby sealing the records.

On September 18, 2008, the Commonwealth sought that the original complaint be stricken from the record of this case. Instead, the Commonwealth filed its Amended Complaint and Second Amended Complaint on the same day. Upon motion by the Commonwealth, the Court directed the Clerk of the Court to physically remove the first complaint from the record and return it to the counsel of the Commonwealth, consistent with the Kentucky Supreme Court's holding in *Roman Catholic Diocese of Lexington v. Noble*, 92 S.W.3d 724 (Ky., 2002).

That afternoon, this Court heard the Commonwealth's Motion for the Seizure of the Defendants 141 Domain Names. In the Commonwealth's Motion, it sought an order to direct the registrars of the Defendants 141 Domain Names to transfer each of the Defendants 141 Domain Names to the Commonwealth's account.

At the September 18, 2008 hearing, the Commonwealth presented evidence that it created a team which engaged in at least 500 man-hours on-line, randomly accessing various internet gambling websites available in Kentucky. This team was created for the purpose of ascertaining whether internet gambling is available in Kentucky.

At the hearing, the Commonwealth called two witnesses to the stand. One witness, Officer Gregory G. Howard, testified that his team conducted an investigation for a period of at least 2 months. During that 2-month period, the team, at his office computer located in Kentucky, accessed gambling websites through the use of various

domain names. Officer Howard's team maintained a log book which recorded which domain names allowed them access to a website with live on-line gambling. According to Officer Howard, they used a Kentucky bank account or Kentucky bank issued credit card to place bets or play on-line slot machines and roulettes.

The second witness, Mr. Derick James Paulson, testified as an expert on cybercrime. Mr. Paulson opined that an Internet domain name is a device or a transport device allowing Kentuckians to engage in internet gambling.

The Commonwealth also offered in evidence several exhibits, described as follows:

1. Exhibit 1 consists of the logbook containing the day-to-day records and notes of all on-line gambling transactions completed or attempted;
2. Exhibit 2 consists of the hard drive from the computer used in investigation, on which all on-line plays and transactions, including computer gaming software, were stored;
3. Exhibit 3 consists of the 141 files covering each of the 141 domain names confirmed to allow access to or registration from a user or consumer from Kentucky;
4. Exhibit 4 consists of prints of computer screens ("screen shots") of the on-line gambling, i.e., 32redpoker, arcticstarpoker.com, nordicbet.net, with access or registration to those websites either blocked or denied.
5. Exhibit 5 consists of 137 pages of screen shots detailing the series of interfaces between the player (while at his desktop located in Kentucky) and the casino website. These interfaces included creation of a gambling account, on-line transfer of financial information where players are asked to "deposit" credits into his/her/their account/s created; the processing and confirmation of the financial information provided by the player; the funding of the gambling accounts through the use of the player's credit card, debit card, ecocard, click2pay card, or neteller card; and the debiting of the gambling account after a loss at the chosen game or play.
6. Exhibit 6 is a table/chart identifying the specific groups of domain names and their corresponding registrars
7. Exhibit 7 consists of hard copies of the printout of the active tracking for all internet gambling activity conducted.

8. Exhibit 8 consists of a table/chart identifying a specific group of domain names which uses Microgaming software when completing internet gambling transactions.

On the basis of the Commonwealth's presentation, the Court rendered Findings of Fact and Conclusions of Laws dated 18 September 2008.¹¹

On the basis of the Commonwealth's presentation, the Court issued its Order of Seizure of Domain Names entered on September 18, 2008. In this Order, this Court found that probable cause existed to support a finding that the Defendants 141 Domain Names are being used in connection with illegal gambling activity within the Commonwealth. The Order of Seizure directed the respective registrars of each of the Defendants 141 Domain Names to transfer the registration to the account of the Commonwealth, without any changes to the domain names' configurations. The Court authorized the service of the Seizure Order upon each Registrar by using the procedures applicable in each Registrar's written policies and the written policies of the Internet Corporation for Assigned Names and Numbers (ICANN), including service by overnight courier. The Commonwealth was also directed to give notice by overnight courier, email, or facsimile to persons identified in the WHOIS information database as claiming ownership for each of the Defendants 141 Domain Names. Finally, the Seizure Order scheduled a hearing to determine whether any party who has a right to the Defendants 141 Domain Names is entitled to the return of his/her/its property. Upon motion of the Commonwealth, the hearing originally set for September 25 was re-scheduled for September 26. The September 26 hearing was for the purpose of forfeiture of the domain names.

This Court then received written motions in opposition to the present civil forfeiture action from IGC, IMEGA, and Group of 7. At the September 26, 2008 hearing, the

¹¹ The Court's September 18, 2008 Findings of Fact and Conclusions of Law were withdrawn and set aside on September 30, 2008.

lawyers for the Commonwealth, and other lawyers representing the Group of 7, Group of 2, IGC, IMEGA, and PPA, were before the Court. Counsel for the Commonwealth, Mr. Robert M. Foote,¹² objected to the standing of any lawyers purporting to represent the Defendants 141 Domain Names without specifying the identity of the actual owner or registrant concerned. On the basis of the foregoing, the Commonwealth's counsel further objected to all the written motions for intervention, motions to dismiss, and motions to vacate the seizure order.

Although standing was objected to by the Commonwealth's counsel, this Court allowed the representatives of the Group of 7, Group of 2, IGC, IMEGA, and PPA to be heard, but subject to the Court's further consideration on the issue of standing.

At the conclusion of the hearing, this Court granted the representatives of the Commonwealth and the Opposing Groups and Lawyers permission to file their respective briefs on the following issues: (a) standing; (b) jurisdiction of the Court; (c) nature or status of Defendants 141 Domain Names as property; (d) nature of Defendants 141 Domain Names as a 'gambling device' as defined in KRS 528.010; (e) exclusion of poker as a gambling activity as defined in KRS 528.010. *See* Order entered on October 2, 2008.

The Commonwealth and the Opposing Groups and Lawyers who were present during the September 26, 2008 hearing timely filed their respective Memoranda on the issues. ICA, who was not then represented at the September 26 hearing, filed its Motion for Leave to File Memorandum Amicus Curiae.

¹² Mr. Foote practices law with Foote, Meyers, Mielke & Flowers, LLC in Illinois and was authorized by this Court to practice pro hac vice in this case.

On October 7, 2008, this Court conducted a second hearing and allowed the representatives of the Commonwealth, the Group of 7, the Group of 2, IGC, IMEGA, PPA, ICA, and Network Solutions to be heard regarding their various motions.

This Court took all matters under advisement and now being sufficiently advised hereby issues its order.

DISCUSSION OF THE ISSUES

1. Does the Court have subject matter jurisdiction over a civil forfeiture action involving internet domain names?

Jurisdiction is a fundamental concept that goes to the very core of a court's authority and power to act or decide a case. *Hisle v. Lexington-Fayette Urban County Government*, 258 S.W. 3d 422, 428 (Ky. Ct. App. 2008) (Discretionary Rev. Denied, Aug. 13, 2008). This Court's power to inquire into facts, apply the law, make decisions and declare judgment over the claims of the Commonwealth and over the Defendants 141Domain Names is both constrained by and a function of this Court's jurisdiction. *Id.*, 429 (citing *Nordike v. Nordike*, 231 S.W. 3d 733,737 (Ky. 2007)).

Kentucky Circuit Courts, like this Court, are courts of general jurisdiction with a wide range of authority over various types of cases. *Hisle*, 258 S.W. 3d 422, 432. The Kentucky Constitution §112(5) states: "The Circuit Court shall have original jurisdiction over all justiciable causes not vested in some other court." This constitutional mandate imbues the circuit courts with the general power to determine all matters of controversy arising under common law or equity, or by reason of statute or constitution, unless the constitution requires that the matter be resolved by another body of the government or another court. *Hisle*, 258 S.W.3d 422, 432. Even the General Assembly does not have the authority to limit or control the circuit court's subject matter jurisdiction. *Id.*, 434.

According to the counsel of the Group of 7, this Court does not have subject matter jurisdiction over the Commonwealth's complaint for civil forfeiture. *See* Motion to Dismiss for Lack of Jurisdiction over the Subject Matter, etc. of Group of 7. The Opposing Groups and Lawyers echoed this objection during the hearings held on September 25 and October 7, 2008.

The Opposing Groups and Lawyers further contend that the language of KRS 528.100 has a bearing on the propriety of any exercise of judicial authority over the instant civil forfeiture action. KRS 528.100, as IGC's lawyers here present, contemplates forfeiture as a consequence of a conviction in a criminal proceeding. As suggested by IGC's counsel, "[w]ithout criminal conviction establishing a violation of some provision of Chapter 528, there can be no violation."¹³ Therefore, the Defendants Domain Names cannot be proceeded against in a forfeiture action.

The text of KRS 528.100 reads as follows:

"528.100 Forfeiture. Any gambling device or gambling record possessed or used in violation of this chapter is forfeited to the state, and shall be disposed of in accordance with KRS 500.900, except that the provisions of this section shall not apply to charitable gaming activity as defined by KRS 528.010(1)."

The predecessor of KRS 528.100, as correctly pointed out by IGC's counsel, is KRS 436.280.¹⁴ KRS 436.280 authorized forfeiture. *See A.B. Long Music Co. v. Com.*, 429 S.W. 2d 391, 395 (Ky. 1968). Our Supreme Court, in the case of *14 Console Type*

¹³ Memorandum in Support of Interactive Gaming Council's Motion to Dismiss, p. 19.

¹⁴ The repealed KRS 436.280 was quoted in part in *Three-One-Ball Pinball Machines v. Commonwealth*, 249 S.W. 2d 144 at 145 (Ky. 1952), in pertinent part as follows : 'Any bank, table, contrivance, machine or article used for carrying on a game prohibited by KRS 436.230, together with all money or other things staked or exhibited to allure persons to wager, may be seized by any justice of the peace, sheriff, constable or police officer of a city, with or without a warrant, and upon conviction of the person setting up or keeping the machine or contrivance, the money or other articles shall be forfeited for the use of the state, and the machine or contrivance and other articles shall be burned or destroyed. * * *'

Slot Machines v. Com., 273 S.W. 2d 582 (Ky. 1954), held that a forfeiture proceeding under KRS 436.280 is a civil action in rem. *Id.*, 583.

Looking to federal jurisprudence, we note that the United States Supreme Court draws a sharp distinction between a forfeiture proceeding that is criminal and punitive in nature, and that which is civil and remedial. See *U.S. v. Ursery*, 518 U.S. 267, 277 (1996); *United States v. One Assortment of 89 Firearms*, 465 U.S. 354 (1984).

Criminal forfeiture is part of a criminal sentence. *Libretti v. United States*, 516 U.S. 29, 42 (1995). Its fundamental purpose is punishment for a person's criminal wrongdoing. *Id.*, 41; *Ursery*, 518 U.S. 267, 293 (J. Kennedy, Concurring Opinion). See also *Horigan v. Commonwealth*, 962 S.W. 2d 860 (Ky. 1998). It forms part of the *in personam* action against the criminal defendant. Criminal forfeiture is an aspect of sentencing. *Libretti v. United States*, 516 U.S. 29, 49.

In contrast, a civil forfeiture is not punitive. *Ursery*, 518 U.S. 267, 293. A civil forfeiture is a proceeding *in rem* to forfeit property used in committing an offense. *Id.* As unanimously held by the United States Supreme Court in *Waterloo Distilling Corp v. US*, 282 U.S. 577 at 581 (1931) :

“[This] forfeiture proceeding ... is in rem. It is the property which is proceeded against, and by resort to a legal fiction, held guilty and condemned as though it were conscious instead of inanimate and insentient.”

An *in rem* civil forfeiture is a remedial civil action, distinct from potentially punitive *in personam* civil penalties such as fines. *Ursery*, 518 U.S. 267, 278. In the case of *Ursery*, 518 U.S. 267 at 284, the United States Supreme Court held that:

“Civil forfeitures ... are designed to do more than simply compensate the Government. Forfeitures serve a variety of purposes, but are designed primarily to confiscate the property used in violation of the law, and to require disgorgement of the fruits of illegal conduct.”

Returning to the IGC's counsel's construction of KRS 528.100, if this section contemplates criminal forfeiture only, then there might be some merit in their contention that forfeiture must follow as a consequence of a criminal conviction. But we find this construction narrow in light of the discussions above. KRS 528.100 has broader remedial aims. It would be absurd for our General Assembly to emphasize the pernicious nature of gambling within the state and to its determination to punish all forms of gambling, yet restrict the remedial measures made available to its law enforcement agents. KRS 528.100 contemplates a separate and independent civil proceeding, having for its purpose the condemnation of the property that is used in violation of KRS Chapter 528, independent of the innocence or guilt of its owner.

Considering the foregoing, the Commonwealth succeeded in presenting a justiciable cause in its *in rem* civil forfeiture complaint. The Commonwealth has presented overwhelming evidence that KRS Chapter 528 prohibits gambling in the Commonwealth; that the Defendants 141Domain Names have been and are being used in connection with on-line or internet gambling activities available and accessible within the Commonwealth; and that KRS 528.100 authorizes forfeiture actions of gambling devices. Based on the foregoing, this Court finds sufficient bases to exercise its authority and hear and adjudicate the civil forfeiture claim presented by the Commonwealth against the Defendants 141 Domain Names.

2. Does the Court have in rem jurisdiction over the Defendants 141 Domain Names?

(a) Are the Defendants 141 Domain Names property?

The Opposing Groups and Lawyers before this Court collectively assert that domain names are akin to a telephone number or a business or residential address only; that

domain names are but a combination of letters and numbers, which serves as a mnemonic aid, nothing more. They argue that domain names are not property, but are rights in a service contract. As such, they conclude that Defendants 141 Domain Names can not be subject to this Court's *in rem* jurisdiction or to a civil forfeiture.

The authorities cited by the Opposing Groups and Lawyers reach the conclusion that domain names are only contract rights in a fairly limited context. See Warrin E. Agin, Esq., *I'm a Domain Name. What am I? Making Sense of Kremen v. Cohen*, 14 J. Bankr. L. & Prac. 3 Art. 3 (2005). Thus, the Court does not find those cases binding and conclusive of the status of a domain name.¹⁵

However, other courts have applied the intangible property theory to domain names in at least two cases : *Online Partners .Com, Inc. v. Atlanticnet Media Corp*, 2000 WL 101242 (N.D. Cal. 2000); *Harrods Ltd. V. 60 Internet Domain Names*, 302 F.3d 214 (4th Cir. 2002). But, neither case addressed head on the issue of a domain name as a form of property. See Warren E. Agin, Esq. *I'm a Domain Name: What am I? Making Sense of Kremen v. Cohen*, 14 J. Bankr. L. & Prac. 3 Art 3 (2005). It was in *Kremen v. Cohen*, 337 F. 3d 1024 (9th Cir. 2003) that a court dealt with this issue unambiguously. *Id.* The relevant legal issue in *Kremen v. Cohen* was whether a domain name was a form of property that could be stolen under California state law. The 9th Circuit found Network

¹⁵ *Network Solutions Inc. v. Umbro Int'l, Inc.*, 529 S.E. 2d 80 (Va. 2000) (statutory garnishment proceeding against domain name registrar as garnishee in order to satisfy a judgment debtor's debt was dismissed because a domain name registrar's services to the domain name registrant is not "liability" in the context of garnishment.) *Lockheed Martin Corp. v. Network Solutions, Inc.*, 194 F. 3d 980 (9th Cir. 1999) (third party action against a domain registrant for contributory service mark infringement, unfair competition and service mark dilution was dismissed because a registrar does not supply a "product" when it enters into a domain name registration service with a putative registrant). *BASF Agrochemical Prods. V. Unkel*, 2006 WL 3533133 (W.D. La. 2006) (action for conversion of intellectual property was dismissed because incorporeal or intangible property cannot be subject of a conversion under LA conversion laws). *Wornow v. Register.com*, 8 A.D. 3d 59 (N.Y. App. Div. 1st Dept., 2004) (action for conversion by domain name registrant against its registrar was dismissed on the ground that a domain name that is not trademarked or patented is not personal property, but rather a contract right that cannot exist separate and apart from the services performed by the defendant-registrar).

Solutions Inc., as a third-party defendant on the claim against Cohen, liable to Cohen for conversion. *Kremen*, 337 F. 3d 1024, 1035. Justice Kozinski applied an attributes approach in arriving at his determination of whether a property right exists in a domain name. See Warren E. Agin, Esq. *I'm a Domain Name: What am I? Making Sense of Kremen v. Cohen*, 14 J. Bankr. L. & Prac. 3 Art 3 (2005). The three-step analysis used included whether: (1) there is an interest capable of precise definition; (2) it is capable of exclusion possession or control; and (3) the putative owner can establish a legitimate claim to exclusivity. *Kremen*, 337 F. 3d 1024, 1030.¹⁶

Domain names surely have a significant place in our modern economy. See George Vona, *Sex in the Courts, Kremen v. Cohen and the Emergency of Property Rights in Domain Names*, 19 I.P.J. 393, 403 (2006). During the oral arguments held on October 7, 2008, the Commonwealth contended that the domain names, in general, and the Defendants Domain Names, in particular, have a market value, being auctioned for sale and bought regularly through registrars acting as brokers. The real issue lies in the tremendous value that domain names have generated apart from their technical function as Internet addresses.

The Court looks to the treatment given by federal agencies to Internet domain names as relevant. The United States Treasury Department is currently advertising for public auction the Internet domain name www.DoctorTalk.com, after having been deemed to be

¹⁶ Some experts and commentators believe that Congress has had this view even before *Kremen v. Cohen* was decided. See Jeffrey M Becker, *Suing An Electronic Address : In Rem Domain Name Actions Under the ACPA*, 8 Tex Wesleyan L. Rev. 629; George Vona, *Sex in the Courts, Kremen v. Cohen and the Emergency of Property Rights in Domain Names*, 19 I.P.J. 393, 420 (2006) (ACPA is about as forceful a recognition of a property right in domain names as exists.) In 1999, Congress enacted the Anti Cybersquatting Consumer Protection Act (ACPA), which is codified in 15 U.S.C. §1125(d). While not directly applicable in the present case, the Court notes that under the ACPA, Congress authorized *in rem* jurisdiction over domain names. This Court also views such an assignment of situs to a domain name as evidence of the treatment of domain names as property.

subject to levy, seizure and sale under 26 U.S.C. §6331.¹⁷ According to the appraisal conducted by the Internal Revenue Service, the Internet domain name www.DoctorTalk.com has a net present value of \$526,000.¹⁸ The United States Department of Justice obtained forfeiture of www.software-inc.com after it was used in the sale and distribution of counterfeit computer software;¹⁹ of www.isonews.com after it was used to traffic illegal modification of chips that allowed pirated videogames.²⁰ The fact that the existence of a domain name springs from the pairing of an alphanumeric name or so-called domain name with an Internet Protocol (IP) address, the registration of such pairing to the Domain Name System does not detract from the fact that, by virtue of its scarcity and desirability, the domain name has an economic value. George Vona, *Sex in the Courts, Kremen v. Cohen and the Emergency of Property Rights in Domain Names*, 19 I.P.J. 393, 403 (2006).

Property is about the relationships of people with respect to things, both tangible and intangible. *Id.* The analogy commonly used to describe property is the bundle of rights concept. *Id.*, 403-404. Those rights include the right to possession, management and control (the right to exclude), the right to income and capital, the right to transfer inter vivos and on death, and the right to the protection under the law. *Id.*

Considering the foregoing, this Court finds the Defendants 141 Domain Names are property and therefore subject to this Court's *in rem* jurisdiction or to possible civil forfeiture.

(b) Do the Defendants 141 Domain Names have a presence in Kentucky?

¹⁷ See Brief of the Commonwealth on the In Rem Seizure of Domain Names, p. 10.

¹⁸ *Id.*

¹⁹ *Id.*, at p.11.

²⁰ *Id.*

The next inquiry is whether the Defendants Domain Names have a presence in Kentucky. This inquiry is critical to this Court's exercise of judicial authority over the Defendants 141 Domain Names.

The important case law to start this analysis with is *Pennoyer v. Neff*, 95 U.S. 714 (1877). In *Pennoyer*, the United States Supreme Court, through Justice Field, enunciated the then prevailing law on state court jurisdiction as follows:

“[E]very State has the power to determine for itself the civil status and capacities of its inhabitants; to prescribe the subjects upon which they may contract, the forms and solemnities with which their contracts shall be executed, the rights and obligations arising from them, and the mode in which their validity shall be determined and their obligations enforced; and also to regulate the manner and conditions upon which property situated within such territory, both personal and real, may be acquired, enjoyed, and transferred. The other principle of public law referred to follows from the one mentioned; that is, that no State can exercise direct jurisdiction over persons or property without its territory. [citations omitted] The several States are of equal dignity and authority, and the independence of one implies the exclusion of power of all others. And so it is laid down by jurists, as an elementary principle, that the laws of one State have no operation outside its territory, except so far as is allowed by comity; and that no tribunal established by it can extend its process beyond that territory so as to subject either persons or property to its decision. Any exertion of authority of this sort beyond this limit,’ says Story, is a mere nullity, and incapable of binding such persons or property in any other tribunals.’

Pennoyer, 95 U.S. 714 at 722-723.

Pennoyer v. Neff stood for the then prevailing law on state court jurisdiction that a person had to be physically present in a state in order to be subject to the state court's authority and its judgment imposing liability on him, i.e., a “personal” judgment. See Restatement (Second) of Law on Judgments §5 cmt. b (1982). *Pennoyer v. Neff* also stood for the then prevailing law that property had to be physically present within a state in order that a judgment could be rendered determining claims to the property. *Id.* These two doctrines became the basic elements of constitutional doctrine governing state-court

jurisdiction. *Shaffer v. Heitner*, 433 U.S. 186, 198 (1977) (citing Hazard, *A General Theory of State-Court Jurisdiction*, 1965 Sup. Ct. Rev. 241).

However, the doctrines enunciated in *Pennoyer v. Neff*, particularly that which dealt with territorial limits on jurisdictional power had been “moderated” by subsequent United States Supreme Court cases. *Shaffer*, 433 U.S. 186, 200. The concept of doing business in the State was deemed “presence” in the State, and so subject to service of process under the rule of *Pennoyer*. *Id.*, 202 (citations omitted). With the advent of automobiles, a fiction, that the out-of-state motorist by having used the state’s highways appointed a designated state official as his agent, was used in *Hess v. Pawloski*, 274 U.S. 352 (1927) to establish “presence” for purposes of the service of process consistent with the conceptual structure of *Pennoyer v. Neff*. *Id.*

In the case of *International Shoe v. Washington*, 326 U.S. 310, (1945), a unanimous United State Supreme Court declared that the demand for ‘presence’ as a prerequisite for state court authority may be met by “minimum contacts” with the state, such that the maintenance of the suit does not offend “traditional notions of fair play and substantial justice.” *Id.* at 316.

Since *International Shoe*, the physical presence requirement for state court jurisdiction over *in personam* actions as enunciated in *Pennoyer v. Neff* has been modernized.

In *Shaffer v. Heitner*, the United States Supreme Court acknowledged that no equally dramatic change occurred in the law governing jurisdiction in rem. *Shaffer*, 433 U.S. 186, 205. But the *Shaffer* Court believed that the fairness standard in *International Shoe* can be easily applied in the vast majority of cases. *Id.*, 211. The *Shaffer* Court further said, after implying the applicability of the fairness standard to jurisdiction *in rem*, that, “in

order to justify an exercise of jurisdiction *in rem*, the basis for jurisdiction must be sufficient to justify exercising “jurisdiction over the interests of the persons in a thing.” *Id* at 207.

Thus, as the law stands on state court jurisdiction, the requirement of “presence” is seen through the lens of “minimum contacts,” for both *in rem* and *in personam* actions.

Section 5 of the Second Restatement of Law on Judgments tracks the *in personam* state-court jurisdiction over persons under modern decisional law as follows:

“A state may exercise jurisdiction over a person who has a relationship to the state such that the exercise of jurisdiction is reasonable. For relationships sufficient to support an exercise of such jurisdiction. *See* Restatement, Second, Conflict of Laws §§27-32, 35-44, 47-52.” Restatement (Second) of Law on Judgments, §5 (1982).

Section 6 of the Second Restatement of Law on Judgments tracks the *in rem* state-court jurisdiction over property under modern decisional law as follows:

“A state may exercise jurisdiction to determine interests in a thing if the relationship of the thing to the state is such that the exercise of jurisdiction is reasonable. For relationships sufficient to supports an exercise of jurisdiction. *See* Restatement (Second) of Law on Judgments, § 6 (1982).

On the legislative front, states and federal legislative bodies have enacted statutes, i.e., long-arm statutes, assigning a *situs* for purposes of determining presence. See KRS 452.210. The assignment of a *situs* is particularly relevant where the thing is an intangible property, which cannot be physically located anywhere. In cases of intangible property, fictional *situs* rules are generally assigned to the property by reference to its owners.

In the context of domain names, Congress has recently assigned them a *situs*, at least for purposes of an *in rem* civil action by a trademark owner against a domain name. Under the Anticybersquatting Consumer Protection Act, a domain name has as its *situs* the judicial district in which:

“(i) the domain name registrar, or other domain name authority that registered or assigned the domain name is located; or

(ii) documents sufficient to establish control and authority regarding the disposition of the registration and use of the domain name are deposited with the court.”

15 U.S.C. §1125(d)(2)(C). The rationale for this assignment of situs is that the data in the computer at the registry is the defendant res.

The Opposing Groups and Lawyers, relying on the Anticybersquatting Consumer Protection Act (ACPA), argue that Defendants Domain Names have no *situs* within Kentucky because there are no registrars or other domain name authorities found in Kentucky. They assert that a domain name has no presence in Kentucky. Therefore, the Opposing Groups and Lawyers contend that this Court has no jurisdiction over the Defendants 141 Domain Names.

We disagree. The ACPA is not applicable in the present case, which does not involve cybersquatting. Moreover, we do not believe Congress intended to foreclose other bases for assigning “presence” for purposes of reasonable exercise of jurisdiction over persons and things, such as that developed by the United States Supreme Court in *Shaffer v. Heitner*. Even if we assume, for the sake of argument, that Congress intends to adopt a similar framework for other Internet-related matters, 15 U.S.C. §1125(d)(2)(C) is unlikely to be the only standard for purposes of recognizing “presence” of persons or property connected with the Internet. 15 U.S.C. §1125(d)(2)(D)(4) is on point. It reads, “[t]he *in rem* jurisdiction established in paragraph (2) is in addition to any other jurisdiction that otherwise exists, whether *in rem* or *in personam*.” (emphasis supplied).

The evidence in the record shows that the gambling operations that the Commonwealth’s team of investigators executed on the Internet from their desktop in Kentucky are multi-faceted: after a player (i.e., Commonwealth agents) has accessed a

gambling website through the use of a domain name, the gambling website entices the Kentucky player with the potential of making money (i.e., “Get a 30% deposit match up to \$300 for free);”²¹ provides the player with an assortment of games to choose from, i.e., slots, roulette, blackjack, craps, video poker.²² One Defendant Domain Name, vegasvilla.com, offers “166 games for the ultimate online casino experience;”²³ invites the player to download a casino software, i.e., Microgaming front-end software, that will allow the player’s computer to run games; to create a casino account which enables the player to play with real money and as a real account user; to play progressive games. After the casino software is downloaded to the player’s computer, the casino website notifies the player whether or not he has an existing casino account. If not, the website asks the player whether he wants to create an account for the purpose of purchasing credits to bet or play with. At that point, the financial or banking arm of the gambling website interfaces with the player and invites the player to purchase credits with his credit card, debit card, ecocard, click2paycard or neteller card. If the player chooses to continue, the casino website invites the player to provide information regarding where he chooses to fund the purchase of credits and the amount of money the player chooses to use the source of the funds. After the player provides that information and after the casino website processes that information and confirms that the source with which to fund the casino credits are available, the player’s computer screen is returned to the home page of the casino website to proceed with play.

²¹ Commonwealth Exhibit “5.”

²² *Id.*

²³ *Id.*

The Court perused more than 130 screen shots documenting and detailing the series of interfaces which the Commonwealth agents and the various casino websites with the corresponding domain names. All those interfaces are rooted in the domain name.

The domain name was ubiquitously present in every interface, not just at the initial access of the gambling casino's home page.²⁴

The counsel for Goldenpalace.com represented during the October 7 hearing that the operation of Goldenpalace.com is limited to maintaining the website and providing advertisement for third-party gambling websites. Thus, the Court's seizure order should be withdrawn as to them.

The Court agrees that the maintenance of a website or Internet advertisement alone, without more, is not enough to constitute presence for purposes of state court jurisdiction analysis. See *Cybersell Inc. v. Cybersell, Inc.*, 130 F. 3d 4144, 418 (9th Cir. 1997). Thus, the Court recognizes that as to any of the Defendants 141 Domain Names that identifies websites which are providing information only, the Seizure Order must be appropriately rescinded and will be rescinded in due course. The appropriate time to make that determination, i.e., whether the operations of the website identified with the domain name goldenpalace.com, however, is not in this proceeding, but during the forfeiture hearing pursuant to KRS 500.090.²⁵ The proper party to raise that defense would be a person who makes a claim over the seized *res* or his duly authorized agents.

For now, however, and considering the foregoing discussion and based on the other evidence offered by the Commonwealth during the seizure hearing on September

²⁴ The Court is also made aware by counsel that notwithstanding the seizures of the Defendants 141 Domain Names, the games that can be played through the gambling websites are still operational. According to counsel, the gambling operations have not been shut down by the Seizure Order of September 18, 2008.

²⁵ Under KRS 528.100, KRS 500.090 governs and provides the mechanism for the uniform disposition of forfeited property.

18, 2008, the Court finds that the Commonwealth has established a prima facie case that the presence of the operators of the casino websites and the Internet domain names which identify these gambling operators with is continuous and systematic, constituting reasonable bases for the exercise of this Court's jurisdiction. As the evidence in the record stands, the Defendants 141 Domain Names transport the virtual premises of an Internet gambling casino inside the houses of Kentucky residents, and are not providing information or advertising only. The Defendants 141 Domain Names perform a critical role in creating and maintaining connection by way of the various interfaces to transact a game or play. Accordingly, but subject to further review during the forfeiture hearing, the Court finds reasonable bases to conclude that the Internet gambling operators and their property, the Internet domain names, are present in Kentucky. Therefore, the Court has reasonable bases to assert its jurisdiction over them.²⁶ As stated best in *Gorman v. Ameritrade Holding Corp.*, 293 F.3d 506, 510 (C.A.D.C. 2002), "[c]yberspace is not some mystical incantation capable of warding off the jurisdiction of courts built from bricks and mortar."

(c) Are Domain Names, by reason of their illegal or unlawful use, gambling devices?

The Opposing Groups and Lawyers contend a domain name does not fit the definition of a gambling device that may be subject of forfeiture under KRS 528.100. According to IGC's counsel, a gambling device, upon the plain meaning of terms of KRS 528.010(4)(a) & (b) is a tangible device, which is designed and manufactured. A domain

²⁶ There are commentators on similar matter who have proposed the principle of "targeting" for the purpose of sanctioning behavior in the Internet as a possible standard for evaluating jurisdiction for the regulation of Internet content. See Thomas Schultz, *Carving Up the Internet : Jurisdiction, Legal Orders and Private/Public International Law*, 19 Eur. J. Int. 799 (September 2008). According to Mr. Shultz, under the model of the "targeting" principle looks to more than just the effects of Internet content, but less than physical presence as basis of exercising jurisdiction.

name is not tangible property. Therefore, a domain name cannot be subject of a forfeiture.

KRS 528.010 (4) (a) and (b) reads as follows:

“(4) ‘Gambling device’ means:

- a. Any so-called slot machine or any other machine or mechanical device an essential part of which when operated is a drum or reel with insignia thereon, and which when operated may deliver, as a result of the application of an element of chance, any money or property, or by the operation of which a person may become entitled to receive, as the result of the application of an element of chance, any money or property; or
- b. Any other machine or any mechanical or other device, including but not limited to roulette wheels, gambling tables and similar devices, designed and manufactured primarily for use in connection with gambling and which when operated may deliver, as the result of the application of an element of change, any money or property, or by the operation of which a person may become entitled to receive, as the result of the application of an element of change, any money or property.”²⁷

The Commonwealth has established, however, that the Defendants Domain Names are virtual keys for entering and creating virtual casinos from the desktop of a resident in Kentucky. The domain name is indispensable in maintaining the player’s continuing access to the virtual casinos which serve as the Internet gambling operators premises for conducting illegal gambling activity.

While the Court finds the presentation on the proper construction of the literal text of KRS 528.010(4) by IGC’s counsel exhaustive, the Court is not persuaded. Like most

²⁷ Tracing the legislative history of KRS 528.010 (4) (a) and (b) confirms that the current text is the same as its original iteration in Act of 1974, c 406, §240. Although KRS 528.010 underwent several amendments, those amendments did not touch upon the definition of a gambling device. Act of 1978, c 321, §5 amended (4) (c) (2) which read, “react only to the deposit of 1, 5 or 10 cent coins” to read “react only to the deposit of coins.” The Act of 1980, c 188, §307 deleted the text “and no more” to the phrase “react only to the deposit of coins” in (4) (c) (2), while c 267, §9 added (10) defining “charitable gaming.” Act of 1988, c 423, §1 amended (10) on the definition of “charitable gaming” further. Act of 1990, c469, §1 made stylistic changes to the first line of (4) (c) and the section (4)(c) (2). Act of 1992, c 254, , §1 added (4)(c) (3), which excluded devices used in the conduct of charitable gaming from the definition of gambling devices. Act of 1994, c 66, §19 inserted (3)(b) which provided that Gambling does not mean charitable gaming which is licensed and regulated under the provisions of KRS Chapter 238.

endeavors, a person who adheres to the literal text of the law, but violates its spirit, cannot succeed. *Welch v. Commonwealth*, 200 S.W. 371 (Ky. 1918). Our legislature has made it clear that all statutes should be interpreted to carry out its intent. *See* KRS 446.080(1). In *Gilley v. Commonwealth*, 229 S.W.2d 60 (Ky. 1950), Kentucky's highest court found numerous "number slips" to be a gambling device or contrivance that was subject to seizure and destruction by the statute. *See also Albright v. Muncrief*, 176 S.W. 2d 426 (Ark. 1943) (teletype machines, because of their use, are treated as gambling devices.)

We are unable to see that the domain name which is an intricate and integral part in creating and maintaining connection to the virtual casino from one's computer terminal is any less tainted by the unlawful activity because it is argued that it is not a manufactured machine, designed to be used in gambling activities. To this Court's mind, domain names in this particular case are designed: they are designed to attract players. Once a player accesses the virtual casino, and maintains connection, with the use of the domain name, a player's propensity to gamble is tickled. Internet domain names, when used as virtual keys to access, create and maintain a virtual casino, contain the vice at which the statute is directed.

More significantly, the Defendants 141 Domain Names, which identify Internet gambling casinos, have been "designed" to reach our state. According to the Commonwealth's counsel during the hearings held on September 26 and October 7, if owners of the Defendants 141 Domain Names operators so chose, they can filter, block and deny access to a website on the basis of geographic locations. There are software that are available, which can provide filtering functions on the basis of geographical location, i.e., geographical blocks. The Court further infers based on the

Commonwealth's Exhibit 3 that there are such Internet gambling operators which have filtering mechanism or devices to block. The blocks denied the Commonwealth's investigative team's further access of an Internet gambling website, i.e, websites identified with the domain names 32redpoker.com, arcticstarpoker.com, nordicbet.net. If there is available technology that allows any Internet gambling operator to so "design" their business activities as to filter access to geographical locations that have local laws regulating their business, then having those filtering mechanisms should be a protocol that may be reasonably required in the "design" of their business plan and their domain name use.²⁸

The Court is aware that the Domain Name System was never intended to avoid compliance with or violate International or Municipal laws, the fact remains that Domain Name System is not (or at least not yet) full-proof from vice and abuse. The Defendants Domain Names here were used and are still being used in connection with Internet gambling transactions in violation of the spirit of KRS Chapter 528. Accordingly, the Defendants 141 Domain Names fall within the meaning of a gambling device and are subject to seizure and possible forfeiture as a gambling device.

(d) Is poker "gambling" as defined by KRS 528.010(3)?

PPA argues that the game of poker is one of skill, and that a poker player will prosper according to his or her level of skill. *Fall v. Commonwealth*, 245 S.W.3d 812 (Ky. Ct. App. 2008) and KRS 528.010(3) are instructive on this matter. KRS 528.010(3) states:

²⁸ These facts support a finding of jurisdiction under the "targeting" principle described in Schultz, *Carving Up the Internet : Jurisdiction, Legal Orders and Private/Public International Law*, 19 Eur. J. Int. 799 (September 2008).

“Gambling” means staking or risking something of value upon the outcome of a contest, game, gaming scheme, or gaming device which is based upon an element of chance, in accord with an agreement or understanding that someone will receive something of value in the event of a certain outcome.”

The statute clearly delineates three components of gambling activity: the element of chance, the risking of something of value in consideration for the chance to win a prize, and the receipt of a prize for the successful player. *Commonwealth v. Malco-Memphis Theatres*, 169 S.W.2d 596 (Ky. Ct. App. 1943). PPA has not denied that its customers risk something of value, namely money, or that they stand to receive a prize if they win. Instead, PPA urges this Court to deny the element of chance inherent in poker and place domain names offering poker for profit beyond the reach of this statute. We decline to do so. KRS 528.010(3) does not require that chance be the only factor in the outcome of a gambling enterprise; just as “(n)o owner of a racehorse or a rooster would ever guarantee a winner” of a race or a fight, even a master poker player cannot guarantee victory. *Fall*, 245 S.W.3d 812 at 871. Chance, though not the only element of a game of poker, is the element which defines its essence. In the end, no matter how skillful or cunning the player, who wins and who loses is determined by the hands the players hold.

(e) Has this Court acquired control over the res?

In the previous discussion, we have examined that it is reasonable for this Court to exercise jurisdiction over the Defendants 141 Domain Names in Kentucky, consistent with the Due Process Clause as enunciated in *Shaffer v. Heitner*. We next turn to the issue of whether the Court has in fact exercised its jurisdiction over them.

For the court to acquire *in rem* jurisdiction over property, the court must take possession of property through an act of seizure. *United States v James Daniel Good Real Property*, 114 S.Ct. 492, 503 (1993). The seizure of the *res* can be either actual or

constructive. See *Miller v. United States*, 78 U.S. (11 Wall.) 268, 294 (1870); *The Brig Ann*, 13 U.S. (9 Cranch) 289 (1815) (Story, J.); *United States v. \$84,740*, 900 F.2d 1402, 1404 (9th Cir.1990); *United States v. \$10,000*, 860 F.2d 1511, 1513 (9th Cir.1988).

Since many of the Domain Names have been “seized” through ICANN, the question is begged, is there possession?

In the context of revenue and admiralty cases, a seizure is necessary to confer upon a court jurisdiction over the thing when the proceeding is in rem. *Miller v. U.S.*, 78 U.S. 268, 294 (1870). In most cases the res is movable property, capable of actual mancipation. *Id.* Unless taken into actual possession by an officer of the court, it might be eloiigned before a decree of condemnation could be made, and thus the decree would be ineffectual. *Id.* It might come into the possession of another court, and thus there might arise a conflict of jurisdiction and decision, if actual seizure and retention of possession were not necessary to confer jurisdiction over the subject. *Id.*

In *Miller*, the property to be forfeited were shares of stock and dividends. *Id.*, 292. The question presented then to the *Miller* Court was whether the mode of seizure employed by the marshal was sufficient to place the property within the jurisdiction or control of the court hearing the confiscation and condemnation proceeding. *Id.*, 293. The mode of seizure employed by the marshal was giving notice upon the vice-president and president of the companies who issued the stocks. *Id.*

The *Miller* Court found this mode of seizure as good and effective, sufficient to give the court jurisdiction over the property. *Id.*, 296. The *Miller* Court emphasized that the mode of seizure may be adapted to the nature of the property directed to be seized. *Id.* “The modes of seizure must vary. Lands cannot be seized as movable chattels may. Actual mancipation cannot be taken of stocks and credits. But it does not follow from

this that they are incapable of being seized.” *Id.* An assertion of control, with a present power and intent to exercise it, is sufficient. *Id.* These are, indeed proceedings to compel appearance, but they are, nevertheless, attachments or seizures, bringing the subject seized within the control of the court, and what is of primary importance, they show that, in admiralty practice, rights in action, things intangible, as stocks and credits, are attached by notice to the debtor, or holder, without the aid of any statute.

In the context of domain names, the domains names are clearly not capable of mancipation or physical seizure. However, it does not follow that it cannot be seized. Adapting the mode of seizure to the nature of the property, and considering the protocols of the Internet Corporation for Assigned Names and Numbers (ICANN), particularly the Uniform Domain Name Dispute Resolution Policy,²⁹ the service of the Seizure Order upon the registrars would be well-suited.

Here, the Seizure Order was served upon the registrars. Accordingly, this mode of service brought the Defendants 141 Domain Names within the control of this Court for purposes of exercising its control over the Defendants 141 Domain Names.

(f) Does the ex parte seizure of the res violate the Due Process Clause?

The Opposing Groups and Lawyers have ardently argued that the pre-notice and pre-hearing seizure of the Defendants Domain Names violated the Constitution and Kentucky’s Rules of Civil Procedure (CR). They allege that the registrants and true owners of the Defendants Domain Names should have been served with summons of the complaint and given the opportunity to be heard. They also allege that the seizure before any prior notice and hearing flies in the face of the Due Process Clause of the U.S. Constitution.

²⁹ See <http://www.icann.org/en/dndr/udrp/policy.htm> (last visited October 16, 2008).

It should be remembered that the present action is an action against property. As earlier mentioned, the nature of an *in rem* civil forfeiture proceeding is that the property violated the law and is sought to be condemned. At least for purposes of initiating and styling the action, the *in rem* civil forfeiture action is directed towards the property, not its owners. From a practical point of view, there is no summons to serve on a person when there is no person named in the complaint. The seizure of the property, discussed earlier, is the mechanism by which the Court acquires control over the property and is, for practical purposes, the mechanism which triggers the notification process to any person who claim an interest in the seized property.

Seizure, obtained without prior notice or hearing, is constitutionally permissible in certain situations. In *Calero-Toledo v. Pearson Yacht Leasing Co.*, 416 U.S. 663 (1974), the United States Supreme Court agreed that seizure for purposes of forfeiture is one of those “extra-ordinary situations” that justify postponing notice and opportunity for a hearing. *Id.*, at 667 (citing *Fuentes v. Shevin*, 407 U.S. 67, 86-87 (1972)).

The situations in which immediate seizure of a property interest, without an opportunity for prior hearing, is constitutionally permissible, includes circumstances in which “the seizure has been directly necessary to secure an important government or general public interest. Second, there has been a special need for very prompt action. Third, the State has kept strict control over its monopoly of legitimate force: the person initiating the seizure has been a government official responsible for determining, under the standards of a narrowly drawn statute, that it was necessary and justified in the particular instance.” *Id* at 91.

The United States Supreme Court denied claims of due process violation where postponement of notice and hearing was necessary to protect the public from

contaminated food, *North American Cold Storage Co. v. Chicago*, 211 U.S. 306 (1908); from a bank failure, *Coffin Bros. & Co. v. Bennett*, 277 U.S. 29 (1928); or for misbranded drugs, *Ewing v. Mytinger & Casselberry, Inc.*, 339 U.S. 594 (1950); or to aid in the collection of taxes, *Philips v. Commissioner*, 283 U.S. 589 (1931).

The Court finds that there is factual support here to justify the postponement of notice and hearing to the owners and claimants of the Defendants 141 Domain Names present here. First, seizure of the domain names serves a significant governmental purpose: seizure permits the Commonwealth to assert *in rem* jurisdiction over the property in order to conduct forfeiture proceedings, thereby fostering the public interest in preventing continued illicit use of the property as a device in accessing virtual gambling casinos and in enforcing criminal sanctions. Second, pre-seizure notice and hearing might frustrate the interests served by the statutes, since the property seized – domain names – like a yacht in the case of *Calero-Toledo*, 416 U.S. 663 at 679, will often be a type of property that could be removed from the reach of the Commonwealth, if advance warning of confiscation is given. Finally, the seizure was only effected after determination by this Court that probable cause existed based upon the evidence presented by the Commonwealth that the domain names were being used in connection with illegal gambling activity available and accessible in Kentucky.

Considering the foregoing, the pre-notice and ex parte seizure authorized on September 18, 2008 is consistent with the requirements of the Due Process Clause of the 14th Amendment.

3. Question of Standing

The issue of standing has been a heated area of discussion between the Commonwealth and the Opposing Groups and Lawyers.

Standing is a judge-made rule designed to ensure that courts are presented with an actual case or controversy. See *Flast v. Cohen*, 392 U.S. 83 (1968).

At the federal level, the doctrine of standing was intended to prevent federal courts from answering abstract questions that are better left to the respective branches of government. See *Flast*, 392 U.S. 83, 99; *Valley Forge Christian Coll. v. Ams. United for Separation of Church & States, Inc.* 454 U.S. 464 (1982). The standing doctrine has three elements: (1) there must be an actual or threatened injury; (2) the injury is traceable to the alleged conduct of the other party, and (3) the injury must be redressable by the court. *Valley Forge Christian Coll.*, 454 U.S. 464, 472.

At the state level, i.e., Kentucky, the standard for standing to sue is “a judicially recognizable interest in the subject matter.” *Yeoman v Commonwealth of Kentucky Health Policy Bd.*, 983 S.W. 2d 459, 473 (Ky. 1998). The interest may not be “remote and speculative,” but must be a present and substantial interest in the subject matter. *HealthAmerica Corporation of Kentucky v. Humana Health Plan, Inc.*, 697 S.W.2d 946, 947 (Ky. 1985). Our courts have recognized the difficulty of formulating a precise standard to determine whether a party has standing and held that the issue must be decided on the facts of each case. See *Rose v. Council for Better Education, Inc.*, 790 S.W.2d 186 (Ky. 1989) (a party has standing if he is charged with a statutory duty to promote public education).

For purposes of organization, this Court turns first to examine whether the Secretary of the Justice and Safety Cabinet has standing or capacity to initiate and prosecute the present *in rem* civil action.

(a) Does the Commonwealth, through the Secretary of Justice and Safety Cabinet, have standing to bring this civil forfeiture action?

The Commonwealth alleges that the violation of its criminal laws, i.e., KRS Chapter 528 on Gambling is being flaunted. The Commonwealth's witnesses provided testimony indicating how these domain names relate to multi-faceted transactions completed on-line with casino operators. These casino operators are unidentified and unknown, except by way of their domain names. The Commonwealth pointed out that, based on the WHOIS database, its law enforcement agents have identified who are the registrars with whom the casino operators have registered their domains names. The Commonwealth represented to this Court that, pursuant to the Uniform Domain Name Dispute Resolution Policy established by ICANN, registrars of domains names can cancel, transfer or otherwise make changes to domain name registrations upon receipt of an order from a court of competent jurisdiction requiring such action.

The Opposing Groups and Lawyers questioned the procedural standing of the Secretary of Justice and Safety Cabinet to initiate and prosecute the present suit on behalf of the Commonwealth. According to the IGC, it is the Attorney General, as provided by law who has been given the procedural capacity to bring suits of this nature on behalf of the Commonwealth. KRS 15.020. Since, under KRS 12.270, bringing suits on behalf of the people of the Commonwealth is not included as one of the duties of any cabinet secretary, Justice and Safety Cabinet Secretary Brown is not authorized to bring the present suit.

While the Court is aware that the language of KRS 15.020 vests in the Attorney General the authority to initiate suits on behalf of the Commonwealth, and as legal counsel for the Commonwealth, the Attorney General is the natural state official to seek a vindication of the Commonwealth's sovereign interest, this does not foreclose other competent officials in the Commonwealth having the same procedural capacity as the

Attorney General. We agree with the assertion of the Commonwealth that Governor Steve Beshear, as the chief executive of the state, retains the authority to direct other responsible officers in his Cabinet to bring a suit of this kind before this Court. Moreover, Secretary Brown is the law enforcement official (second only to the Governor) primarily responsible for promoting and preserving justice and safety in the Commonwealth. As such, he is, at least in the instant case, an appropriate and natural choice for bringing the present *in rem* civil action, which is civil forfeiture, not any regular civil suit. The Opposing Groups and Lawyers lose sight of the fact that Secretary Brown is the chief law enforcement officer in the Executive Branch and, notwithstanding his title as Secretary, acts here as the police or sheriff who, in a regular gambling operation, would take actions to seize and forfeit gambling devices. The only difference with a seizure conducted by a regular street cop is that Secretary Brown is dealing with the Internet. The actions remain the same as found in KRS 528.100, 500.090, and 528.010.

Considering the foregoing discussion, the Court is satisfied that the law enforcement interest of the Commonwealth, to curb Internet casino gambling, is a judicially cognizable interest sufficient to bring this suit. The Commonwealth has shown that there was a violation of KRS Chapter 528 that is ongoing. Thus, the Commonwealth's interest is neither remote nor speculative. Secretary Brown, as a law enforcement police officer and duly authorized by Governor Beshear, has the procedural capacity to initiate and prosecute this instant suit on behalf of the Commonwealth. The Attorney General, from a strictly procedural context, is not a real party in interest, nor is he an indispensable party for purposes of proceeding with the instant action.

(b) Do the other entities before this Court have standing?

(i) Standing of PPA, ICA, and NSI

The Commonwealth's counsel zealously argued during hearings held in this case that none of the members of the Opposing Groups and Lawyers have standing to be heard. According to the Commonwealth's counsel, none of the Opposing Groups and Lawyers should be allowed to present arguments in opposition to the Commonwealth's civil forfeiture action.

The representatives of the PPA and the ICA filed their respective written motions for leave from this Court to file memoranda as *amici curiae* or friends of the court, and for the sole purpose of providing the Court background and technical information relating to the Internet and the Domain Name System. Neither the PPA nor the ICA purports to seek any reliefs from this Court.

The PPA and ICA have been and still are permitted to appear before this Court. But, as *amici curiae*, the Court emphasizes that they are not parties to the present *in rem* civil action. The Court, at its own discretion at any time, can withdraw this authority to participate in the proceedings in this case, as the Court sees fit and when their participation would unduly delay or prejudice the adjudication of the rights of the original parties.

The Court treats NSI and its representatives similarly as *amici curiae*, even if the NSI admitted in open court that it was one of the registrars of some (but not all) of the named Defendants 141 Domain Names, and who had been notified of the Seizure Order of September 18, 2008. Until such time that the NSI actually stakes a claim on any of the Defendants 141 Domain Names, the NSI and its representatives will be treated as friends of the Court.

(ii) Standing of IGC and IMEGA

IGC and IMEGA invoke the right of associational standing for the purpose of intervening as a party-defendant in the instant civil forfeiture action. In that capacity, both IGC and IMEGA filed separate motions to dismiss the instant civil forfeiture action.

IGC filed a written motion before this Court to intervene pursuant to CR 24, in a representative capacity and asserting the interests of its members whose domain names were impleaded as party-defendants. IGC seeks to intervene as a matter of right pursuant to CR 24.01, as well as a matter of this Court's discretion pursuant to CR 24.02.

IMEGA, on the other hand, did not file any formal motion to intervene under either CR 24.01 or CR 24.02. This notwithstanding, the Court will treat IMEGA as having filed a motion to intervene under CR 24.01 and 24.02.

Associational standing is the doctrine that allows associations generally to assert claims or defenses on behalf of its members of the association. *Warth v. Seldin*, 422 U.S. 490, 511 (1975). This is called representational standing, as opposed to a situation where an association seek judicial relief from injury to itself and to vindicate whatever rights and immunities the association itself may enjoy. *Id.*

On the federal court level, when an association seeks to bring claims in its representative capacity, the United States Supreme Court applies a 3-part test for determining an association's standing to assert representational claims. In *Washington State Apple Advertising Commission*, 432 U.S. 333 (1977), the United States Supreme Court announced the three-part test as follows:

“[A]n association has standing to bring suit on behalf of its members when: (a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization's purpose and (c) neither the claim asserted nor the relief requested requires the participation of the individual members in the lawsuit.”

In Kentucky, our state courts have had their share of associations invoking associational standing in a representative capacity in order to prosecute a claim, *City of Ashland v. Ashland F.O.P. No. 3, Inc.*, 888 S.W.2d 667 (Ky.,1994) (the association had standing after showing that more than 50% of its members were the aggrieved policemen); pursue an appeal, *Louisville Retail Package Liquor Dealers' Ass'n v. Shearer*. 313 Ky. 316, 231 S.W.2d 47 (Ky.,1950). Unlike the federal courts, however, our rules on associational standing are not as developed. In these cited cases, we only emphasized that the members represented must have a clearly recognizable interest in the dispute or controversy.

Intervention, upon the other hand, is a procedural device through which a person who is not a party to an existing lawsuit is allowed to interject himself into a lawsuit, cutting against the grain of traditional notion that a plaintiff controls his suit. Friedenthal, Miller, Sexton & Hershkoff, *Civil Procedure: Cases and Materials* 652 (9th ed. 2005).

Kentucky's CR 24.01 (intervention as of right) closely follows the language of Federal Rule on Civil Procedure (FRCP) 24. Kurt A. Phillips, Jr., David V. Kramer, & David W. Burleigh, 6 Ky. Prac. R. Civ. Proc. Ann. rule 24.02, (6th ed. 2008). CR 24.02 (permissive intervention), on the other hand, is substantially the same as Federal Rule on Civil Procedure 24(b), respectively. *Id.* Thus, the standards developed on the federal court level are, to an extent, applicable to Kentucky's state courts.

Following the language of CR 24.01, there are four parts of CR 24.01 that must be satisfied in order for an applicant may qualify for intervention as a matter of right. See 6 Ky. Prac. R. Civ. Proc. Ann rule 24.02 (6th ed. 2008), comment §3. These 4 parts are : (1) a timely application is filed by the proposed intervenor, (2) who claims an interest relating to the property or transaction that is the subject of the action, (3) who is so

situated that the disposition of the action may as a practical matter impair or impeded the applicant's ability to protect his or her interest, and (4) his interest is not adequately represented by existing parties. *Id.* In Kentucky, the interest means a significantly protectable interest. *Id.* Moreover, the interest in the proceeding be direct, substantial and legally protectable. *Id.*

Applying the federal three-part test enunciated in *Washington State Apple Advertising Commission* for evaluating standing, the Court does not find IGC or IMEGA to have associational standing for purposes of representing the interests of the purported owners or claimants to the Defendants 141 Domain Names. The present civil forfeiture action involves a determination of the specific rights of persons with interest or claims over each of the Defendants 141 Domain Names. Neither IGC nor IMEGA has shown that the individual participation of their members, whose rights over any of the Defendants 141 Domain Names will be determined at the forfeiture proceeding, is not indispensable for the complete and proper resolution. Accordingly, the third prong of the test for associational standing in *Washington State Apple Advertising Commission* will not be satisfied. The registrants or other persons with an interest in the *res* must present their claims over the seized *res*, if they wish to be fully heard.

Not having associational standing in the matter, neither IGC nor IMEGA may be allowed to intervene as a matter of right. Their absence will not impair or impede none of their legally protectible interests. Neither would permissive intervention be allowed, absent associational standing. Without associational standing, both IGC and IMEGA have no claim to bring before the court for adjudication, save the perspective they bring as lobbyists on the issue of governance of the Internet.

However, like PPA, ICA, and NSI, both IGC and IMEGA will be allowed to continue to present briefs and memoranda for purposes of informing the court of the ever-changing facets of the Internet. In essence, all have friend-of-the-court status. IGC and IMEGA, however, do not have intervenor status.

(iii) Standing of Group of 7 and Group of 2

The lawyers of the Group of 7 and the Group of 2 filed motions to dismiss and motions to vacate or alter the Seizure Order of September 18, 2008. These lawyers manifested to the Court that they represent some (but not all) of the *res*, but without identifying their principals' identities or whether they are representing persons making a claim to or having an interest in the identified *res*.

The Commonwealth's counsel objected to the "standing" of the lawyers of the Group of 7 and the Group of 2 on the ground that they must identify the persons or corporations they represent. The Commonwealth's counsel moved for striking all the motions filed by these attorneys.

The Court finds that striking the motions and pleadings filed by these lawyers of the Group of 7 and the Group of 2 is too harsh a penalty for a lawyer's failure to disclose the identity of his client. Obviously, these domain names could not have engaged the lawyers who purport to appear on their behalf, but they are nonetheless beneficiaries of legal services obtained by another.

Considering, however, that the identity of a lawyer's client is not privileged information, the Court is inclined, as it has already ordered on the bench during the hearings on these lawyers' motion to dismiss and motion to vacate or alter the Seizure Order, to direct said lawyers to disclose to the Court the names and identities of the

persons who engaged them to represent the 9 Defendants Domain Names and to describe the nature of their clients' interest as it relates to the aforementioned *res*.

CONCLUSION AND ORDER

We note that Opposing Groups and Lawyers argue any judicial interference of the Internet will create havoc. This doomsday argument does not ruffle the Court. The Internet, with all its benefits and advantages to modern day commerce and life, is still not above the law, whether on an international or municipal level. The challenge here is to reign in illegal activity and abuse of the Internet within the framework of our nation's and Commonwealth's existing common law norms and principles, until expressed guidelines from state and federal legislative bodies say otherwise.

ACCORDINGLY, IT IS HEREBY ORDERED that further proceedings will be held in the instant civil forfeiture action without delay. Moreover, **IT IS HEREBY ORDERED AND ADJUDGED** as follows:

1. The Motions to Dismiss filed on behalf of the Group of 7, the Group of 2, of Interactive Gaming Council, of Interactive Media Entertainment & Gaming Association, Inc., are all hereby **DENIED**.
2. The Motion of the Interactive Gaming Council to intervene is **DENIED**.
3. The Court's Seizure Order of September 18, 2008 is hereby **AMENDED** so that any of the Defendants 141 Domain Names, their respective registrants or their agent, or any other person with an interest or a claim who, on or before 30 days from entry of this Opinion and Order, installs the applicable software or device, i.e, geographic blocks, which has the capability to block and deny access to their on-line gambling sites through the use of any of the Defendants 141 Domain Names from any users or consumers within the territorial boundaries of the Commonwealth, and reasonably establishes to the

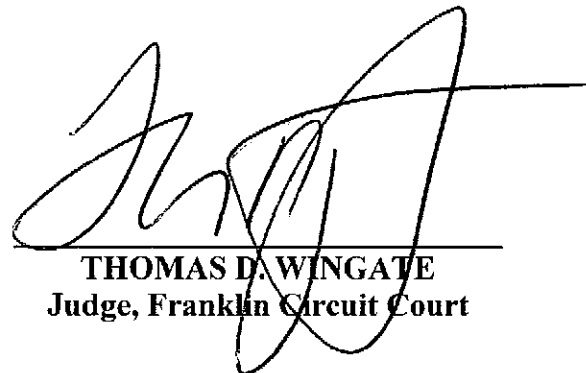
satisfaction of the Kentucky's Justice and Safety Cabinet or this Court that such geographical blocks are operational, shall be relieved from the effects of the Seizure Order and from any further proceedings in the instant civil forfeiture action. The Court acknowledges that *in rem* jurisdiction is not unlimited. Once the domain name is satisfactorily shown as not being used in the Commonwealth for illegal or unlawful gambling, this Court relinquishes jurisdiction.

4. Upon a showing of proof that geographic blocks and/or such other similar software or device have been installed and are operational by any registrant or person with interest over any of the Defendants 141 Domain Names, the COMMONWEALTH is hereby DIRECTED to serve prompt written notice upon the registrar/s and/or registry/ies of the corresponding defendant Internet Domain Name that the Seizure Order, as to the said relevant Internet domain name, has been withdrawn or rescinded.

5. The Court hereby sets the final hearing on forfeiture on the 17th of November 2008, at 10:00 a.m./EST.

6. The Seizure Order of September 18, 2008, REMAINS IN EFFECT as amended by this Order.

SO ORDERED, this 16 day of October 2008.



THOMAS D. WINGATE
Judge, Franklin Circuit Court

ANNEX "1"

LIST OF THE DEFENDANTS 141 DOMAIN NAMES

123bingo.com	fortunejunction.com	redflush.com
777dragon.com	fortuneroom.com	redstarpoker.com
7sultans.com	fulltiltpoker.com	reeferpoker.com
absolutepoker.com	galaxiworld.com	riopartycasino.com
aceshighcasino.com	gamblingboard.com	riverbelle.com
alljackpots.com	goldencasino.com	rivernilecasino.com
allslots.com	goldgatecasino.com	roadhouse reels.com
arthuriancasino.com	goldenpalace.com	royalbetcasino.com
atriumcasino.com	grandmondial.com	royalvegas.com
aztecrichescasino.com	highrollerslounge.com	rushmorecasino.com
bellavegas.com	indiancasino.com	sbgglobal.com
bet21.com	inetbet.com	showdowncasino.com
betroyalcasino.com	itsrealpoker.com	simonsayscasino.com
bigtimebingo.com	ivegas.com	slotfever.com
bingoknights.com	jackpotcapital.com	slotocash.com
bingoville.com	jackpotcity.com	slotsoffortune.com
bingoworkz.com	jackpotkingcasino.com	slotsplus.com
blackjackballroom.com	jackpotwheel.com	sportsbetting.com
bodoglife.com	jupiterclub.com	sportsbook.com
bonuslevelslots.com	kingneptunescasino.com	sportsinteraction.com
bookmaker.com	lakepalace.com	sunpalacecasino.com
bugsysclub.com	lasvegasusacasino.com	sunvegas.com
cakepoker.com	linesmaker.com	superslots.com
capitalcasino.com	luckycoincasino.com	thisisvegas.com
captaincookscasino.com	luckynugget.com	thunderluckcasino.com
caribbeangold.com	lucky pyramidcasino.com	tridentlounge.com
casinobar.com	magicislandcasino.com	truepoker.com
casinoclassic.com	mapau.com	ultimatebet.com
casinoextreme.com	maplecasino.com	usabingo.com
casinofortune.com	miamiparadisecasino.com	vegascasinoonline.com
casinograndbay.com	microgaming.com	vegaslucky.com
casinokingdom.com	mightyslots.com	vegasmagic.com
casinoshare.com	millionairecasino.com	vegaspalms.com
casinous.com	musichallcasino.com	vegasusacasino.com
cirruscasino.com	mysportsbook.com	vegasvilla.com
ukcasinoclub.com	oneclubcasino.com	vicsbingo.com
clubusacasino.com	orbitalcasino.com	viploungecasino.com
cocoacasino.com	orchidcasino.com	virtualcitycasino.com
coolcatcasino.com	paradise8.com	wildjack.com
countycasino.com	phoeniciancasino.com	win4real.com
crazypoker.com	pitbullpoker.com	winabingo.com
crazyvegascasino.com	platinumplay.com	worldwidevegas.com
desperatehousewivesbingo.com	playersonly.com	wsex.com
doylesroom.com	pokerhost.com	yukongoldcasino.com
dsipoker.com	pokerroyaleonline.com	valueactive.com
englishharbour.com	2010 pokerstars 43m	
ezbets.com	pokertime.com	
firstwebcasino.com	powerbet.com	

DISTRIBUTION:

D. Eric Lycan

William H. May III

William C. Hurt, Jr.

Hurt, Crosbie & May, PLLC
127 Main Street
Lexington, KY 40507
Counsel for Plaintiff

Robert M. Foote

Mark Bulgarelli

Foote, Meyers, Mielke & Flowers, LLC
28 North First Street, Suite 2
Geneva, IL 60314
Counsel for Plaintiff

Bruce F. Clark

Stites & Harbison, PLLC
421 West Main Street
Frankfort, KY 40601
Counsel for Interactive Gaming Council

William E. Johnson

Johnson, True & Guarnieri, LLP
326 West Main Street
Frankfort, KY 40601
Counsel for Defendants
playersonly.com; pokerhost.com;
sbglobal.com; sportsbook.com;
sportsinteraction.com;
mysportsbook.com; linesmaker.com)

Kevin Finger

Greenberg Traurig, LLP
77 West Wacker Drive, Suite 500
Chicago, IL 60601
Counsel for Defendants
playersonly.com; pokerhost.com;
sbglobal.com; sportsbook.com;
sportsinteraction.com;
mysportsbook.com; linesmaker.com)

Ian T. Ramsey

Joel T. Beres

Stites & Harbison, PLLC
400 West Market Street
Suite 1800
Louisville, KY 40202
Counsel for Interactive Gaming Council

A. Jeff Ifrah

Jerry Stouch

Greenberg Taurig

2101 L Street, Suite 1000
Washington, DC 20037
Counsel for Interactive Gaming Council

Patrick T. O'Brien

Greenberg Traurig, LLP
401 E. Las Olas Blvd., Suite 2000
Fort Lauderdale, FL 33301
Counsel for Defendants
playersonly.com; pokerhost.com;
sbglobal.com; sportsbook.com;
sportsinteraction.com;
mysportsbook.com; linesmaker.com)

Charles M Pritchett

Joshua T. Rose

Frost Brown Todd LLC
400 West Market Street, 32nd Floor
Louisville, KY 40202
Counsel for Poker Players Alliance

John L. Krieger
Lewis & Roca LLP
c/o Frost Brown Todd LLC
400 West Market Street, 32nd Floor
Louisville, KY 40202
Counsel for Poker Players Alliance

Jon L. Fleischaker
R. Kenyon Meyer
James L. Adams
Dinsmore & Shohl, LLP
1400 PNC Plaza
500 West Jefferson Street
Louisville, KY 40202
Counsel for Interactive Media
Entertainment and Gaming Association

Edward J. Leyden
Hollrah Leyden LLC
1850 K Street, N.W.
International Square, Suite 390
Washington, D.C. 20006
Counsel for Interactive Media
Entertainment and Gaming Association,
Inc.

P. Douglas Barr
Palmer G. Vance II
Alison Lundergran Grimes
Stoll Keenon Ogden PLLC
300 West Vine Street, Suite 2100
Lexington, KY 40507
Counsel for Goldencasion.com,
Goldenpalace.com

John L. Krieger
Lewis & Roca LLP
c/o Frost Brown Todd LLC
400 West Market Street, 32nd Floor
Louisville, KY 40202
Counsel for Poker Players Alliance

Mr. Timothy Hyland
Mr. Micahael R. Mazzoli
600 West Main Street, Suite 300
Louisville, KY 40202
Counsel for Network Solutions, Inc.

Jon L. Fleischaker
R. Kenyon Meyer
James L. Adams
Dinsmore & Shohl, LLP
1400 PNC Plaza
500 West Jefferson Street
Louisville, KY 40202
Counsel for Interactive Media
Entertainment and Gaming Association

Edward J. Leyden
Hollrah Leyden LLC
1850 K Street, N.W.
International Square, Suite 390
Washington, D.C. 20006
Counsel for Interactive Media
Entertainment and Gaming Association,
Inc.

Merrill S. Schell
David A. Calhoun
Wyatt Tarrant & Combs, LLP
500 West Jefferson Street, Suite 2800
Louisville, KY 40202-2898
Counsel for Internet Commerce
Association

P. Douglas Barr
Palmer G. Vance II
Alison Lundergran Grimes
Stoll Keenon Ogden PLLC
300 West Vine Street, Suite 2100
Lexington, KY 40507
Counsel for Goldencasion.com,
Goldenpalace.com

Lawrence G. Walters
Weston, Garrou, Walters & Mooney
781 Douglas Avenue, Almonte Springs,
Florida, 32714
Counsel for Goldenpalace.com

COURT OF APPEALS OF KENTUCKY
NO. 2008-CA-2036
(Related to 2008-CA-2000 and 2008-CA-2019)

VICSBINGO.COM and INTERACTIVE GAMING COUNCIL

PETITIONERS

v.

HONORABLE THOMAS D. WINGATE and
COMMONWEALTH OF KENTUCKY

RESPONDENTS

**AMICUS CURIAE BRIEF OF THE ELECTRONIC FRONTIER FOUNDATION,
THE CENTER FOR DEMOCRACY AND TECHNOLOGY, AND THE
AMERICAN CIVIL LIBERTIES UNION OF KENTUCKY IN SUPPORT OF THE
WRIT PETITION OF PETITIONERS VICSBINGO.COM AND INTERACTIVE
GAMING COUNCIL**

Respectfully submitted,

On the brief:

David A. Friedman, General Counsel
William E. Sharp, Staff Attorney
ACLU of Kentucky
315 Guthrie Street, Suite 300
Louisville, KY 40202
Phone: (502) 581-9746
Fax: (502) 589-9687

Attorneys for Amici Curiae

Matthew Zimmerman, Senior Staff Attorney
Electronic Frontier Foundation
454 Shotwell Street
San, Francisco, CA 94110
Phone: (415) 436-9333 (x127)
Fax: (415) 436-9993

John B. Morris, Jr., General Counsel
Center for Democracy and Technology
1634 I Street NW, Suite 1100
Washington, DC 20006
Phone: (202) 637-9800
Fax: (202) 637-0968

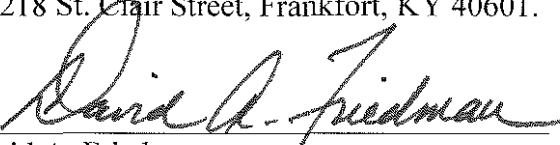
CERTIFICATE OF SERVICE

I hereby certify that I have served copies of this document by mailing copies, first class postage prepaid, on November 12, 2008, to: D. Eric Lycan, William H. May III, William C. Hurt, Jr., HURT, CROSBIE & MAY, PLLC, 127 Main Street, Lexington, KY

(continued on back of cover)

(continued from front of cover)

40507; Robert M. Foote, Mark Bulgarelli, FOOTE, MEYERS, MIELKE & FLOWERS, LLC, 28 N. First Street, Suite 2, Geneva, IL 60134; Lawrence G. Walters, WESTON, GARROU, WALTERS & MOONEY, 781 Douglas Avenue, Altamonte Springs, FL 32714; P. Douglas Barr, Palmer G. Vance II, Alison Lundergan Grimes, STOLL KEENON OGDEN PLLC, 300 W. Vine Street, Suite 2100, Lexington, KY 40507; William E. Johnson, JOHNSON, TRUE & GUARNIERI, LLP, 326 W. Main Street, Frankfort, KY 40601; John L. Krieger, Anthony Cabot, LEWIS & ROCA LLP, 3993 Howard Hughes Parkway, Suite 600, Las Vegas, NV 89169; Patrick T. O'Brien, GREENBERG TRAURIG, LLP, 401 E. Las Osas Blvd., Suite 2000, Ft. Lauderdale, FL 33301; Kevin D. Finger, Paul D. McGrady, GREENBERG TRAURIG, LLP, 77 W. Wacker Drive, Suite 2500, Chicago, IL 60601; Timothy B. Hyland, STEIN, SPURLING, BENNETT, DE JONG, DRISCOLL & GREENFEIG, P.C., 25 W. Middle Lane, Rockville, MD 20850; Michael R. Mazzoli, COX & MAZZOLI, 600 W. Main Street, Suite 300, Louisville, KY 40202; Merrill S. Schell, David A. Calhoun, WYATT, TARRANT & COMBS, LLP, 500 W. Jefferson Street, Suite 2800, Louisville, KY 40202; Phillips S. Corwin, Ryan D. Israel, BUTERA & ANDREWS, 1301 Pennsylvania Avenue, N.W., Suite 500, Washington, DC 20004; John L. Tate, Ian T. Ramsey, Joel T. Beres, STITES & HARBISON, PLLC, 400 W. Market Street, Suite 1800, Louisville, KY 40202; Bruce F. Clark, STITES & HARBISON, PLLC, 421 W. Main Street, P. O. Box 634, Frankfort, KY 40602-0634; A. Jeff Ifrah, Jerry Stouck, GREENBERG TRAURIG, LLP, 2101 L Street, NW, Suite 1000, Washington, DC 20037; and Hon. Thomas D. Wingate, Franklin Circuit Court, 218 St. Clair Street, Frankfort, KY 40601.


David A. Friedman

STATEMENT OF POINTS AND AUTHORITIES

I. INTRODUCTION	1
II. BACKGROUND	1
http://en.wikipedia.org/wiki/Website	2
<i>Register.com, Inc. v. Verio, Inc.</i> , 356 F.3d 393 (2d Cir. 2004).....	2
<i>Peterson v. National Telecommunications and Information Admin.</i> , 478 F.3d 626 (4th Cir. 2007)	2
http://en.wikipedia.org/wiki/Domain_name_system	2
<i>Name.Space, Inc. v. Network Solutions, Inc.</i> , 202 F.3d 573 (2d Cir. 2000).....	2
III. ARGUMENT	3
A. The Trial Court’s Order is Overbroad and Would Infringe the First Amendment Interests of the Domain Name Owners as Well as the Public at Large.....	3
<i>Tory v. Cochran</i> , 544 U.S. 734 (2005)	4
<i>Carroll v. President and Comm’rs of Princess Anne</i> , 393 U.S. 175 (1968).....	4
<i>Madsen v. Feminist Women’s Health Clinic</i> , 512 U.S. 753 (1994).....	4
George C.C. Chen, “A Cyberspace Perspective on Governance, Standards and Control,” 16 J. Marshall J. Computer & Info. L. 77 (Fall 1997).....	5
<i>Shell Trademark Mgmt. BV v. Canadian AMOCO</i> , No. 02-01365, 2002 U.S. Dist. LEXIS 9597 (N.D. Cal. May 21, 2002)	5
<i>Organization for a Better Austin v. Keefe</i> , 402 U.S. 415 (1971).....	5
<i>Nebraska Press Ass’n v. Stuart</i> , 427 U.S. 539 (1976)	5

<i>Center for Democracy & Technology v. Pappert</i> , 337 F.Supp.2d 606 (E.D. Pa. 2004)	5
<i>Vance v. Universal Amusement Co.</i> , 445 U.S. 308 (1980)	5
<i>Martin v. City of Struthers</i> , 319 U.S. 141 (1943)	6
<i>Board of Education v. Pico</i> , 457 U.S. 853 (1982)	6
<i>Kleindienst v. Mandel</i> , 408 U.S. 753 (1972).....	6
<i>Red Lion Broadcasting Co. v. F.C.C.</i> , 395 U.S. 367 (1969)	6
<i>Stanley v. Georgia</i> , 394 U.S. 557 (1969).....	6
<i>Lamont v. Postmaster General</i> , 381 U.S. 301 (1965).....	6
<i>Clement v. California Dept. of Corrections</i> , 364 F.3d 1148 (9 th Cir. 2004)	6
<i>Reno v. ACLU</i> , 521 U.S. 844 (1997).....	6, 7
<i>Taubman Co. v. Webfeats</i> , 319 F.3d 770 (6 th Cir. 2003)	6-7
<i>Central Hudson Gas & Elec. Corp. v. Public Serv. Comm’n</i> , 447 U.S. 557 (1980).....	7
<i>Schneider v. New Jersey</i> , 308 U.S. 147 (1939).....	7
<i>Southeastern Promotions, Ltd. V. Conrad</i> , 420 U.S. 546 (1975)	8
<i>Elrod v. Burns</i> , 427 U.S. 347 (1976)	8
B. A Geolocation Filtering Requirement Could Dramatically Increase the Cost of Operating a Website, Likely Driving a Significant Number of Sites Out of Business Worldwide.....	8
<i>American Civil Liberties Union v. Gonzales</i> , 478 F.Supp.2d 775 (E.D. Pa. 2007)	9, 10
http://www.anonymize.com	9
http://www.torproject.com	9

Bamba Gueye, <i>et al.</i> , “Investigating the Imprecision of IP Block-Based Geolocation” (2007), available at http://www.nas.ewi.tudelft.nl/people/Steve/papers/Geolocation-pam07.pdf	9
Netcraft.com 2008 Web Server Survey, available at http://news.netcraft.com/archives/2008/10/29/october_2008_web_server_survey.html	10
C. The Trial Court’s Order Violates the Commerce Clause	10
U.S. Const., art. I, § 8.....	11
<i>American Library Association v. Pataki</i> , 969 F. Supp. 160 (S.D.N.Y. 1997).....	11
<i>Cyberspace Communications, Inc. v. Engler</i> , 55 F.Supp.2d 737 (E.D. Mich. 1999), <i>aff’d</i> , 238 F.3d 420 (6 th Cir. 2000).....	11
31 U.S.C. § 5361 <i>et seq.</i>	11
31 U.S.C. § 5361(b)	11
31 U.S.C. § 5362(10)(D)(ii).....	11
Decision, World Trade Organization, WT/DS285/R (“United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services”), Nov. 10, 2004, available at http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm	12
<i>Yahoo! Inc. v. LaLigue Contre Le Racisms et L’Antisemitisme</i> , 433 F.3d 1199 (9 th Cir. 2006)	12
D. The Trial Court Has Not Established – and Cannot Establish – That It Has Jurisdiction Over Domain Name Registrars Outside of Kentucky	13
<i>Shaffer v. Heitner</i> , 433 U.S. 186 (1977)	13
<i>International Shoe v. Washington</i> , 326 U.S. 310 (1945)	13, 14
KRS § 454.210.....	13, 14

<i>Burger King Corp. v. Rudzewicz</i> , 471 U.S. 462 (1985).....	14
<i>Davis H. Elliot Co. v. Caribbean Utilities Co.</i> , 513 F.2d 1176 (6 th Cir. 1975)	14
<i>Auto Channel, Inc. v. Speedvision Network, LLC</i> , 995 F. Supp. 761 (W.D. Ky. 1997).....	14
GoDaddy.com’s “Uniform Domain Name Dispute Resolution Policy” at http://www.godaddy.com/gdshop.legal_agreements/ show_doc.asp?plvid=1&pageid=uniform_domain	14
IV. CONCLUSION	15

I. INTRODUCTION

Amici curiae the Electronic Frontier Foundation (“EFF”), the Center for Democracy and Technology (“CDT”), and the American Civil Liberties Union of Kentucky (“ACLU of Kentucky”) respectfully urge this Court to grant Viscbingo.com and the Interactive Gaming Council (“IGC”)’s Writ Petition of October 28, 2008, and vacate the trial court’s Order of October 16, 2008, which purported to seize the domain names of 141 Internet domain names pointing to websites operating on Internet web servers around the globe. Judge Wingate’s Order (a) raises serious First Amendment concerns, (b) violates the Commerce Clause of the U.S. Constitution, and (c) is otherwise unenforceable as the trial court does not have jurisdiction over the domain name registrars who were ordered to transfer the domain names at issue. If allowed to stand, the Court’s flawed Order would needlessly create uncertainty about the basic rules governing the operation of the Internet as well as the authority of courts both inside and outside of the United States to affect behavior in other jurisdictions. Moreover, if carried to its logical conclusion, the trial court’s Order could well impose literally billions of dollars of additional costs on individuals and businesses throughout the world that have no significant contacts with Kentucky. *Amici* take no position on the substance or legality of the gambling websites that would be affected by the domain name seizure but instead file this brief to underscore the Order’s lack of merit as well as the substantial damage that would result from Judge Wingate’s flawed central premise – that website operators the world over have an affirmative duty to block visitors from visiting their sites on the basis of local rules, and that Kentucky courts can reach outside the state’s borders to seize the domain names of entities that do not comply with this edict.

II. BACKGROUND

On October 16, 2008, Franklin Circuit Court Judge Wingate affirmed his previous Order of September 18, 2008, which ordered the seizure of over 100 Internet domain names that purportedly (a) constituted illegal “gambling devices” prohibited by Kentucky

law, and (b) that refused to impose “geographic blocks” to prevent Internet users in Kentucky from accessing any of the material on the sites to which the domain names currently point. *See* Order at 39-40. As discussed below, Judge Wingate’s Order is not only unconstitutional and unlawful but also rests on incorrect factual assumptions.

As Petitioners explain, the distinctions between “websites,” “IP addresses,” and “domain names” are critical to the proper application of the law here. A “website” is “a collection of Web pages, images, videos or other digital assets that is hosted on one or more web servers.”¹ An “IP address” is a unique, numerical number – like “89.2.164.31” or “222.34.1.4” – assigned to every web server or other computer connected to the Internet that functions much like a street address or telephone number for the computer to which it is assigned.² A domain name is an easy-to-remember alphanumeric text representation (often a word or phrase) that is linked through the “domain name system” to the numeric IP Address where a website is actually located.³ A series of domain name servers contain massive databases, listing the proper IP address for each domain name.⁴

Thus, to analogize to the “real world,” a website is akin to a building, such as the Grand Theater in Frankfort. An IP address is like the address of the building, “308 St. Clair Street, Frankfort, KY,” while the domain name is the commonly known way to refer to the building – the words “Grand Theater” in this example. Finally, the “domain name system” is like a “Yellow Pages” directory that one can use to look up “Grand Theater” and learn that it is located at “308 St. Clair Street, Frankfort, KY.” Both “Grand

¹ *See* “Website.” Wikipedia. November 10, 2008. <<http://en.wikipedia.org/wiki/Website>>.

² *See Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 409-410 (2d Cir. 2004). *See also* Writ Petition of Vicsbingo.com and Interactive Gaming Council of October 28, 2008 (“Writ Petition”) at 21.

³ *See Register.com, Inc.*, 356 F.3d at 410; Writ Petition at 21. *See also Peterson v. National Telecommunications and Information Admin.*, 478 F.3d 626, 629 (4th Cir. 2007) (describing domain name system) and “Domain Name System.” Wikipedia. November 10, 2008. <http://en.wikipedia.org/wiki/Domain_name_system>.

⁴ *See Name.Space, Inc. v. Network Solutions, Inc.*, 202 F.3d 573, 577 (2d Cir. 2000) (describing the domain name server system in detail).

Theater” and “308 St. Clair St., Frankfort, KY” accurately refer to the same building in different ways, but one is easier for humans to remember.

The court’s seizure of the domain names in this case is akin to ordering the Yellow Pages company to erase the accurate listing for “Grand Theater” (which points visitors to “308 St. Clair St., Frankfort, KY”) and instead point visitors to a different address. Although this misdirection may be of little consequence to those who know their way around Frankfort, it is of huge consequence on the Internet, where there are literally billions of different web pages and the “addresses” are in numeric forms (such as “216.97.231.225” or “205.204.132.139”) that have no meaning to most human visitors. An accurate appreciation of what domain names are and how they function is important to understand the First Amendment and Commerce Clause implications of the court ordering the seizure of domain names.

III. ARGUMENT

A. The Trial Court’s Order is Overbroad and Would Infringe the First Amendment Interests of the Domain Name Owners as Well As the Public at Large.

Any order purporting to transfer domain name registrations from registrants to the Commonwealth of Kentucky raises serious First Amendment concerns because it would necessarily impede access to material that is legal not only in Kentucky but throughout the country and the world. Moreover, it would chill speech of all types, not simply the speech directly at issue in this case.

As conceived by Judge Wingate, domain names would be subject to seizure – and therefore can be disabled so that they will no longer correctly correlate to their respective intended sites’ IP address – if the site enables behavior that is arguably illegal in Kentucky but may be legal elsewhere. Conversely, the court noted that for any of the domain names at issue “which are providing information only, the Seizure Order must be appropriately rescinded” (but even then the court placed the burden on the domain name owners to prove these facts at a forfeiture hearing). Such a ruling turns First Amendment

protections on their head. Third-parties who may wish to access such (legal) information, including *amici* and their constituents, would be prohibited from doing so if the court's Order is not rescinded.

Critically, there is nothing in the court's analysis that would limit its application to gambling domains. Under the court's theory, Kentucky would be able to seize *any* domain name, from anywhere in the world, that pointed to a website that Kentucky deemed to violate a local law. The court's jurisdictional theory literally puts speakers and publishers the world over – not to mention those who otherwise provide information regarding the location of sites on the Internet, such as by simply linking to them – at risk. The trial court's global reach for extra-territorial jurisdiction over the Internet cannot withstand First Amendment scrutiny.

First, as discussed above, “domain names” are nothing more than alphanumeric text representations that point to the IP addresses of the computer servers that host websites (like a phone book, which correlates a person's name with a phone number, or a map, which provides directions to a particular street address). Because the seizure Order demanded the transfer of domain name control, it implicates the ability of Internet users to access *any* of the content on the websites to which those domain names point, not just to the content to which the Commonwealth of Kentucky (and the trial court) object. For this reason alone, the Order is massively overbroad and unconstitutional. *See, e.g., Tory v. Cochran*, 544 U.S. 734, 736 (2005) (citing *Carroll v. President and Comm'rs of Princess Anne*, 393 U.S. 175, 183-84 (1968), for the proposition that an “order” issued in “the area of First Amendment rights” must be “precis[e]” and narrowly “tailored” to achieve the “pin-pointed objective” of the “needs of the case”); *Madsen v. Feminist Women's Health Clinic*, 512 U.S. 753, 765-66 (1994) (injunction may burden no more speech than necessary).

Second, regardless of whether domain names constitute “property” or not, the trial court's Order was based purely on the truthful speech inherent in the domain names in

question. Hardly amounting to “virtual keys for entering and creating” allegedly illegal materials (Order at 23), domain names are more accurately conceived of as maps or street signs, providing factual information regarding the location – the unique IP address – associated with a computer server. *See, e.g.,* George C.C. Chen, *A Cyberspace Perspective on Governance, Standards and Control*, 16 J. Marshall J. Computer & Info. L. 77, 113 (1997) (“The domain name is similar to a street sign in the real world, indicating the location of the Internet merchant and the nature of his business.”); *Shell Trademark Mgmt. BV v. Canadian AMOCO*, No. 02-01365, 2002 U.S. Dist. LEXIS 9597, at *10-11 (N.D. Cal. May 21, 2002) (analogizing domain names to road signs).

As the court’s Order targets the domain names at issue solely because of the truthful content of the speech contained in the domain name registry (the identification of a corresponding IP address), it is no different from a hypothetical order prohibiting domain name registrars from passing out leaflets telling potential viewers how to access the sites in question. That plainly would violate the First Amendment (*Organization for a Better Austin v. Keefe*, 402 U.S. 415 (1971)), and so does the trial court’s Order here. Accordingly, like the injunction against leafleting overturned in *Organization for a Better Austin*, a seizure Order rendering the domain name inoperable would be a classic prior restraint, “the most serious and the least tolerable infringement on First Amendment rights.” *Nebraska Press Ass’n v. Stuart*, 427 U.S. 539, 559 (1976).

Moreover, because content on an Internet server can readily be changed, the permanent seizure of a domain name continues to impede access to speech even if the content changes so that it no longer violates any Kentucky law. *See, e.g., Center For Democracy & Technology v. Pappert*, 337 F. Supp. 2d 606, 657 (E.D. Pa. 2004) (holding that statute requiring the blocking of access to particular domain names and that IP addresses be blocked amounted to an unconstitutional prior restraint (citing *Vance v. Universal Amusement Co.*, 445 U.S. 308 (1980) (overturning a permanent injunction against a movie theater))).

Not only are the First Amendment rights of domain name registrars harmed by the seizure of domain names on the ground that they point to foreign websites where the content of those sites is legal, the First Amendment rights of Internet users are affected as well. As the Supreme Court has repeatedly held, the First Amendment not only “embraces the right to distribute literature,” it also “necessarily protects the right to receive it.” *Martin v. City of Struthers*, 319 U.S. 141, 143 (1943); *accord Board of Education v. Pico*, 457 U.S. 853, 867 (1982) (“the right to receive ideas is a necessary predicate to the *recipient’s* meaningful exercise of his own rights of speech, press, and political freedom”) (emphasis in original); *Kleindienst v. Mandel*, 408 U.S. 753, 762 (1972) (First Amendment encompasses “right to receive information and ideas”); *Red Lion Broadcasting Co. v. F.C.C.*, 395 U.S. 367, 390 (1969) (“It is the right of the public to receive suitable access to social, political, esthetic, moral, and other ideas and experiences which is crucial here. That right may not constitutionally be abridged ...”); *Stanley v. Georgia*, 394 U.S. 557, 564 (1969) (“It is now well established that the Constitution protects the right to receive information and ideas”); *Lamont v. Postmaster General*, 381 U.S. 301, 308 (1965) (“The dissemination of ideas can accomplish nothing if otherwise willing addressees are not free to receive and consider them. It would be a barren marketplace of ideas that had only sellers and no buyers”) (Brennan, J., concurring).

This Constitutional right to receive information applies specifically to information disseminated over the Internet. *See, e.g., Clement v. California Dept. of Corrections*, 364 F.3d 1148, 1150 (9th Cir. 2004) (holding that alleged that Pelican Bay State Prison violated the First Amendment rights of an inmate by prohibiting inmates from receiving material downloaded from the Internet); *Reno v. ACLU*, 521 U.S. 844, 874 (1997) (invalidating law that restricted adults’ right to access information on the Internet). Indeed, the First Amendment protection for Internet speech applies specifically to domain names themselves. *Taubman Co. v. Webfeats*, 319 F.3d 770, 778 (6th Cir. 2003) (“the

domain name is a type of public expression, no different in scope than a billboard or a pulpit”). Accordingly, the trial court’s overbroad seizure Order compelling domain name registrars to transfer domain names to the Commonwealth of Kentucky implicates the First Amendment interests of the general public in receiving documents and information through the use of the identified domain names to find the IP addresses of particular businesses.

The Justice and Public Safety Cabinet may assert that some or all of the documents and information available through the targeted domain names remain available to the public using foreign domain names other than those at issue here, or by typing in the site’s IP addresses directly. However, this merely proves the pointlessness of, and thus the lack of constitutionally adequate justification for, the court’s blunt seizure Order. *See, e.g., Central Hudson Gas & Elec. Corp. v. Public Serv. Comm’n*, 447 U.S. 557, 564 (1980) (law that restricts speech “may not be sustained if it provides only ineffective or remote support for the government’s purpose”).

Nor can the availability of alternate routes to the websites at issue compromise *amici*’s First Amendment rights in obtaining access to those sites through the specific domain names here. The Supreme Court has repeatedly held that “one is not to have the exercise of his liberty of expression in appropriate places abridged on the plea that it may be exercised elsewhere.” *Schneider v. New Jersey*, 308 U.S. 147, 163 (1939); *accord Reno v. ACLU*, 521 U.S. 844, 879-80 (1997) (rejecting the government’s contention that content-based restriction on speech in numerous Internet modalities was permissible because the law allowed a “reasonable opportunity” for such speech to occur elsewhere on the Internet; citing *Schneider*, the Court noted that “[t]he Government’s position is equivalent to arguing that a statute could ban leaflets on certain subjects as long as individuals are free to publish books.”); *Va. State Bd. of Pharmacy*, 425 U.S. at 757 n.15 (“We are aware of no general principle that the freedom of speech may be abridged when the speaker’s listeners could come by his message by some other means . . .”);

Southeastern Promotions, Ltd. v. Conrad, 420 U.S. 546, 556 (1975) (holding an otherwise impermissible prior restraint against performance of musical “Hair” is not saved by availability of other forums for production). It is equally immaterial if the seizure order’s only effect was to delay, rather than completely frustrate, access to the corresponding websites. *See Elrod v. Burns*, 427 U.S. 347, 373 (1976) (“The loss of First Amendment freedoms, even for minimal periods of time, constitutes irreparable injury”).

B. A Geolocation Filtering Requirement Could Dramatically Increase the Cost of Operating a Website, Likely Driving a Significant Numbers of Sites Out of Business Worldwide.

The First Amendment deficiencies of the court’s Order are in no way avoided by the additional imposition of an alternative Internet-wide “geographic filtering” requirement; indeed, the requirement compounds the problem. Not only does the requirement run afoul of the Commerce Clause (as discussed below), it would impose enormous and chilling burdens on lawful websites around the world. And in any event, the “geographic filtering” technology simply does not work well enough to afford any website legal protection from the asserted long arm of the Kentucky trial court.

In its Order, the court makes the remarkable assertion that the 141 Domain Names have been “designed” to reach Kentucky residents because the owners of those domain names could, if they “so chose,” “filter, block and deny access to a website on the basis of geographic locations.” Order at 24. “There are software that are available, which can provide filtering functions on the basis of geographical location, *i.e.*, geographical blocks.” *Id.* No evidence is cited to support the court’s findings or its striking conclusion that every operator of every website that fails to filter by location therefore affirmatively “targets” Internet users in Kentucky or consequently that the domain names used by such operators may be subject to seizure in every jurisdiction worldwide.

Even a cursory examination of factual findings by other courts cast serious doubt’s on the trial court’s theory and strongly indicates that server-side filtering is not a realistic option with which to comply with such a legal mandate:

• Filtering is not 100% accurate. First, due to the nature of various methods of connecting to the Internet (including, but not limited to, proxy servers, satellite connections, and other large corporate proxies), it is simply not possible to guarantee that website visitors are from a particular city, state, or even country. See, e.g., *American Civil Liberties Union v. Gonzales*, 478 F. Supp. 2d 775, 807 (E.D. Pa. 2007) (“A product that Quova markets can determine, within a 20 to 30 mile radius, the location from which a user is accessing a Web site through a proxy server, satellite connection, or large corporate proxy. ... The fact that Quova can only narrow down a user’s location to a 20 to 30 mile radius results in Quova being unable to determine with 100 percent accuracy which side of a city or state border a user lives on if the user lives close to city or state borders.”) (internal citations omitted). In addition, the ability to “geo-locate” users of large Internet service providers (“ISPs”) like AOL drops even further because these ISPs route traffic through centralized proxies that identify the source of browser requests not as the location of the individual Internet user but as the location of the proxy server itself, which may or may not be anywhere close to the Internet user. See, e.g., *id.* (“If a visitor is accessing a Web site through AOL, Quova can only determine whether the person is on the East or West coast of the United States.”).⁵

Moreover, the ability to accurately identify the geographic location of users is further diminished by the growing use of anonymizing proxy services such as those provided by companies by anonymize.com and by peer-to-peer technologies such as Tor. See, e.g., Anonymize.com (located at <http://www.anonymize.com>), Tor (located at <http://www.torproject.com>). Using these services, it is trivially easy for a user in Kentucky to evade any “geolocation filtering” a website might use, and thus no website can confidently use such services to prevent access from Kentucky.

⁵ Bamba Gueye, *et. al.*, *Investigating the Imprecision of IP Block-Based Geolocation*, in *Lecture Notes in Computer Science* Vol. 4427 237, 240 (Springer Berlin, Heidelberg 2007) available at <http://www.nas.ewi.tudelft.nl/people/Steve/papers/Geolocation-pam07.pdf> (finding “large geolocation errors” in technology that claimed to be able to identify the location of Internet users).

• Filtering would impose significant cost on website operators. Critically, the location services that the trial court asserts can be used are *not* built into the Internet or available to all websites. On the contrary, they are very expensive. One service that provides geolocation services, recently cited by the Eastern District of Pennsylvania, estimated that the cost of such services “can cost anywhere from \$6,000 to \$500,000 a year.” *ACLU v. Gonzales*, 478 F.Supp.2d at 807.

Applying the court’s analysis to its logical conclusion – that every operator of every website in the world may be found liable for infractions of local laws even though the site material may be legal in the jurisdiction(s) in which the operator, server, and domain name registrar are located – dramatically increases the sites’ ongoing operational costs. Apart from the starkly higher legal compliance costs that such a rule would impose (associated with determining which laws of which of the world’s 195 countries might apply to a given site’s content), the collective cost associated with the technological implementation of such filters could – conservatively – be in the tens of billions of dollars *per year* (and this figure assumes that only 10% of world’s active websites⁶ used the service and the average annual total of *all* implementation costs was equal to the lowest amount cited above for the cost of the filtering technology alone). Given the percentage of small and/or non-commercial sites on the Internet whose owners would likely find a mandate to filter browsers from every jurisdiction in the world that may argue that the sites’ content is illegal where it is viewed, the global makeup of Internet content would be invariably changed for the worse.

C. The Trial Court’s Order Violates the Commerce Clause.

Under the trial Court’s overly expansive jurisdictional theory, Kentucky courts would be authorized to seize any Internet domain name that linked to content deemed illegal under Kentucky law. Kentucky thus would be able to globally disable any

⁶ See, e.g., Netcraft.com 2008 Web Server Survey, available at http://news.netcraft.com/archives/2008/10/29/october_2008_web_server_survey.html, estimating that the number of active websites in the world is currently over 65 million.

website, thereby imposing its laws on the other 49 states and on the rest of the world. The Commerce Clause of the U.S. Constitution will not tolerate this exertion of authority, because it prohibits individual states from regulating “Commerce with foreign Nations, and among the several States.” U.S. Const. art. I, § 8. By authorizing the seizure of domain names, the Commonwealth and trial court are attempting to do just that – regulate interstate and foreign commerce.

In one of the leading cases applying the Commerce Clause to the Internet, a federal district court explained:

The courts have long recognized that certain types of commerce demand consistent treatment and are therefore susceptible to regulation only on a national level. *The Internet represents one of those areas*; effective regulation will require national, and more likely global, cooperation. Regulation by any single state can only result in chaos, because at least some states will likely enact laws subjecting Internet users to conflicting obligations. Without the limitations imposed by the Commerce Clause, these inconsistent regulatory schemes could paralyze the development of the Internet altogether.

American Library Association v. Pataki, 969 F. Supp. 160, 181 (S.D.N.Y. 1997) (emphasis added). Numerous cases across the country have applied the Commerce Clause to strike down attempted state burdens on Internet communications. *See, e.g., Cyberspace Communications, Inc. v. Engler*, 55 F. Supp. 2d. 737, 752 (E.D. Mich. 1999), *aff’d*, 238 F.3d 420 (6th Cir. 2000) (finding Commerce Clause violation because state regulation “would subject the Internet to inconsistent regulations across the nation”).

Congress has legislated in the area of Internet gambling, *see* 31 U.S.C. § 5361 *et seq.*, but it specifically did not empower the states to regulate Internet gambling. *See id.* §§ 5361(b), 5262(10)(D)(ii) (neither extending nor preempting state laws). Thus, any state regulation of Internet gambling that has any impact outside of the state (as almost all Internet regulations would) is governed pursuant to an ordinary Commerce Clause analysis. And under the Commerce Clause, it is simply not permissible for Kentucky to prohibit access by residents of Las Vegas, for example, to access a site that is lawful in Nevada. Yet the trial court’s Order represents just such an exertion of authority.

Beyond the interstate implications of a Kentucky seizure of domain names, such action would directly implicate the United States' foreign relations with the rest of the world, a subject that the Commerce Clause specifically reserves to the national government. Indeed, the United States has *already* been penalized by the global World Trade Organization for its discriminatory treatment of online gambling (in which some forms of gambling are permitted and some are not). *See* Decision, World Trade Organization, WT/DS285/R ("United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services"), Nov. 10, 2004 (available at http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm). An action by Kentucky to disable *global* access to *any* domain name (gambling or otherwise) would have a direct and concrete impact on the United States' trade and diplomatic relations with the rest of the world.

This Commerce Clause analysis connects directly to the free speech and civil liberties concerns discussed above. While the Kentucky trial court may attempt to seize domain names for alleged violations of local gambling regulations, other countries (ones that do not enjoy First Amendment protections) may choose to seize the domain names of foreign websites based (for example) solely on their expressive content. China, for example, may be very happy to follow Kentucky's lead by seizing the domain names of U.S. websites that promote religions that China bans. Even Western nations such as France have attempted to censor U.S.-located content that is completely lawful and constitutionally protected in this country. *See, e.g., Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 433 F.3d 1199 (9th Cir. 2006) (case arising out of France's efforts to censor content on Yahoo.com). Under the trial court's jurisdictional theory, the French court in the *Yahoo!* case would not need to take action directly against the Yahoo! company (as the French in fact did) – instead, it would simply seize the "yahoo.com" domain name. While the trial court may believe that the impact of its Order is limited,

the principle it articulates is one that threatens to undermine crucial legal principles that have prevented jurisdictions from attempting to assert such authority in the past.

D. The Trial Court Has Not Established – and Cannot Establish – That It Has Jurisdiction Over Domain Name Registrars Outside of Kentucky.

The trial court's Order is further deficient in that the court failed to consider – and indeed does not have – jurisdiction over the registrars, the entities with which the owners registered their domain names. While the trial court held that minimum contacts existed between Kentucky and the owners of the sites to which all 141 domain names direct Internet browsers (*see* Order at 19-21) (a dubious finding that the Petitioners properly challenge), the court never opined on any minimum contacts with the registrars themselves, the entities who received the court's Order to transfer the domain names.

The trial court purported to seize domain names pursuant to *in rem* jurisdiction over the domain names themselves (authority effectively contested by Petitioners in their writ application (*see* Writ Petition at 9-13)), but the seizure Order is necessarily directed at out-of-state registrars, *i.e.*, entities over which the court must have *in personam* jurisdiction. *See, e.g., Shaffer v. Heitner*, 433 U.S. 186, 207 (1977) (“[I]n order to justify an exercise of jurisdiction *in rem*, the basis for jurisdiction must be sufficient to justify exercising ‘jurisdiction over the interests of persons in a thing.’”). And while the court perhaps concludes (indirectly) that its exercise of personal jurisdiction over out-of-state registrars would satisfy the “minimum contacts” test mandated by the Due Process Clause as articulated by the Supreme Court in *International Shoe v. Washington*, 326 U.S. 310 (1945), it makes no explicit findings to that effect, and it further fails to cite any *statutory* authority that would grant Kentucky courts the authority to exercise jurisdiction to the full extent permissible under the Due Process clause.

Pursuant to Kentucky's long-arm statute, no such jurisdiction exists. Under KRS § 454.210, a court may only exercise long-arm jurisdiction against tort-feasors, under certain circumstances, and “only a claim arising from acts enumerated in this section may

be asserted against him.” KRS § 454.210(2)(b). No explicit statutory authorization exists to assert personal jurisdiction over foreign domain name registrars solely because they may “purposefully avail[] [themselves] of the privilege of conducting activities” within Kentucky (*see Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 475 (1985)); rather, the legislature must affirmatively grant that authority. *See, e.g., Davis H. Elliot Co. v. Caribbean Utilities Co.*, 513 F.2d 1176, 1179 (6th Cir. 1975) (applying Kentucky law) (“The basic inquiry as to the validity of asserted *in personam* jurisdiction is a two-fold one which requires (1) a determination of whether the state legislature has authorized the courts of the state to exercise jurisdiction over the nonresident in question, and (2) a determination of whether the jurisdiction so authorized is consistent with Fourteenth Amendment due process as that concept is delineated in the ‘minimum contacts’ formula of *International Shoe Co. v. Washington ...*”); *Auto Channel, Inc. v. Speedvision Network, LLC*, 995 F. Supp. 761, 764 fn. 3 (W.D. Ky. 1997) (“The fact that the requirements of K.R.S. 454.210(2)(a) are theoretically satisfied by the same minimum contacts required by due process should not be taken to mean that the long-arm statute is superfluous ... [I]t is possible to decline jurisdiction based only on the language of the statute, without recourse to a due process analysis.”).

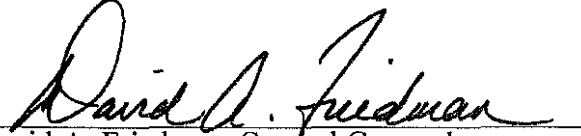
As it was not authorized by any Kentucky statute, the trial court’s seizure Order is *ultra vires* and unenforceable, regardless of whether or not any out-of-state registrar complied with it.⁷

⁷ As the trial court did not have jurisdiction over the domain name registrars that it purportedly “ordered” to transfer the domain names in question, registrars that complied with the court’s Order, in whole or in part, may have violated their contractual obligations to their domain name customers. *See, e.g.,* GoDaddy.com’s “Uniform Domain Name Dispute Resolution Policy” at <http://www.godaddy.com/gdshop/legal_agreements/show_doc.asp?plvid=1&pageid=uniform_domain> (“We will cancel, transfer or otherwise make changes to domain name registrations under the following circumstances: [including] our receipt of an order from a court or arbitral tribunal, in each case of competent jurisdiction, requiring such action. ... We will not cancel, transfer, activate, deactivate, or otherwise change the status of any domain name registration under this Policy except as provided ... above.”) (emphasis added).

IV. CONCLUSION

The trial court's Order of October 16, 2008, purporting to seize the domain names associated with over 100 websites was, quite simply, unconstitutional and made without jurisdictional authority. *Amici* strongly urge this Court to vacate the trial court's Order, and order the Franklin Circuit Court to dismiss the case for lack of jurisdiction, and that the Circuit Court be directed to take those steps necessary to return the parties, and the domain names, to the status quo prior to the trial court litigation.

Respectfully submitted,



David A. Friedman, General Counsel
William E. Sharp, Staff Attorney
ACLU of Kentucky
315 Guthrie Street, Suite 300
Louisville, KY 40202
Phone: (502) 581-9746
Fax: (502) 589-9687
Email: dfriedman@ffgklaw.com

On the brief:

Matthew Zimmerman
Senior Staff Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
Phone: (415) 436-9333 (x127)
Fax: (415) 436-9993
Email: mattz@eff.org

John B. Morris, Jr.
General Counsel
Center for Democracy and Technology
1634 I Street NW, Suite 1100
Washington, DC 20006
Phone: (202) 637-9800
Fax: (202) 637-0968 fax
Email: jmorris@cdt.org

Attorneys for Amici Curiae



Commonwealth of Kentucky

Court of Appeals

NO. 2008-CA-002000-OA

INTERACTIVE MEDIA
ENTERTAINMENT AND
GAMING ASSOCIATION, INC.

PETITIONER

v. AN ORIGINAL ACTION
ARISING FROM FRANKLIN CIRCUIT COURT
ACTION NO. 08-CI-01409

HONORABLE THOMAS D. WINGATE,
JUDGE, FRANKLIN CIRCUIT COURT

RESPONDENT

COMMONWEALTH OF KENTUCKY, EX
REL. J. MICHAEL BROWN, SECRETARY,
JUSTICE AND PUBLIC SAFETY CABINET;
AND JACK CONWAY, ATTORNEY
GENERAL, CABINET OF KENTUCKY

REAL PARTIES IN INTEREST

AND

NO. 2008-CA-002019-OA

PLAYERONLY.COM; SPORTSBOOK.COM;
SPORTSINTERACTION.COM;
MYSportsBOOK.COM; AND LINESMAKER.COM

PETITIONERS

v. AN ORIGINAL ACTION
ARISING FROM FRANKLIN CIRCUIT COURT
ACTION NO. 08-CI-01409

HONORABLE THOMAS D. WINGATE, JUDGE
FRANKLIN CIRCUIT COURT

RESPONDENT

COMMONWEALTH OF KENTUCKY, EX REL.
J. MICHAEL BROWN, SECRETARY, JUSTICE
AND SAFETY CABINET

REAL PARTY IN
INTEREST

AND NO. 2008-CA-002036-OA

VICSBINGO.COM AND INTERACTIVE
GAMING COUNCIL

PETITIONERS

v. APPEAL FROM FRANKLIN CIRCUIT COURT
ACTION NO. 08-CI-01409

HONORABLE THOMAS D. WINGATE,
JUDGE, FRANKLIN CIRCUIT COURT

RESPONDENT

COMMONWEALTH OF KENTUCKY, EX
REL. J. MICHAEL BROWN, SECRETARY,
JUSTICE AND PUBLIC SAFETY CABINET

REAL PARTY IN INTEREST

ORDER
GRANTING PETITION FOR
WRIT OF PROHIBITION

*** **

BEFORE: CAPERTON, KELLER AND TAYLOR, JUDGES.

These consolidated petitions for a writ of prohibition stem from orders of the Franklin Circuit Court seizing 141 Internet domain names identified in a civil complaint filed by the Justice and Public Safety Cabinet of the Commonwealth of Kentucky. The trial court justified the seizure order on the basis that the domain names constituted "gambling devices" subject to the court's in rem jurisdiction. The petitioners argue that they are entitled to the extraordinary remedy of prohibition because the Franklin Circuit Court is acting outside its jurisdiction and the parties have no adequate remedy by appeal. Having considered the consolidated petitions for relief, the response of the Cabinet, the briefs submitted by the amici curiae, argument of counsel, and being otherwise sufficiently advised, the Court ORDERS that the petitions be GRANTED and the Franklin Circuit Court is hereby PROHIBITED from enforcing its order seizing the 141 domain names and from conducting a scheduled forfeiture hearing.

There is no dispute as to the facts. The Cabinet instituted a civil in rem action pursuant to Kentucky Revised Statute (KRS) 528.100 and KRS 500.090 against 141 named domain defendants for the purpose of stopping, as stated in

their response, "unregulated, unlicensed illegal Internet gambling that is occurring within the Commonwealth, in blatant disregard for, and in violation of, Kentucky law." After conducting an *ex parte* hearing on the Cabinet's application for seizure and forfeiture of the domain names, the Franklin Circuit Court entered an order on September 18, 2008, adjudging that:

1. Probable cause did and does exist under KRS 528.100 to believe that the Domain names listed on Exhibit A [the 141 domain names in issue here] were and are being used in connection with illegal gambling activity within the Commonwealth of Kentucky in violation of KRS Chapter 528.
2. A sufficient basis did and does exist for the seizure and forfeiture of the Domain Defendants by the Commonwealth.
3. The Domain Defendants are properly seized by the Commonwealth of Kentucky pursuant to KRS 528.100.

The order also directed the domain names to be "immediately transferred by their respective Registrars" to an account or other Registrar as designated by the Commonwealth and set a forfeiture hearing pursuant to KRS 500.090.

After the forfeiture hearing conducted on September 26, 2008, the trial court entered an order on October 2, 2008, which granted the motions of the Interactive Gaming Council (IGC), Interactive Media Entertainment and Gaming Association, Inc. (iMEGA), and counsel for seven specifically enumerated domain names (7 Domain Names) for leave to intervene in order to appear and assert the rights of their members regarding the following issues:

a) whether the Intervening Parties have standing to appear in this matter; b) whether this Court has Jurisdiction; c) whether the Domain Defendants are property; d) whether the Domain Defendants constitute a "gambling device or gambling record" for purposes of KRS Chapter 528; and e) whether poker is "gambling" for purposes of KRS Chapter 528.

That order also provided that if the trial court determined that jurisdiction exists and that the domain defendants were properly subject to forfeiture, only the owners of the domain defendants would be permitted to appear and defend the forfeiture.

Finally, the trial court entered the October 16, 2008 order which precipitated the petitions now under review by this Court. In essence, that order set forth the followings conclusions of the trial court:

1. that it had jurisdiction to adjudicate the Cabinet's civil forfeiture claim;
2. that there was a reasonable basis for the Court to assert jurisdiction over the domain names and their owners/operators;
3. that the domain names are property subject to *in rem* jurisdiction;
4. that the domain names are "gambling devices" subject to seizure and forfeiture;
5. that the seizure was consistent with Due Process;
6. that the Secretary of the Justice Cabinet has standing to bring the action on behalf of the Commonwealth;
7. that IGC and iMEGA lacked standing to intervene but could continue to appear as amici; and
8. that counsel for the group of 7 Domain Names must disclose the identities of the persons who engaged them and divulge their interest in the *res*.

A final hearing on forfeiture was scheduled for November 17, 2008, which was later rescheduled for December 3, 2008. This Court subsequently entered a stay of that forfeiture hearing to allow for oral argument on the consolidated petitions.

ANALYSIS

As a preliminary matter, we address the availability of the extraordinary remedy of prohibition as an avenue of redress for the seizure of the 141 domain names. Writs are generally divided into two classes: (1) those where the inferior court is acting without jurisdiction; or (2) those in which the court is acting within its jurisdiction but erroneously. *Grange Mutual Insurance Co. v. Trude*, 151 S.W.3d 803, 808 (Ky. 2004). If the inferior court is acting erroneously but within its jurisdiction, a writ may be granted if "there exists no adequate remedy by appeal or otherwise and great injustice and irreparable injury will result if the petition is not granted." *Hoskins v. Maricle*, 150 S.W.3d 1, 10 (Ky. 2004). However, irreparable harm need not be shown "provided a substantial miscarriage of justice will result if the lower court is proceeding erroneously, and correction of the error is necessary and appropriate in the interest of orderly judicial administration." (Emphasis in original) *Bender v. Eaton*, 343 S.W.2d 799, 801 (Ky. 1961). Finally, we note that the right to appeal does not necessarily indicate an adequate remedy. *Chamblee v. Rose*, 249 S.W.2d 775, 777 (Ky. App. 1952).

Thus, the focus of our inquiry is necessarily whether the trial court had jurisdiction to act. This determination requires analysis of two factors: 1) whether petitioners have standing to pursue a writ in this forum; and 2) whether the domain names fit within the statutory definition of "gambling devices" so as to trigger subject matter jurisdiction over the nature of the case and the type of relief sought.

Although the trial court concluded in its October 16th order that the associations had no standing to advance the interests of their members, the fact remains that they were initially granted leave to intervene to assert those very interests. Having participated in the proceedings below, and given the adverse ruling on their claims of lack of jurisdiction, we find no basis for denying those same participants the right to seek relief in this proceeding.

Next, because the Cabinet predicated its claim of entitlement to seize the domain names upon their status as illegal gambling devices, we turn our attention to a matter of statutory construction. Before proceeding, we note that the single issue presented in this regard, whether domain names fall within the statutory definition of KRS 528.010(4), is purely a matter of law and is subject to *de novo* review by this Court. *Revenue Cabinet v. Hubbard*, 37 S.W.3d 717, 719 (Ky. 2000).

KRS 528.010(4) defines "gambling device" as:

(a) Any so-called slot machine or any other machine or mechanical device an essential part of which is a drum or reel with insignia thereon, and which when operated may deliver, as a result of the application of an element of chance, any money or property, or by the operation of which a person may become entitled to receive, as the result of the application of an element of chance, any money or property; or

(b) Any other machine or any mechanical or other device, including but not limited to roulette wheels, gambling tables and similar devices, designed and manufactured primarily for use in connection with gambling and which when operated may deliver, as the result of the application of an element of chance, any money or property, or by the operation of which a person may become entitled to receive, as the result of the application of an element of chance, any money or property; [Emphasis added.]

Suffice it to say that given the exhaustive argument both in brief and oral form as to the nature of an Internet domain name, it stretches credulity to conclude that a series of numbers, or Internet address, can be said to constitute a "machine or any mechanical or other device...designed and manufactured primarily for use in connection with gambling." We are thus convinced that the trial court clearly erred in concluding that the domain names can be construed to be gambling devices subject to forfeiture under KRS 528.100.

We find the analysis of subject matter jurisdiction in this case remarkably similar to the analysis set out by the Supreme Court in *J.N.R. v. O'Reilly*, 264 S.W.3d 587 (Ky. 2008). In that case, the Supreme Court concluded that the General Assembly's decision to enact a narrow definition of "out-of-

wedlock birth" deprived the family court of subject matter jurisdiction to rule upon a putative father's paternity petition. We find the following rationale set out in that opinion particularly *apropos* to the matter before us here:

We recognize that the General Assembly may have chosen to bar paternity suits where there is no allegation of a cessation of marital relations for the ten-month period in part because of difficulties in accurately determining the biological father of a child at the time these statutes were enacted or amended to their present form. In view of modern DNA testing, the legislature might reasonably choose to amend the statutes again to recognize an alleged biological father's right to have paternity determined in court of a child born to a mother married to another man even where (as here) there is no evidence or allegation that marital relations ceased ten months before the child's birth. **But the choice is a policy decision that belongs to the General Assembly. And since the General Assembly has not yet chosen to amend KRS Chapter 406 in such a manner, we are without authority to amend the law for them.**

Id. at 593, footnote omitted, emphasis added.

So it is in the instant case. Regardless of our view as to the advisability of regulating or criminalizing Internet gambling sites, the General Assembly has not seen fit to amend KRS 528.010(4) so as to bring domain names within the definition of gambling devices. Neither we, nor the Justice Cabinet, are free to add to the statutory definition. If domain names cannot be considered gambling devices, Chapter 528 simply does not give the circuit court jurisdiction over them. Accordingly, petitioners have satisfied the criteria for obtaining a writ

prohibiting enforcement of the circuit court's previous orders and the conduct of the scheduled forfeiture hearing. No showing of irreparable injury is required.

Because we have concluded that petitioners are entitled relief on the above-stated basis, we decline to address other issues presented in the briefs and/or argued at oral argument.

TAYLOR, JUDGE, CONCURS BY SEPARATE OPINION.

CAPERTON, JUDGE, DISSENTS BY SEPARATE OPINION.

TAYLOR, JUDGE, CONCURRING: I concur with the majority's opinion in its entirety, but I would also grant the Writ of Prohibition pursuant to CR 76.36 for an additional reason. I do not believe there is statutory authority for an *in rem* civil forfeiture proceeding under KRS 528.100. Thus, the forfeiture of the 141 internet domain names under KRS 528.100 was improper. My rationale is as follows.

The forfeiture statute at issue, KRS 528.100, is found in the Kentucky Penal Code under the caption of "Gambling." To properly dispose of this petition, it is necessary to understand the legislative history of the statute and that of its predecessor, KRS 436.280.

KRS 436.280 (now repealed) read as follows:

Any bank, table, contrivance, machine or article used for carrying on a game prohibited by KRS 436.230, together with all money or other things staked or exhibited to allure persons to wager, may be seized by any justice of

the peace, sheriff, constable or police officer of a city, with or without a warrant, and upon conviction of the person setting up or keeping the machine or contrivance, the money or other articles shall be forfeited for the use of the state, and the machine or contrivance and other articles shall be burned or destroyed. Though no person is convicted as the setterup or keeper of the machine or contrivance, yet, if a jury, in summary proceedings, finds that the money, machine or contrivance or other articles were used or intended to be used for the purpose of gambling, they shall be condemned and forfeited.

Under the provisions of KRS 436.280, gaming devices could be forfeited under two scenarios: (1) upon conviction of any person using the gaming device as prohibited by statute; or (2) upon a finding by a jury that the device was used for gaming. Under the second scenario, a number of cases have interpreted the plain language of KRS 436.280 as providing for a civil *in rem* forfeiture proceeding allowing confiscation of gaming devices. See *Sterling Novelty Co. v. Com.*, 271 S.W.2d 366 (Ky. 1954). However, KRS 436.280 was repealed effective January 1, 1976, and KRS 528.100 was enacted to replace it.

KRS 528.100 reads:

Any gambling device or gambling record possessed or used in violation of this chapter is forfeited to the state, and shall be disposed of in accordance with KRS 500.090, except that the provisions of this section shall not apply to charitable gaming activity as defined by KRS 528.010(10).

Particularly of interest is the following 1974 Kentucky Crime Commission/LRC Commentary (commentary) to KRS 528.100:

This section provides for the forfeiture of gambling devices and records and for the uniform disposition of such forfeited devices and records.

Previously, possession of a gambling device was not an offense and a conviction of using the device was necessary before forfeiture was authorized. If there was no conviction, KRS 436.280 required that a jury be impanelled and find that the money, machine or contrivance or other articles were used or intended to be used for the purpose of gambling. In effect, this resulted in a forfeiture of gambling devices possessed although possession was not previously an offense.

As succinctly stated in the commentary, the prior forfeiture statute, KRS 436.280, provided for a civil *in rem* civil forfeiture proceeding because at that time "possession" of gambling devices was not a criminal offense; rather, "use" of a gambling device was criminally prohibited. Upon enactment in 1974 of KRS Chapter 528 and specifically KRS 528.080, the Legislature criminalized possession of a gambling device if a person in possession believed that the device was to be used in the advancement of unlawful gambling activity.¹ Concomitantly therewith, the General Assembly repealed the prior forfeiture statute, KRS 436.280. As possession of a gambling device may now constitute a crime under KRS 528.080, KRS 528.100 does not provide a civil *in rem* forfeiture proceeding, in my opinion.

¹ I do not believe that mere possession of a gambling device alone constitutes criminal conduct under KRS 528.080. Rather, a defendant must also have knowledge of the character of the device and believe or intend that the device is to be used in the advancement of gambling activity. See 10 Leslie W. Abramson, *Kentucky Practice – Substantive Criminal Law* § 10.9 (2008).

Indeed, the plain language of the statute specifically states that for a gambling device to be forfeited, it must be "possessed or used in violation of this chapter." Considering the legislative history of KRS 528.100 and the unambiguous language of the current statute, it is clear that the General Assembly intended to extinguish the civil *in rem* forfeiture proceeding as to gambling devices.² It is also interesting to note that there are no reported civil *in rem* forfeiture cases under KRS 528.100 since its enactment in 1974.

Thus, to trigger a forfeiture under KRS 528.100, we must closely look at the language therein. As noted, the statute clearly states that for a gambling device to be forfeited, it must be possessed or used in violation of KRS Chapter 528. The operative statutes in this Chapter are KRS 528.020-.080, which set out several separate crimes for which violations thereof could result in criminal penalties, including imprisonment.

However, in this case, there have been no criminal charges or indictments filed against any persons or entities involved. I believe for there to be a forfeiture, the clear legislative intent requires a conviction of one of the crimes enumerated in KRS Chapter 528. No other logical interpretation of the "violation" requirement of KRS 528.100 can be made, given that KRS Chapter 528 is a penal

² When considering a forfeiture statute, it is generally recognized that such statute is to be construed strictly against forfeiture and liberally in favor of the individual opposing forfeiture. See *Bratcher v. Ashley*, 243 S.W.2d 1011 (Ky. 1951).

statute. This deficiency in the Commonwealth's case is further amplified by the conspicuous absence of the Kentucky Attorney General, the Commonwealth's chief law officer, who pursuant to KRS 15.020 clearly has the authority to pursue the prosecution of crimes under KRS Chapter 528. The Secretary of the Justice and Public Safety Cabinet has no such authority.

Even assuming for argument that the dissent is correct that the domain names are gambling devices as defined in KRS 528.010, without a conviction under KRS Chapter 528, there can be no forfeiture in my opinion.

CAPERTON, JUDGE, DISSENTING: The issues before our Court necessarily turn upon the meaning of "device" as the term is used in KRS 528.100. I limit my dissent to this issue as this was the issue addressed by the majority.³

In Black's Law Dictionary 483 (8th ed. 2004) *device* is defined as "an apparatus or an article of manufacture." *Article* is defined as "[p]atents. An article of manufacture. See Manufacture." Black's Law Dictionary 119 (8th ed. 2004). *Manufacture* is defined as "[a] thing that is made or built by a human being, as distinguished from something that is a product of nature . . ." Black's Law Dictionary 984 (8th ed. 2004). Little doubt can be cast upon the fact that a computer is built by a human being; thus, a computer is a device.

³ In search of the meaning of device, I found little if any Kentucky case law relevant to the issue before our Court. Thus, I resorted to Black's Law Dictionary, Eighth Edition.

Is programming a device? The Computer Software Protection Act of 1980 says it is a literary work. However, a *software based invention* is defined as “[a] *device* or machine that uses innovative software to achieve results.” Black’s Law Dictionary 844 (8th ed. 2004). (Emphasis added). Thus, it appears that a computer using software remains a “device”.

In the case before our Court, internet gambling requires several components. First, there is a local computer terminal located in Kentucky. Second, there is a remote computer located elsewhere. Third, the two computers are linked by the internet and compatible software. Thus, we have two devices using software and linked by the internet into a system. Based on the foregoing analysis, I believe it to be a computer system⁴ that is, for the period of time linked together for the purpose of internet gambling, unified into one device.⁵


⁴ The system consists of at least two computers, the internet, and the addresses at issue.

⁵ If the gambling system at issue consisted of a local computer connected to a remote computer, whether in the same room or across the world and connected by a cable consisting of wires, then I believe there would be little question that the combination of such components would be a device. However, the question posed today is when the connecting cable is replaced with the internet and an address, i.e., a string of numbers or domain name, is the gambling system then something else or does the substitution present a mere differentiation with no real difference? I am of the opinion that even though the components of the device may change, it is still a device nonetheless. For instance, if a wire were removed from the computer all would likely agree that it is a wire, but when replaced into the computer it is then a part of the computer. Mere removal and replacement did not change the computer to something else, nor does mere substitution of the internet and a domain name for a wired cable change the gambling device to some mystical marvel of science that rises above the law of this Commonwealth.

At issue is the seizure of 141 internet gambling domain names. The internet gambling domain names⁶ serve as addresses which enable the local computer to locate and communicate with the remote computer. While we see a name on the computer screen, the computer "sees" a string of numbers. The "string of numbers" is a *necessary component*⁷ of the internet gambling device because without these numbers, the link between the computers could not be initiated and/or maintained. Just as a wire placed into a computer becomes part of the computer, so do the internet domain names that link remote computers for purposes of gambling become part of the gambling device.

Therefore, based on the foregoing analysis, I believe that internet domain names are but one of the components that are unified into an internet gambling device and properly within the definition of device as that term is used in KRS 528.100.

ENTERED: 1-20-09


JUDGE, COURT OF APPEALS

the internet and a domain name for a wired cable change the gambling device to some mystical marvel of science that rises above the law of this Commonwealth.

⁶ One argument of counsel was that the domain names are free speech and invoke the protection of the first amendment. Assuming the domain names are entitled to the protections of the first amendment, then speak the words but strip them of the underlying "numbers" seen by the computer.

⁷ Just as is the local computer, the remote computer, the software and the internet.

RENDERED: MARCH 18, 2010
TO BE PUBLISHED

Supreme Court of Kentucky

2009-SC-000043-MR

FINAL

COMMONWEALTH OF KENTUCKY,
EX REL. J. MICHAEL BROWN,
SECRETARY, JUSTICE AND PUBLIC
SAFETY CABINET

DATE 4/8/10 Kelly Kleber D.C.
APPELLANT

APPEAL FROM COURT OF APPEALS
V. CASE NOS. 2008-CA-002000-OA, 2008-CA-002019-OA
AND 2008-CA-002036-OA
FRANKLIN CIRCUIT COURT NO. 08-CI-1409

INTERACTIVE MEDIA
ENTERTAINMENT AND GAMING
ASSOCIATION, INC.; INTERACTIVE
GAMING COUNCIL; VICSBINGO.COM;
PLAYERSONLY.COM;
SPORTSBOOK.COM;
SPORTSINTERACTION.COM;
MYSportsBOOK.COM;
LINESMAKER.COM; AND HON.
THOMAS D. WINGATE, JUDGE,
FRANKLIN CIRCUIT COURT

APPELLEES

OPINION OF THE COURT BY JUSTICE NOBLE

REVERSING

This case arises from an order by the Franklin Circuit Court that 141 internet domain names be seized from their owners and operators and transferred to the dominion and control of the Commonwealth. Attorneys acting on behalf of the domain names sought a writ of prohibition against the seizure, which the Kentucky Court of Appeals granted. Because the parties

seeking the writ have failed to demonstrate that they have standing to do so, this Court reverses, though this does not foreclose the possibility of future relief.

I. Background

Initiating a fight against internet gambling in Kentucky, the Commonwealth filed an *in rem* action in Franklin Circuit Court over multiple pieces of intangible property—141 internet domain names. The Commonwealth had funded an extensive research project, whereby several civilians were employed to search the internet for gambling domains. The 141 domains discovered in the search were, in the Commonwealth's view, hosting illegal gambling activities. Armed with KRS 528.010 and acting through the Secretary of the Justice and Public Safety Cabinet, J. Michael Brown, the Commonwealth sued in Franklin Circuit Court to have those domain names seized.

In a hearing where only the Commonwealth participated, the trial court heard testimony regarding the discovery and nature of the domain names. Using a probable-cause standard, the court concluded that the websites were indeed violating Kentucky's gambling laws. Pursuant to what it found to be a civil forfeiture remedy in KRS 528.010, the court ordered seizure of the domain names and instructed their registrars to transfer them to the Commonwealth of Kentucky.

When those supposedly affected learned of the order, counsel appeared in Franklin Circuit Court on their behalf to challenge the seizure. The parties purporting to be affected by the seizure were atypical *in rem* claimants,

however. Instead of owners, operators, or registrants of the website domain names, the lawyers opposing the Commonwealth claimed to represent two types of entities: (1) the domain names themselves and (2) gaming trade associations who profess to include as members registrants of the seized domains, though they have yet to reveal any of their identities. The various groups of domain names and gaming associations sought to intervene in the case and dismiss the seizure. The circuit court ultimately denied all motions to intervene or dismiss and scheduled a forfeiture hearing where the actual registrants and owners of the seized domains could prove their innocence.¹ The court specifically noted in its order that only the domain name owners, operators, and registrants had a legal interest in the domain names and only they or their representatives could defend against forfeiture.

Upon the denial of their motions, the groups and associations sought a writ of prohibition from the Court of Appeals to enjoin the impending forfeiture. The Court of Appeals issued the writ, reasoning that the trial court acted beyond the jurisdiction of KRS 528.100. The Commonwealth, appealing as a matter of right, asks this Court to vacate the writ of prohibition.

II. Analysis

Numerous, compelling arguments endorsing the grant of the writ of prohibition have been presented throughout the Court of Appeals' opinion, Judge Taylor's separate concurrence, the Appellees' briefs, the amici briefs, and oral argument before this Court. This plethora of arguments includes, among

¹ The court did, however, permit the gaming associations to participate in the litigation as *amici curiae*.

others, that (1) Kentucky law only mandates the seizure of tangible gambling devices, and not intangible things such as domain names; (2) the court's civil forfeiture was unauthorized because KRS 528.100 only contemplates criminal sanctions; and (3) Kentucky lacks *in rem* jurisdiction over the domain names because they are not located in Kentucky.

Although all such arguments may have merit, none can even be considered unless presented by a party with standing. No such party has appeared at the original proceedings in Franklin Circuit Court, the writ petition at the Court of Appeals, or on the appeal here to this Court. As mentioned above, two types of Appellees sought the writ, claiming an interest in the domain names: (1) the purported domain names themselves and (2) associations of anonymous domain registrants. Neither group meets the basic requirements of standing.

A. Six Domain Names

Counsel purportedly appeared directly on behalf of six domain names and participated in the writ action at the Court of Appeals. The advocacy on behalf of five of these domain names was consolidated into one representation. These five domain names—*playersonly.com*, *sportsbook.com*, *sportsinteraction.com*, *mysportsbook.com*, and *linesmaker.com*—have been referred to as the “group of five.” The sixth, *vicsbingo.com*, joined in the appeal through separate counsel, together with the Interactive Gaming Council, one of the gaming associations. Counsel for these six domain names have consistently claimed the names are some of the intangible property seized by the trial court and that the names are appearing to protect their own interests

in themselves. Put simply, counsel purports to represent property that is protecting itself.

Although unaddressed in the Court of Appeals opinion below, the Commonwealth has apparently challenged the standing of these individual domain names at every stage of the proceedings. It has insisted that the property seized cannot defend itself, but can only be defended by those having an interest in the property—namely owners and registrants of domain names. Since no owners or registrants have ever claimed to be participating in this case at any level, the Commonwealth requests that this Court vacate the writ and restore the seizure of the domain names.

The domain names' assertion of standing hinges on the origination of this controversy as an *in rem* proceeding. They claim that since the Commonwealth named the domain names as the *in rem* defendants, the names must have an opportunity to represent themselves.

The domain names' argument confuses the nature of *in rem* litigation. It has long been recognized in Kentucky, as well as elsewhere, that in *in rem* litigation, only those with an interest in the property, such as current owners, have an interest in the litigation. See *Taylor v. City of La Grange*, 262 Ky. 383, 90 S.W.2d 357 (1936); *City of Middlesborough v. Coal & Iron Bank*, 33 Ky. L. Rptr. 469, 110 S.W. 355, 356 (1908); *United States v. One 1965 Cessna 320C Twin Engine Airplane*, 715 F. Supp. 808, 810 (E.D. Ky. 1989). The property does not have an interest in itself and, therefore, does not have any interest in the litigation. See *United States v. One Parcel of Real Property*, 831 F.2d 566, 568 (5th Cir. 1987) (“[O]wners are persons, not pieces of real property; [a] piece

of real property has no standing to contest its forfeiture.”). An internet domain name does not have an interest in itself any more than a piece of land is interested in its own use. Just as with real property, a domain name cannot own itself; it must be owned by a person or legally recognized entity. Nor does the property itself care whether it is owned and operated by private business or seized by state government.

When faced with a similar claim, the Fifth Circuit found the concept of property having *in rem* standing to be so far-fetched as to be “not arguable on its merits” and “frivolous,” *id.*, that it issued sanctions against the attorneys purporting to represent such property. *See id.* at 568-69. This Court agrees that the contention that mere property can represent itself is frivolous.

The fundamental standing requirement of an interest *in* the property does not dissipate in a writ case. A writ of prohibition, just like any other judicial remedy, may only be sought by a party with a “judicially recognizable interest.” *Schroering v. McKinney*, 906 S.W.2d 349, 350 (Ky. 1995). The writ granted below serves only the interests of the owners and registrants of the domain names. It does not benefit the domains themselves; they *are* the interest at question in this case and belong to still unnamed owners and registrants.

The group of five mistakenly suggests unfairness in the Commonwealth proceeding *in rem* against property without giving the property a “right to defend.” Property possesses no such right. Kentucky’s judicial system exists to protect the interests of persons—both individuals and groups—not property. Property does not have constitutional or statutory rights. Nor does it have a

right of access to the judicial system. Nor does it have a judicially recognizable interest in this writ.

Counsel for vicsbingo.com, meanwhile, misinterprets the unorthodox styling of *in rem* case names to mean that the usual standing requirements do not apply. It cites *Three One-Ball Pinball Machines v. Commonwealth*, 249 S.W.2d 144 (Ky. 1952), as an example of property contesting its own seizure under Kentucky's old gambling laws. To be sure, that case name is styled so that the pinball machines themselves are listed as a party (in that case, the appellant), as is routine for civil forfeiture proceedings. This is because *in rem* "case captions have historically referenced the property subject to forfeiture and not the interested parties." *Commonwealth v. Maynard*, 294 S.W.3d 43, 49 (Ky. App. 2009). But as Justice Combs pointed out in the second sentence of *Three One-Ball Pinball Machines*, "[t]he style of the case is a misnomer. Although the machines are designated as the appellants in the case, it is their owners who argue" against the seizure. 249 S.W.2d. at 145 (emphasis added); see also *14 Console Type Slot Machines v. Commonwealth*, 273 S.W.2d 582, 582 (Ky. 1954) ("On this appeal by the slot machines (*through their owner*), the main contention is that. . . .") (emphasis added). Likewise, in the situation at hand, the style of the case title does not change the fact that only those with an interest in the property have standing. The writ may be styled as being sought in the *name* of the domains, but the parties arguing on their behalf must be ones with standing, such as owners.

The domain names are not their own owners or registrants, nor do they claim to be. Thus, they lacked standing to pursue the writ.

B. Gaming Associations

Two gaming associations have attempted to enroll in this litigation: the Interactive Media Entertainment & Gaming Association (iMEGA) and the Interactive Gaming Council (IGC). iMEGA and IGC both claim to represent registrants of some of the seized domains. They claim to have standing on behalf of their members under the doctrine of associational standing.

iMEGA refuses to reveal which registrants it represents, or even how many. It simply claims to have members who registered some, but not all, of the seized domains.

IGC, on behalf of its members, stakes claim to 61 seized domain names.² IGC is not all that clear, perhaps intentionally, about whether it represents registrants or the actual domain names. For example, on page 13 of its brief, it claims to be “[r]epresenting the *registrants* for 61 of the 141 Domain Names.” (Emphasis added.) Yet the following sentence of the brief reads, “IGC identified all 61 *domain names* it represents. . . .” (Emphasis added.) For purposes of this appeal, we will interpret IGC as purporting to represent registrants. The problem, however, is that IGC fails to disclose who these registrants are.

Associational standing inherently depends on the membership of the association. The U.S. Supreme Court has set out three requirements for an association to have standing in federal court:

- (a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization’s purpose; and (c) neither the claim asserted nor the relief requested

² Which 61 of the 141 is not apparent from our record.

requires the participation of the individual members in the lawsuit.

Hunt v. Washington State Apple Adver. Comm’n, 432 U.S. 333, 343 (1977). In *Hunt*, the Court found that the Washington State Apple Advertising Commission had standing to challenge a North Carolina statute which prevented its members, Washington apple dealers, from displaying Washington apple grades. *See id.* at 337-45.

While this Court has not held that the precise requirements of federal associational standing apply in Kentucky courts, at least the first requirement must apply. An association can have standing only if its members could have sued in their own right. Otherwise the primary requirement for standing, that the party has a real interest in the litigation, would be thwarted.

In *City of Ashland v. Ashland F.O.P. No. 3*, 888 S.W.2d 667 (Ky. 1994), this Court granted the Fraternal Order of Police standing to challenge a city ordinance that limited public employment to people living within city limits. The F.O.P. had standing because its members—the police—had a “real and substantial interest” in striking the ordinance. *Id.* at 668. Although the ordinance only applied to new employees, other police officers depended on the quality of the new police for their own safety. *Id.* “Such an interest conferred standing on the police association because, according to stipulation, it represented the majority of city police.” *Id.*

Unlike the F.O.P., the gaming associations in this case have failed to disclose whom they represent. While IGC claims to represent 61 of the seized domains and iMEGA purports to represent “some” more, this Court cannot

simply take their words for it. The associations bear the burden to demonstrate that they satisfy the requirements of standing, and to do so requires proving that their members would have standing themselves. See *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992) (party invoking jurisdiction bears burden of proving standing); *Am. Chemistry Council v. DOT*, 468 F.3d 810, 820 (D.C. Cir. 2006) (association bears burden to prove members have standing). Without even revealing any of the registrants they purport to represent, the associations cannot hope to achieve associational standing. “At the very least, the identity of the party suffering an injury in fact must be firmly established.” *Am. Chemistry Council*, 468 F.3d at 820; see also *United States v. AVX Corp.*, 962 F.2d 108, 117 (1st Cir. 1992) (no associational standing where injured members were unidentified); *Sierra Club v. SCM Corp.*, 747 F.2d 99, 103, 107-08 (2nd Cir. 1984) (same); *Revell v. Port Authority of N.Y. and N.J.*, 321 Fed. App’x. 113, 117 n.2 (3rd Cir. 2009) (failure to identify affected members causes standing to “evaporate quickly”). But see *Doe v. Stincer*, 175 F.3d 879, 882 (11th Cir. 1999) (taking contrary position).

The cyber-age status of their members does not let iMEGA and IGC escape traditional standing requirements. In another suit brought on by an association of internet domain registrants, the Coalition for ICANN Transparency (CFIT) initially merely “alleged vague categories of members that might suffer harm.” *Coalition for ICANN Transparency Inc. v. VeriSign, Inc.*, 464 F. Supp. 2d 948, 956 (N.D. Cal. 2006), *rev’d on other grounds*, 567 F.3d 1084 (9th Cir. 2009). Thus, “associational standing had not been alleged because CFIT failed to name even one member.” *Id.* CFIT was able to solve this

problem, however, by identifying one of its members, Pool.com, Inc., which allegedly suffered injury-in-fact. *Id.* Here as well, the associations had every opportunity to cure their standing defects by identifying their seized members; in fact, they were ordered to do so by the Franklin Circuit Court. Refusing to follow this straightforward requirement, iMEGA and IGC do not have standing.

Admittedly, in some cases the surrounding particulars may not demand that an association identify specific members. For example, in *Ashland F.O.P.*, this Court did not discuss whether the fraternal order had identified affected members. Indeed, the *Ashland F.O.P.* may not have provided a membership list. But in that case it was stipulated that the F.O.P. represented the majority of the police force. 888 S.W.2d at 668. Since all members of the police could claim injury from the ordinance (albeit indirectly), it necessarily followed that the F.O.P.'s members would have had standing in their own right. Unlike in *Ashland F.O.P.*, there is no stipulation as to iMEGA or IGC's memberships. In fact, nothing is known about their members, other than their attorneys' vague assertions they represented "some" of the registrants.

Moreover, notably distinct from *Ashland F.O.P.*, not all internet gaming registrants are affected by the seizure; only the registrants of the 141 seized domains. In cases where the harm is specific, the proof of standing must be equally specific. See *Forum for Academic & Inst. Rights, Inc. v. Rumsfeld*, 291 F. Supp. 2d 269, 288 (D.N.J. 2003). For example, in cases where only people in a certain geographical area may be harmed, a showing that members are located in that area is "critical" to associational standing. See *id.* (distinguishing *AVX*

Corp., 962 F.2d at 117, stating, “Geographic location was critical to establishing members’ injury-in-fact in the environmental context. . . .”).

Similarly, where, as here, the injury is limited to those whose property was actually seized, associational standing requires some assurance that members actually have an interest in the property. Thus, the associations must specifically identify some of the affected registrants they represent.

This is not to say that showing associational standing requires heavy proof. On the contrary, it must simply be proven to the same extent as any other “indispensable part of the plaintiff’s case.” *Lujan*, 504 U.S. at 561. “[E]ach element must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation.” *Id.* At the pleading stage, less specificity is required. At that point, an association may speak generally of the injuries to “some” of its members, for the “presum[ption] [is] that general allegations embrace those specific facts that are necessary to support the claim.” *Id.*; accord *Bldg. & Constr. Trades Council of Buffalo v. Downtown Dev., Inc.*, 448 F.3d 138, 145 (2nd Cir. 2006). By the summary judgment stage, however, more particulars regarding the association’s membership must be introduced or referenced. See *Bldg. & Constr. Trades Council of Buffalo*, 448 F.3d at 144-45; *Sierra Club v. SCM Corp.*, 747 F.2d 99, 102 (2nd Cir. 1984) (affirming dismissal where association “indicated that it did not intend to identify any of its members who might have been harmed”). Finally, before a favorable judgment can be attained, the association’s general allegations of injury must clarify into “concrete” proof that “one or more of its

members” has been injured. *See Sierra Club*, 747 F.2d at 107. “By refus[ing] to come forward with any such showing,” any claim to associational standing, and the potential for success on the merits is forfeited. *See id.*

While the normal sequence of litigation is muddled in a writ petition, since only pleadings are filed and no discovery is allowed, the basic requisites for a judgment remain. This includes proof of standing. When associational standing is the chosen route, the writ petitioner must prove it represents at least one member with an injury in order to obtain relief. This may be done by reference to the facts in the underlying litigation or a verified assertion, such as in an affidavit, attached to the petition. Through their unwillingness to identify any of their members, iMEGA and IGC failed to meet this burden. As such, iMEGA and IGC lack standing and, therefore, their writ petition should have been denied.

Writs are to be granted only as an extraordinary remedy, and certainly only when parties who have demonstrated a concrete interest are before the court. This is not to say, however, that the failure to establish standing in this writ action completely forecloses relief by way of a writ in the future. If a party that can properly establish standing comes forward, the writ petition giving rise to these proceedings could be re-filed with the Court of Appeals. The Court of Appeals could then properly proceed to the merits of the issues raised, or upon a proper motion, this Court could accept transfer of the case, as the merits of the argument have already been briefed and argued before this Court. Until then, however, consideration of the merits of this matter is improper for lack of standing.

III. Conclusion

Due to the incapacity of domain names to contest their own seizure and the inability of iMEGA and IGC to litigate on behalf of anonymous registrants, the Court of Appeals is reversed and its writ is vacated. This case is hereby remanded to the Court of Appeals with instructions to dismiss the Appellee's writ petition.

Minton, C.J.; Abramson, Schroder and Venters, JJ., concur. Scott, J., concurs in result only. Cunningham, J., not sitting.

COUNSEL FOR APPELLANT:

David Eric Lycan
William Harvey May
Aaron Davis Reedy
Hurt, Crosbie & May PLLC
The Equis Building
127 West Main
Lexington, Kentucky 40507

William Cecil Hurt, Jr.
Wethington, Hurt & Crosbie, PLLC
127 West Main Street
Lexington, Kentucky 40507

COUNSEL FOR APPELLEE, INTERACTIVE MEDIA ENTERTAINMENT &
GAMING ASSOCIATION, INC.:

Jon L. Fleischaker
Robert Kenyon Meyer
James Lee Adams
Dinsmore & Shohl, LLP
1400 PNC Plaza
500 W. Jefferson Street
Louisville, Kentucky 40202

COUNSEL FOR APPELLEE, INTERACTIVE GAMING COUNCIL:

Margaret Eileen Mary Keane
Greenebaum, Doll & McDonald, PLLC
101 S. 5th Street
3500 National City Tower
Louisville, Kentucky 40202

Phillip D. Scott
Greenebaum, Doll & McDonald, PLLC
300 West Vine Street, Suite 1100
Lexington, Kentucky 40507-1665

COUNSEL FOR APPELLEES, INTERACTIVE GAMING COUNCIL AND
VICSBINGO.COM:

Bruce F. Clark
Stites & Harbison, PLLC
421 West Main Street
PO Box 634
Frankfort, Kentucky 40602-0634

Ian Thomas Ramsey
John Lewis Tate
Joel Beres
Stites & Harbison, PLLC
400 West Market Street
Suite 1800
Louisville, Kentucky 40202

COUNSEL FOR APPELLEES, PLAYERONLY.COM, SPORTSBOOK.COM,
SPORTSINTERACTION.COM, MYSportsBOOK.COM AND LINESMAKER.COM:

William E. Johnson
Johnson, True & Guarnieri, LLP
326 West Main Street
Frankfort, Kentucky 40601-1887

APPELLEE, HON. THOMAS D. WINGATE:

Honorable Thomas D. Wingate
Judge, Franklin Circuit Court
214 St. Clair Street
PO Box 678
Frankfort, Kentucky 40601

COUNSEL FOR AMICUS CURIAE, EBAY, INC.:

Laura Anne D'Angelo
Wyatt, Tarrant & Combs, LLP
250 West Main Street
Suite 1600
Lexington, Kentucky 40507-1746

Daniel G. Dougherty
Ebay, Inc.
2065 Hamilton Avenue
San Jose, California 95125

COUNSEL FOR AMICUS CURIAE, NETWORK SOLUTIONS, LLC.: .

Michael Romano Mazzoli
Cox & Mazzoli, PLLC
600 West Main Street
Suite 300
Louisville, Kentucky 40202

Timothy B. Hyland
25 West Middle Lane
Rockville, MD 20850

COUNSEL FOR AMICUS CURIAE, THE ELECTRONIC FRONTIER
FOUNDATION, THE CENTER FOR DEMOCRACY AND TECHNOLOGY, THE
AMERICAN CIVIL LIBERTIES UNION OF KENTUCKY, THE MEDIA ACCESS
PROJECT, THE UNITED STATES INTERNET INDUSTRY ASSOCIATION, THE
INTERNET COMMERCE COALITION, THE INTERNET COMMERCE
ASSOCIATION:

David Alan Friedman
325 West Main Street, Suite 150
Louisville, Kentucky 40202

COUNSEL FOR AMICUS CURIAE, POKER PLAYERS ALLIANCES:

Joshua Taylor Rose
Charles M. Pritchett, Jr.
Bart Loveman Greenwald
Frost, Brown, Todd, LLC
400 West Market Street, 32nd Floor
Louisville, Kentucky 40202-3363