

UNITED STATES DISTRICT COURT

UNITED STATES OF AMERICA,

Plaintiff,

V.

LORI DREW,

Defendant.

No. CR 08-0582-GW

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 that the intentional accessing of a computer without authorization or in excess of authorization

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 appears most often in Supreme Court opinions. See, e.g., Pac. Bell Tel. Co. v. linkline Comms., Inc., 555 U.S. , 129 S.Ct. 1109, 1115 (2009).

1 be in furtherance of the commission of a criminal or tortious act) within the CFAA
 2 felony provision as delineated in 18 U.S.C. § 1030(c)(2)(B)(ii) overcame Defendant's
 3 constitutional challenges and arguments against the criminalization of breaches of
 4 contract involving the use of computers. See Reporter's Transcripts of Hearings on
 5 September 4 and October 30, 2008. However, Drew was subsequently acquitted by
 6 a jury of the felony CFAA counts but convicted of misdemeanor CFAA violations.
 7 Hence, the question in the present motion under Federal Rule of Criminal Procedure
 8 ("F.R.Crim.P.") 29(c) is whether an intentional breach of an Internet website's terms
 9 of service, without more, is sufficient to constitute a misdemeanor violation of the
 10 CFAA; and, if so, would the statute, as so interpreted, survive constitutional
 11 challenges on the grounds of vagueness and related doctrines.²

12 **II. BACKGROUND**

13 **A. Indictment**

14 In the Indictment, Drew was charged with one count of conspiracy in violation
 15 of 18 U.S.C. § 371 and three counts of violating a felony portion of the CFAA, i.e.,
 16 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii), which prohibit accessing a com-
 17 puter without authorization or in excess of authorization and obtaining information
 18

19 ² While this case has been characterized as a prosecution based upon purported "cyberbullying," there
 20 is nothing in the legislative history of the CFAA which suggests that Congress ever envisioned such an
 21 application of the statute. See generally, A. Hugh Scott & Kathleen Shields, Computer and Intellectual
 22 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):

23 The federal computer fraud and abuse statute, 18 U.S.C. 1030, protects
 24 computers in which there is a federal interest – federal computers, bank
 25 computers, and computers used in interstate and foreign commerce. It
 shields them from trespassing, threats, damage, espionage, and from being
 26 corruptly used as instruments of fraud. It is not a comprehensive provision,
 instead it fills cracks and gaps in the protection afforded by other state and
 federal criminal laws.

27 Moreover, once Drew was acquitted by the jury of unauthorized accessing of a protected computer in
 28 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.

1 from a protected computer where the conduct involves an interstate or foreign
2 communication and the offense is committed in furtherance of a crime or tortious act.
3 See Doc. No. 1.

4 The Indictment included, inter alia, the following allegations (not all of which
5 were established by the evidence at trial). Drew, a resident of O’Fallon, Missouri,
6 entered into a conspiracy in which its members agreed to intentionally access a
7 computer used in interstate commerce without (and/or in excess of) authorization in
8 order to obtain information for the purpose of committing the tortious act of
9 intentional infliction of emotional distress³ upon “M.T.M.,” subsequently identified
10 as Megan Meier (“Megan”). Megan was a 13 year old girl living in O’Fallon who had
11 been a classmate of Drew’s daughter Sarah. Id. at ¶¶ 1- 2, 14. Pursuant to the
12 conspiracy, on or about September 20, 2006, the conspirators registered and set up a
13 profile for a fictitious 16 year old male juvenile named “Josh Evans” on the
14 www.MySpace.com website (“MySpace”), and posted a photograph of a boy without
15 that boy’s knowledge or consent. Id. at ¶ 16. Such conduct violated MySpace’s terms
16 of service. The conspirators contacted Megan through the MySpace network (on
17 which she had her own profile) using the Josh Evans pseudonym and began to flirt
18 with her over a number of days. Id. On or about October 7, 2006, the conspirators
19 had “Josh” inform Megan that he was moving away. Id. On or about October 16,
20 2006, the conspirators had “Josh” tell Megan that he no longer liked her and that “the
21 world would be a better place without her in it.” Id. Later on that same day, after
22 learning that Megan had killed herself, Drew caused the Josh Evans MySpace account
23 to be deleted. Id.

24
25 ³ The elements of the tort of intentional infliction of emotional distress are the same under both
26 Missouri and California state laws. Those elements are: (1) the defendant must act intentionally or recklessly;
27 (2) the defendant’s conduct must be extreme or outrageous; and (3) the conduct must be the cause (4) of
28 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 (2007).

1 **B. Verdict**

2 At the trial, after consultation between counsel and the Court, the jury was
 3 instructed that, if they unanimously decided that they were not convinced beyond a
 4 reasonable doubt as to the Defendant's guilt as to the felony CFAA violations of 18
 5 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii), they could then consider whether the
 6 Defendant was guilty of the "lesser included"⁴ misdemeanor CFAA violation of 18
 7 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A).⁵

8 At the end of the trial, the jury was deadlocked and was unable to reach a
 9 verdict as to the Count 1 conspiracy charge.⁶ See Doc. Nos. 105 and 120. As to
 10 Counts 2 through 4, the jury unanimously found the Defendant "not guilty" "of [on
 11

12 ⁴ As provided in F.R.Crim.P. 31(c)(1), a "defendant may be found guilty of . . . an offense necessarily
 13 included in the offense charged" A "lesser included" crime is one where "the elements of the lesser
 14 offense are a subset of the elements of the charged offense." *Carter v. United States*, 530 U.S. 255, 260
 15 (2000) (quoting *Schmuck v. United States*, 489 U.S. 705, 716 (1989)). Because the felony CFAA crime in
 16 18 U.S.C. § 1030(c)(2)(B)(ii) consists of committing acts which constitute a violation of the misdemeanor
 17 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
 18 element that the acts were done "in furtherance of any crime or tortious act in violation of the Constitution
 19 or laws of the United States or any State," the misdemeanor CFAA crime is a "lesser included" offense as
 20 to the felony CFAA violation.

21 A defendant is entitled to a "lesser included" offense jury instruction if the evidence warrants it.
 22 *Guam v. Fejerman*, 687 F.2d 302, 305 (9th Cir. 1982).

23 ⁵ Specifically, the jury was instructed that:

24 The crime of accessing a protected computer without authorization or in
 25 excess of authorization to obtain information, and to do so in furtherance of
 26 a tortious act in violation of the laws of any State, includes the lesser crime
 27 of accessing a protected computer without authorization or in excess of
 28 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.

⁶ The conspiracy count was subsequently dismissed without prejudice at the request of the Government.

1 the dates specified in the Indictment] accessing a computer involved in interstate or
 2 foreign communication without authorization or in excess of authorization to obtain
 3 information in furtherance of the tort of intentional infliction of emotional distress in
 4 violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B)(ii) . .
 5 . .” Id. The jury did find Defendant “guilty” “of [on the dates specified in the
 6 Indictment] accessing a computer involved in interstate or foreign communication
 7 without authorization or in excess of authorization to obtain information in violation
 8 of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(A), a misdemeanor.”
 9 Id.

10 C. MySpace.com

11 As Jae Sung (Vice President of Customer Care at MySpace) (“Sung”) testified
 12 at trial, MySpace is a “social networking” website where members can create
 13 “profiles” and interact with other members. See Reporter’s Transcript of the
 14 November 21, 2008 Sung testimony (“11/21/08 Transcript”) at pages 40-41. Anyone
 15 with Internet access can go onto the MySpace website and view content which is open
 16 to the general public such as a music area, video section, and members’ profiles which
 17 are not set as “private.” Id. at 42. However, to create a profile, upload and display
 18 photographs, communicate with persons on the site, write “blogs,” and/or utilize other
 19 services or applications on the MySpace website, one must be a “member.” Id. at 42-
 20 43. Anyone can become a member of MySpace at no charge so long as they meet a
 21 minimum age requirement and register. Id.

22 In 2006, to become a member, one had to go to the sign-up section of the
 23 MySpace website and register by filling in personal information (such as name, email
 24 address, date of birth, country/state/postal code, and gender) and creating a password.
 25 Id. at 44-45. In addition, the individual had to check on the box indicating that “You
 26 agree to the MySpace **Terms of Service** and **Privacy Policy**.” See Government’s⁷

27
 28 ⁷ All exhibits referenced herein were proffered by the Government and admitted during the trial.

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 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

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 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.

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).

1 By using the Services, you represent and warrant that (a) all
2 registration information you submit is truthful and accurate;
3 (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.

4 Id. at 2.

5 The MSTOS prohibited the posting of a wide range of content on the website
6 including (but not limited to) material that: a) “is potentially offensive and promotes
7 racism, bigotry, hatred or physical harm of any kind against any group or individual”;
8 b) “harasses or advocates harassment of another person”; c) “solicits personal
9 information from anyone under 18”; d) “provides information that you know is false
10 or misleading or promotes illegal activities or conduct that is abusive, threatening,
11 obscene, defamatory or libelous”; e) “includes a photograph of another person that
12 you have posted without that person’s consent”; f) “involves commercial activities
13 and/or sales without our prior written consent”; g) “contains restricted or password
14 only access pages or hidden pages or images”; or h) “provides any phone numbers,
15 street addresses, last names, URLs or email addresses” Id. at 4. MySpace also
16 reserved the right to take appropriate legal action (including reporting the violating
17 conduct to law enforcement authorities) against persons who engaged in “prohibited
18 activity” which was defined as including, inter alia: a) “criminal or tortious activity”,
19 b) “attempting to impersonate another Member or person”, c) “using any information
20 obtained from the Services in order to harass, abuse, or harm another person”, d)
21 “using the Service in a manner inconsistent with any and all applicable laws and
22 regulations”, e) “advertising to, or solicitation of, any Member to buy or sell any
23 products or services through the Services”, f) “selling or otherwise transferring your
24 profile”, or g) “covering or obscuring the banner advertisements on your personal
25 profile page” Id. at 5. The MSTOS warned users that “information provided by
26 other MySpace.com Members (for instance, in their Profile) may contain inaccurate,
27 inappropriate, offensive or sexually explicit material, products or services, and
28 MySpace.com assumes no responsibility or liability for this material.” Id. at 1-2.

1 Further, MySpace was allowed to unilaterally modify the terms of service, with such
2 modifications taking effect upon the posting of notice on its website. Id. at 1. Thus,
3 members would have to review the MSTOS each time they logged on to the website,
4 to ensure that they were aware of any updates in order to avoid violating some new
5 provision of the terms of service. Also, the MSTOS provided that “any dispute”
6 between a visitor/member and MySpace “arising out of this Agreement must be settled
7 by arbitration” if demanded by either party. Id. at 7.

8 At one point, MySpace was receiving an estimated 230,000 new accounts per
9 day and eventually the number of profiles exceeded 400 million with over 100 million
10 unique visitors worldwide. 11/21/08 Transcript at 74-75. “Generally speaking,”
11 MySpace would not monitor new accounts to determine if they complied with the
12 terms of service except on a limited basis, mostly in regards to photographic content.
13 Id. at 75. Sung testified that there is no way to determine how many of the 400
14 million existing MySpace accounts were created in a way that violated the MSTOS.⁹
15 Id. at 82-84. The MySpace website did have hyperlinks labelled “Safety Tips” (which
16 contained advice regarding personal, private and financial security vis-a-vis the site)
17 and “Report Abuse” (which allowed users to notify MySpace as to inappropriate
18 content and/or behavior on the site). Id. at 51-52. MySpace attempts to maintain
19 adherence to its terms of service. Id. at 60. It has different teams working in various
20 areas such as “parent care” (responding to parents’ questions about this site), handling
21 “harassment/cyberbully cases, imposter profiles,” removing inappropriate content,
22 searching for underage users, etc. Id. at 60-61. As to MySpace’s response to reports
23

24 ⁹ As stated in the MSTOS:

25 MySpace.com does not endorse and has no control over the Content.
26 Content is not necessarily reviewed by MySpace.com prior to posting and
27 does not necessarily reflect the opinions or policies of MySpace.com.
28 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.

1 of harassment:

2 It varies depending on the situation and what's being
3 reported. It can range from . . . letting the user know that if
4 they feel threatened to contact law enforcement, to us
removing the profile, and in rare circumstances we would
actually contact law enforcement ourselves.

5 Id. at 61.

6 Once a member is registered and creates his or her profile, the data is housed
7 on computer servers which are located in Los Angeles County. Id. at 53. Members
8 can create messages which can be sent to other MySpace members, but messages
9 cannot be sent to or from other Internet service providers such as Yahoo!. Id. at 54.
10 All communications among MySpace members are routed from the sender's computer
11 through the MySpace servers in Los Angeles. Id. at 54-55.

12 Profiles created by adult MySpace members are by default available to any user
13 who accesses the MySpace website. Id. at 56. The adult members can, however,
14 place privacy settings on their accounts such that only pre-authorized "friends" are
15 able to view the members' profile pages and contents. Id. For members over 16 but
16 under 18, their profiles are by default set at "private" but can be changed by the
17 member. Id. at 57. Members under 16 have a privacy setting for their profiles which
18 cannot be altered to allow regular public access. Id. To communicate with a member
19 whose profile has a privacy setting, one must initially send a "friend" request to that
20 person who would have to accept the request. Id. at 57-58. To become a "friend" of
21 a person under 16, one must not only send a "friend" request but must also know his
22 or her email address or last name. Id. at 58.

23 According to Sung, MySpace owns the data contained in the profiles and the
24 other content on the website.¹⁰ MySpace is owned by Fox Interactive Media which

25
26 ¹⁰ Technically, as delineated in the MSTOS, Exhibit 3 at pages 2-3:

27 By displaying or publishing ("posting") any Content, messages, text, files,
28 images, photos, video, sounds, profiles, works or authorship, or any other
materials (collectively, "Content") on or through the Services, you hereby

1 is part of News Corporation. Id. at 42.

2 **III. APPLICABLE LAW**

3 **A. F.R.Crim.P. 29(c)**

4 A motion for judgment of acquittal under F.R.Crim.P. 29(c) may be made by
 5 a defendant seeking to challenge a conviction on the basis of the sufficiency of the
 6 evidence, see, e.g., United States v. Freter, 31 F.3d 783, 785 (9th Cir. 1994), or on
 7 other grounds including ones involving issues of law for the court to decide, see, e.g.
 8 United States v. Pardue, 983 F.2d 843, 847 (8th Cir. 1993) (issue as to whether a
 9 defendant is entitled to a judgment of acquittal based on outrageous government
 10 conduct is “one of law for the court”). Where the Rule 29(c) motion rests in whole
 11 or in part on the sufficiency of the evidence, the evidence must be viewed “in the light
 12 most favorable to the government” (see Freter, 31 F.3d at 785), with circumstantial
 13 evidence and inferences drawn in support of the jury’s verdict. See United States v.
 14 Lewis, 787 F.2d 1318, 1323 (9th Cir. 1986).

15 **B. The CFAA**

16 In 2006, the CFAA (18 U.S.C. § 1030) provided in relevant part that:

17 (a) Whoever –
 * * * *

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

20 (A) information contained in a financial record of a
 21 financial institution, or of a card issuer as defined in section
 22 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.);

23 grant to MySpace.com, a non-exclusive, fully-paid and royalty-free,
 24 worldwide license (with the right to sublicense through unlimited levels of
 25 sublicensees) to use, copy, modify, adapt, translate, publicly perform,
 26 publicly display, store, reproduce, transmit, and distribute such Content on
 27 and through the Services. This license will terminate at the time you remove
 28 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.

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

(C) information from any protected computer if the conduct involved an 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

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 . . .

¹¹ On September 26, 2008, the Identity Theft Enforcement and Restitution Act of 2008 was 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.

1 .” Id. § 1030(e)(6).

2 In addition to providing criminal penalties for computer fraud and abuse, the
3 CFAA also states that “[A]ny person who suffers damage or loss by reason of a
4 violation of this section may maintain a civil action against the violator to obtain
5 compensatory damages and injunctive relief or other equitable relief.” 18 U.S.C. §
6 1030(g). Because of the availability of civil remedies, much of the law as to the
7 meaning and scope of the CFAA has been developed in the context of civil cases.

8 **IV. DISCUSSION**

9 **A. The Misdemeanor 18 U.S.C. § 1030(a)(2)(C) Crime Based on** 10 **Violation of a Website’s Terms of Service**

11 During the relevant time period herein,¹² the misdemeanor 18 U.S.C. §
12 1030(a)(2)(C) crime consisted of the following three elements:

13 First, the defendant intentionally [accessed without author-
14 ization] [exceeded authorized access of] a computer;

15 Second, the defendant’s access of the computer involved an
16 interstate or foreign communication; and

17 Third, by [accessing without authorization] [exceeding
18 authorized access to] a computer, the defendant obtained
19 information from a computer . . . [used in interstate or
20 foreign commerce or communication]

21 Ninth Circuit Model Criminal Jury Instruction 8.79 (2003 Ed.) (brackets in original).

22 In this case, a central question is whether a computer user’s intentional violation
23 of one or more provisions in an Internet website’s terms of services (where those
24 terms condition access to and/or use of the website’s services upon agreement to and
25 compliance with the terms) satisfies the first element of section 1030(a)(2)(C). If the
26 answer to that question is “yes,” then seemingly, any and every conscious violation
27 of that website’s terms of service will constitute a CFAA misdemeanor.

28 Initially, it is noted that the latter two elements of the section 1030(a)(2)(C)

¹² See footnote 11, supra.

1 crime will always be met when an individual using a computer contacts or
 2 communicates with an Internet website. Addressing them in reverse order, the third
 3 element requires “obtain[ing] information” from a “protected computer” - which is
 4 defined in 18 U.S.C. § 1030(e)(2)(B) as a computer “which is used in interstate or
 5 foreign commerce or communication” “Obtain[ing] information from a
 6 computer” has been described as “‘includ[ing] mere observation of the data. Actual
 7 aspiration . . . need not be proved in order to establish a violation’ S.Rep. No.
 8 99-432, at 6-7 (1986), reprinted at 1986 U.S.C.C.A.N. 2479, 2484.” Comment, Ninth
 9 Circuit Model Criminal Instructions 8.77.¹³ As for the “interstate or foreign
 10 commerce or communication” component, the Supreme Court in Reno v. American
 11 Civil Liberties Union, 521 U.S. 844, 849 (1997), observed that: “The Internet is an
 12 international network of interconnected computers.” See also Brookfield Communi-
 13 cations v. West Coast Entertainment Corp., 174 F.3d 1036, 1044 (9th Cir. 1999) (“The
 14 Internet is a global network of interconnected computers which allows individuals and
 15 organizations around the world to communicate and to share information with one
 16 another.”). The Ninth Circuit in United States v. Sutcliffe, 505 F.3d 944, 952 (9th Cir.
 17 2007), found the Internet to be “similar to - and often using - our national network of
 18 telephone lines.” It went on to conclude that:

19 We have previously agreed that “[i]t can not be
 20 questioned that the nation’s vast network of telephone lines
 21 constitutes interstate commerce,” United States v. Holder,
 22 302 F.Supp. 296, 298 (D. Mont. 1969)), aff’d and adopted,
 23 427 F.2d 715 (9th Cir. 1970) (per curiam), and, a fortiori,
 24 it seems clear that use of the internet is intimately related to
 25 interstate commerce. As we have noted, “[t]he Internet
 26 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). It is “comparable . . . to both a vast library
 including millions of readily available and indexed
 publications and a sprawling mall offering goods and

27 ¹³ As also stated in Senate Report No. 104-357, at 7 (1996), reprinted at 1996 WL 492169 (henceforth
 28 “S. Rep. No. 104-357”), “. . . the term ‘obtaining information’ includes merely reading it.”

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 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.

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., 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

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.

1 Patterson Custom Homes, 586 F.Supp.2d at 1033-34; Modis, Inc. v. Bardelli, 531
 2 F.Supp.2d 314, 318-19 (D. Conn. 2008); Charles Schwab & Co., 2005 U.S. Dist.
 3 LEXIS 21348 at *26-27. This interpretation is consistent with the legislative history
 4 of the CFAA.¹⁶ Therefore, where contact is made between an individual's computer
 5 and an Internet website, the second element is per se established.

6 As to the first element (i.e. intentionally accessing a computer without
 7 authorization or exceeding authorized access), the primary question here is whether
 8 any conscious violation of an Internet website's terms of service will cause an
 9 individual's contact with the website via computer to become "intentionally
 10 access[ing] . . . without authorization" or "exceeding authorization." Initially, it is
 11 noted that three of the key terms of the first element (i.e., "intentionally," "access a
 12 computer," and "without authorization") are undefined, and there is a considerable
 13 amount of controversy as to the meaning of the latter two phrases. See EF Cultural
 14 Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n.10 (1st Cir. 2001) ("Congress did
 15 not define the phrase 'without authorization,' perhaps assuming that the words speak
 16 for themselves. The meaning, however, has proven to be elusive."); Southwest
 17 Airlines Co. v. BoardFirst, L.L.C., 2007 U.S. Dist. LEXIS 96230 at *36 (N.D. Tex.
 18 2007) ("BoardFirst") ("The CFAA does not define the term 'access.'"); Orin S. Kerr,
 19 Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse

21 ¹⁶ For example, as stated in S. Rep. No. 104-357, at 13:

22 The bill would amend subsection 1030(e)(2) by replacing the term
 23 "Federal interest computer" with the new term "protected computer" and a
 24 new definition The new definition also replaces the current limitation
 25 in subsection 1030(e)(2)(B) of "Federal interest computer" being "one of
 26 two or more computers used in committing the offense, not all of which are
 27 located in the same State." Instead, "protected computer" would include
 28 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.

1 Statutes, 78 N.Y.U. L. Rev. 1596, 1619-21 (2003) (“Kerr, Cybercrime’s Scope”);
 2 Mark A. Lemley, Place and Cyberspace, 91 Cal. L. Rev. 521, 528-29 (2003); Dan
 3 Hunter, Cyberspace as Place and the Tragedy of the Digital Anticommons, 91 Cal. L.
 4 Rev. 439, 477 (2003).

5 While “intentionally” is undefined, the legislative history of the CFAA clearly
 6 evinces Congress’s purpose in its choice of that word. Prior to 1986, 18 U.S.C. §
 7 1030(a)(2) utilized the phrase “knowingly accesses.” See United States Code 1982
 8 Ed. Supp. III at 16-17. In the 1986 amendments to the statute, the word
 9 “intentionally” was substituted for the word “knowingly.” See 18 U.S.C.A. § 1030
 10 “Historical and Statutory Notes” at 450 (West 2000). In Senate Report No. 99-432
 11 at 5-6, reprinted at 1986 U.S.C.C.A.N. 2479, 2483-84, it was stated that:

12 Section 2(a)(1) amends 18 U.S.C. 1030(a)(2) to change the
 13 scienter requirement from “knowingly” to “intentionally,”
 14 for two reasons. First, intentional acts of unauthorized
 15 access - rather than mistaken, inadvertent, or careless ones -
 16 are precisely what the Committee intends to proscribe.
 17 Second, the Committee is concerned that the “knowingly”
 18 standard in the existing statute might be inappropriate for
 19 cases involving computer technology The substitution
 20 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.]

21 Under § 1030(a)(2)(C), the “requisite intent” is “to obtain unauthorized access of a
 22 protected computer.” United States v. Willis, 476 F.3d 1121, 1125 (10th Cir. 2007)
 23 (“The government need not also prove that . . . the information was used to any
 24 particular ends.”); see also S.Rep. No.104-357, at 7-8 (“[T]he crux of the offense
 25 under subsection 1030(a)(2)(C) . . . is abuse of a computer to obtain the
 26 information.”).

27 As to the term “accesses a computer,” one would think that the dictionary
 28 definition of verb transitive “access” would be sufficient. That definition is “to gain

1 or have access to; to retrieve data from, or add data to, a database” Webster’s
2 New World Dictionary, Third College Edition, 7 (1988) (henceforth “Webster’s New
3 World Dictionary”). Most courts that have actually considered the issue of the
4 meaning of the word “access” in the CFAA have basically turned to the dictionary
5 meaning. See e.g. BoardFirst, 2007 U.S. Dist. LEXIS 96230 at *36; Role Models
6 Am., Inc. v. Jones, 305 F. Supp. 2d 564, 566-57 (D. Md. 2004); Am. Online, Inc. v.
7 Nat’l Health Care Discount, Inc., 121 F.Supp.2d 1255, 1272-73 (N.D. Iowa 2000).
8 However, academic commentators have generally argued for a different interpretation
9 of the word. For example, as stated in Patricia L. Bellia, Defending Cyberproperty,
10 79 N.Y.U. L. Rev. 2164, 2253-54 (2004):

11 We can posit two possible readings of the term “access.”
12 First, it is possible to adopt a broad reading, under which
13 “access” means any interaction between two computers. In
14 other words, “accessing” a computer simply means
15 transmitting electronic signals to a computer that the
16 computer processes in some way. A narrower under-
17 standing of “access” would focus not merely on the
18 successful exchange of electronic signals, but rather on
19 conduct by which one is in a position to obtain privileges or
20 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, only
breach of a code-based restriction on the system would
qualify.

21 Professor Bellia goes on to conclude that “[c]ourts would better serve both the
22 statutory intent of the CFAA and public policy by limiting its application to unwanted
23 uses only in connection with code-based controls on access.” Id. at 2258. But see
24 Kerr, Cybercrime’s Scope, 78 N.Y.U. L. Rev. at 1619-21, 1643, and 1646-48 (arguing
25 for a “broad construction of access as any successful interaction with the
26 computer”). It is simply noted that, while defining “access” in terms of a code-based
27
28

1 restriction might arguably be a preferable approach, no case has adopted it¹⁷ and the
2 CFAA legislative history does not support it.

3 As to the term “without authorization,” the courts that have considered the
4 phrase have taken a number of different approaches in their analysis. See generally
5 Kerr, Cybercrime’s Scope, 78 N.Y.U. L. Rev. at 1628-40. Those approaches are
6 usually based upon analogizing the concept of “without authorization” as to
7 computers to a more familiar and mundane predicate presented in or suggested by the
8 specific factual situation at hand. See e.g. United States v. Phillips, 477 F.3d 215, 219
9 (5th Cir.), cert. denied, 128 S.Ct. 119 (2007), (“Courts have therefore typically
10 analyzed the scope of a user’s authorization to access a protected computer on the
11 basis of the expected norms of intended use or the nature of the relationship
12 established between the computer owner and the user.”). Thus, for example, where
13 a case arises in the context of employee misconduct, some courts have treated the
14 issue as falling within an agency theory of authorization. See, e.g., International
15 Airport Centers, L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006); Shurgard
16 Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F.Supp.2d 1121, 1124-25
17 (W.D. Wash. 2000). Likewise, the Ninth Circuit (in dealing with the issue of
18 purported consent to access emails pursuant to a subpoena obtained in bad faith in the
19 context of the Stored Communications Act, 18 U.S.C. § 2701 et seq., and the CFAA)
20 applied the law of trespass to determine whether a subpoenaed party had effectively
21 authorized the defendants’ access. See Theofel v. Farey-Jones, 359 F.3d 1066, 1072-
22 75, 1078 (9th Cir. 2004). Further, where the relationship between the parties is
23 contractual in nature or resembles such a relationship, access has been held to be
24 unauthorized where there has been an ostensible breach of contract. See e.g., EF
25 Cultural Travel BV, 274 F.3d at 583-84; Phillips, 477 F.3d at 221 (“[c]ourts have

26
27 ¹⁷ But see BoardFirst, 2007 U.S. Dist. LEXIS 96230 at *43-44 (“§ 1030(a)(2)(C). However, the
28 BoardFirst court did not adopt a “code-based” definition of “accessing without authorization” but requested further briefing on the issue.

1 recognized that authorized access typically arises only out of a contractual or agency
2 relationship.”). But see Brett Senior & Associates v. Fitzgerald, 2007 U.S. Dist.
3 LEXIS 50833 at *13-14 (E.D. Pa. 2007) (observing - in the context of an employee’s
4 breach of a confidentiality agreement when he copied information from his firm’s
5 computer files to give to his new employer: “It is unlikely that Congress, given its
6 concern ‘about the appropriate scope of Federal jurisdiction’ in the area of computer
7 crime, intended essentially to criminalize state-law breaches of contract.”).

8 Within the breach of contract approach, most courts that have considered the
9 issue have held that a conscious violation of a website’s terms of service/use will
10 render the access unauthorized and/or cause it to exceed authorization. See, e.g.,
11 Southwest Airlines Co. v. Farechase, Inc., 318 F.Supp.2d 435, 439-40 (N.D. Tex.
12 2004); Nat’l Health Care Disc., Inc., 174 F.Supp.2d at 899; Register.com, Inc. v.
13 Verio, Inc., 126 F.Supp.2d 238, 247-51 (S.D.N.Y. 2000), aff’d, 356 F.3d 393 (2d Cir.
14 2004); Am. Online, Inc. v. LCGM, Inc., 46 F.Supp.2d 444, 450 (E.D. Va. 1998); see
15 also EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62-63 (1st Cir. 2003) (“A
16 lack of authorization could be established by an explicit statement on the website
17 restricting access [W]e think that the public website provider can easily spell out
18 explicitly what is forbidden”). But see BoardFirst, 2007 U.S. Dist. LEXIS 96230
19 at *40 (noting that the above cases and their particular application of the law “have
20 received their share of criticism from commentators”). The court in BoardFirst further
21 stated:

22 [I]t is at least arguable here that BoardFirst’s access
23 of the Southwest website is not at odds with the site’s
24 intended function; after all, the site is designed to allow
25 users to obtain boarding passes for Southwest flights via the
26 computer. In no sense can BoardFirst be considered an
27 “outside hacker[] who break[s] into a computer” given that
28 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 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).

In this particular case, as conceded by the Government,¹⁹ the only basis for finding that Drew intentionally accessed MySpace’s 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(b)(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.

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

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.

¹⁹ See Reporter’s Transcript of July 2, 2009 Hearing at 3-4.

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 accessor 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.”

1 indicates that Congress intended for them to have specialized meanings.²¹ As
2 delineated in Webster's New World Dictionary at 92, to "authorize" ordinarily means
3 "to give official approval to or permission for"

4 It cannot be considered a stretch of the law to hold that the owner of an Internet
5 website has the right to establish the extent to (and the conditions under) which
6 members of the public will be allowed access to information, services and/or
7 applications which are available on the website. See generally Phillips, 477 F.3d at
8 219-21; EF Cultural Travel BV, 318 F.3d at 62; Register.com, Inc., 126 F.Supp.2d at
9 245-46; CompuServe Inc. v. Cyber Promotions, Inc., 962 F.Supp. 1015, 1023-24
10 (S.D. Ohio 1997). Nor can it be doubted that the owner can relay and impose those
11 limitations/restrictions/conditions by means of written notice such as terms of service
12 or use provisions placed on the home page of the website. See EF Cultural Travel
13 BV, 318 F.3d at 62-63. While issues might be raised in particular cases as to the
14 sufficiency of the notice and/or sufficiency of the user's assent to the terms, see
15 generally Specht v. Netscape Communications Corp., 306 F.3d 17, 30-35 (2d Cir.
16 2002); BoardFirst, 2007 U.S. Dist. LEXIS 96230 at *11-21, and while public policy
17 considerations might in turn limit enforcement of particular restrictions, see EF
18 Cultural Travel BV, 318 F.3d at 62, the vast majority of the courts (that have
19 considered the issue) have held that a website's terms of service/use can define what
20 is (and/or is not) authorized access vis-a-vis that website.

21 Here, the MSTOS defined "services" as including "the MySpace.com Website
22 . . . , the MySpace.com instant messenger, and any other connection with the Website
23" See Exhibit 3 at 1. It further notified the public that the MSTOS "sets forth the
24

25 See S.Rep. No. 99-432, at 13 (1986), reprinted at 1986 U.S.C.C.A.N. 2479, 2491.

26 ²¹ Commentators have criticized the legislatures' understandings of computers and the accessing of
27 computers as "simplistic" and based upon the technology in existence in the 1970's and 1980's (e.g. pre-
28 Internet) rather than upon what currently exists. See, e.g., Kerr, Cybercrime's Scope, 78 N.Y.U. L. Rev. at
1640-41.

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

B. Contravention of the Void-for-Vagueness Doctrine

1. Applicable Law

Justice Holmes observed that, as to criminal statutes, there is a “fair warning”

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; 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; 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).

1 requirement. As he stated in McBoyle v. United States, 283 U.S. 25, 27 (1931):

2 Although it is not likely that a criminal will carefully
3 consider the text of the law before he murders or steals, it
4 is reasonable that a fair warning should be given to the
5 world in language that the common world will understand,
6 of what the law intends to do if a certain line is passed. To
7 make the warning fair, so far as possible the line should be
8 clear.

9 As further elaborated by the Supreme Court in United States v. Lanier, 520 U.S. 259,
10 266 (1997):

11 There are three related manifestations of the fair
12 warning requirement. First, the vagueness doctrine bars
13 enforcement of “a statute which either forbids or requires
14 the doing of an act in terms so vague that men of common
15 intelligence must necessarily guess at its meaning and differ
16 as to its application.” Connally v. General Constr. Co., 269
17 U.S. 385, 391 (1926) Second, as a sort of “junior
18 version of the vagueness doctrine,” H. Packer, *The Limits*
19 *of the Criminal Sanction* 95 (1968), the canon of strict
20 construction of criminal statutes, or rule of lenity, ensures
21 fair warning by so resolving ambiguity in a criminal statute
22 as to apply it only to conduct clearly covered Third,
23 although clarity at the requisite level may be supplied by
24 judicial gloss on an otherwise uncertain statute, . . . due
25 process bars courts from applying a novel construction of
26 a criminal statute to conduct that neither the statute nor any
27 prior judicial decision has fairly disclosed to be within its
28 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.]

19 The void-for-vagueness doctrine has two prongs: 1) a definitional/notice
20 sufficiency requirement and, more importantly, 2) a guideline setting element to
21 govern law enforcement. In Kolender v. Lawson, 461 U.S. 352, 357-58 (1983), the
22 Court explained that:

23 As generally stated, the void-for-vagueness doctrine
24 requires that a penal statute define the criminal offense with
25 sufficient definiteness that ordinary people can understand
26 what conduct is prohibited and in a manner that does not
27 encourage arbitrary and discriminatory enforcement
28 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 guidelines to govern law enforcement.”

1 Smith [v. Goguen], 415 U.S. [566,] 574 [1974]. Where the
 2 legislature fails to provide such minimal guidelines, a
 3 criminal statute may permit “a standardless sweep [that]
 4 allows policemen, prosecutors, and juries to pursue their
 5 personal predilections.” Id. at 575. [Footnote and citations
 6 omitted.]

7 To avoid contraving the void-for-vagueness doctrine, the criminal statute must
 8 contain “relatively clear guidelines as to prohibited conduct” and provide “objective
 9 criteria” to evaluate whether a crime has been committed. Gonzalez v. Carhart, 550
 10 U.S. 124, 149 (2007) (quoting Posters ‘N’ Things, Ltd. v. United States, 511 U.S. 513,
 11 525-26 (1994)). As stated in Connally v. General Construction Co., 269 U.S. 385,
 12 391-92 (1926):

13 The question whether given legislative enactments have
 14 been thus wanting in certainty has frequently been before
 15 this court. In some of the cases the statutes involved were
 16 upheld; in others, declared invalid. The precise point of
 17 differentiation in some instances is not easy of statement.
 18 But it will be enough for present purposes to say generally
 19 that the decisions of the court upholding statutes as
 20 sufficiently certain, rested upon the conclusion that they
 21 employed words or phrases having a technical or other
 22 special meaning, well enough known to enable those within
 23 their reach to correctly apply them, . . . or a well-settled
 24 common law meaning, notwithstanding an element of
 25 degree in the definition as to which estimates might differ,
 26 . . . or, as broadly stated . . . in United States v. Cohen
 27 Grocery Co., 255 U.S. 81, 92, “that, for reasons found to
 28 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.]

20 However, a “difficulty in determining whether certain marginal offenses are within
 21 the meaning of the language under attack as vague does not automatically render a
 22 statute unconstitutional for indefiniteness . . . Impossible standards of specificity are
 23 not required.” Jordan v. De George, 341 U.S. 223, 231 (1951) (citation and footnote
 24 omitted). “What renders a statute vague is not the possibility that it will sometimes
 25 be difficult to determine whether the incriminating fact it establishes has been proved;
 26 but rather the indeterminacy of precisely what that fact is.” United States v. Williams,
 27 ____ U.S. ____, 128 S.Ct. 1830, 1846 (2008). In this regard, the Supreme Court “has
 28 made clear that scienter requirements alleviate vagueness concerns.” Gonzales, 550

1 U.S. at 149; see also Colautti v. Franklin, 439 U.S. 379, 395 (1979) (“This Court has
2 long recognized that the constitutionality of a vague statutory standard is closely
3 related to whether that standard incorporates a requirement of *mens rea*”).

4 “It is well established that vagueness challenges to statutes which do not
5 involve First Amendment freedoms must be examined in the light of the facts of the
6 case at hand.” United States v. Mazurie, 419 U.S. 544, 550 (1975); United States v.
7 Purdy, 264 F.3d 809, 811 (9th Cir. 2001). “Whether a statute is . . . unconstitutionally
8 vague is a question of law” United States v. Ninety-Five Firearms, 28 F.3d 940,
9 941 (9th Cir. 1994).

10 **2. Definitional/Actual Notice Deficiencies**

11 The pivotal issue herein is whether basing a CFAA misdemeanor violation as
12 per 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A) upon the conscious violation of a
13 website’s terms of service runs afoul of the void-for-vagueness doctrine. This Court
14 concludes that it does primarily because of the absence of minimal guidelines to
15 govern law enforcement, but also because of actual notice deficiencies.

16 As discussed in Section IV(A) above, terms of service which are incorporated
17 into a browsewrap or clickwrap agreement can, like any other type of contract, define
18 the limits of authorized access as to a website and its concomitant computer/server(s).
19 However, the question is whether individuals of “common intelligence” are on notice
20 that a breach of a terms of service contract can become a crime under the CFAA.
21 Arguably, they are not.

22 First, an initial inquiry is whether the statute, as it is written, provides sufficient
23 notice. Here, the language of section 1030(a)(2)(C) does not explicitly state (nor does
24 it implicitly suggest) that the CFAA has “criminalized breaches of contract” in the
25 context of website terms of service. Normally, breaches of contract are not the subject
26 of criminal prosecution. See generally United States v. Handakes, 286 F.3d 92, 107
27 (2d Cir. 2002), overruled on other grounds in United States v. Rybicki, 354 F.3d 124,
28 144 (2d Cir. 2003) (en banc). Thus, while “ordinary people” might expect to be

1 exposed to civil liabilities for violating a contractual provision, they would not expect
 2 criminal penalties.²³ Id. This would especially be the case where the services
 3 provided by MySpace are in essence offered at no cost to the users and, hence, there
 4 is no specter of the users “defrauding” MySpace in any monetary sense.²⁴

5 Second, if a website’s terms of service controls what is “authorized” and what
 6 is “exceeding authorization” - which in turn governs whether an individual’s
 7 accessing information or services on the website is criminal or not, section
 8 1030(a)(2)(C) would be unacceptably vague because it is unclear whether any or all
 9 violations of terms of service will render the access unauthorized, or whether only
 10 certain ones will. For example, in the present case, MySpace’s terms of service
 11 prohibits a member from engaging in a multitude of activities on the website,
 12 including such conduct as “criminal or tortious activity,” “gambling,” “advertising to
 13 . . . any Member to buy or sell any products,” “transmit[ting] any chain letters,”
 14 “covering or obscuring the banner advertisements on your personal profile page,”
 15 “disclosing your password to any third party,” etc. See Exhibit 3 at 5. The MSTOS
 16 does not specify which precise terms of service, when breached, will result in a
 17 termination of MySpace’s authorization for the visitor/member to access the website.
 18 If any violation of any term of service is held to make the access unauthorized, that
 19 strategy would probably resolve this particular vagueness issue; but it would, in turn,
 20 render the statute incredibly overbroad and contravene the second prong of the void-
 21
 22
 23

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
 25 Cir. 2008), cert. denied, 129 S.Ct. 1308 (2009) (“[S]imply because . . . actions can be considered violations
 26 of the ‘contract’ . . . does not mean that those same actions do not qualify as violations of [a criminal]
 statute.”).

27 ²⁴ Also, it is noted here that virtually all of the decisions which have found a breach of a website’s terms
 28 of service to be a sufficient basis to establish a section 1030(a)(2)(C) violation have been in civil actions, not
 criminal cases.

1 for-vagueness doctrine as to setting guidelines to govern law enforcement.²⁵

2 Third, by utilizing violations of the terms of service as the basis for the section
3 1030(a)(2)(C) crime, that approach makes the website owner - in essence - the party
4 who ultimately defines the criminal conduct. This will lead to further vagueness
5 problems. The owner's description of a term of service might itself be so vague as to
6 make the visitor or member reasonably unsure of what the term of service covers. For
7 example, the MSTOS prohibits members from posting in "band and filmmaker
8 profiles . . . sexually suggestive imagery or any other unfair . . . [c]ontent intended to
9 draw traffic to the profile." Exhibit 3 at 4. It is unclear what "sexually suggestive
10 imagery" and "unfair content"²⁶ mean. Moreover, website owners can establish terms
11 where either the scope or the application of the provision are to be decided by them
12 *ad hoc* and/or pursuant to undelineated standards. For example, the MSTOS provides
13 that what constitutes "prohibited content" on the website is determined "in the sole
14 discretion of MySpace.com" *Id.* Additionally, terms of service may allow the
15 website owner to unilaterally amend and/or add to the terms with minimal notice to
16 users. See, e.g., id. at 1.

17 Fourth, because terms of service are essentially a contractual means for setting
18 the scope of authorized access, a level of indefiniteness arises from the necessary
19 application of contract law in general and/or other contractual requirements within the
20 applicable terms of service to any criminal prosecution. For example, the MSTOS has
21 a provision wherein "any dispute" between MySpace and a visitor/member/user
22 arising out of the terms of service is subject to arbitration upon the demand of either
23 party. Before a breach of a term of service can be found and/or the effect of that
24 breach upon MySpace's ability to terminate the visitor/member/user's access to the

25
26 ²⁵ Another uncertainty is whether, once a user breaches a term of service, is every subsequent accessing
27 of the website by him or her without authorization or in excess of authorization.

28 ²⁶ See Time Warner Entm't Co., L.P. v. FCC, 240 F.3d 1126, 1135 (D.C. Cir. 2001) ("The word 'unfair'
is of course extremely vague.").

1 site can be determined, the issue would be subject to arbitration.²⁷ Thus, a question
 2 arises as to whether a finding of unauthorized access or in excess of authorized access
 3 can be made without arbitration.

4 Furthermore, under California law,²⁸ a material breach of the MSTOS by a
 5 user/member does not automatically discharge the contract, but merely “excuses the
 6 injured party’s performance, and gives him or her the election of certain remedies.”
 7 1 Witkin, Summary of California Law (Tenth Ed.): Contracts § 853 at 940 (2008).
 8 Those remedies include rescission and restitution, damages, specific performance,
 9 injunction, declaratory relief, etc. Id. The contract can also specify particular
 10 remedies and consequences in the event of a breach which are in addition to or a
 11 substitution for those otherwise afforded by law. Id. at § 855 at 942. The MSTOS
 12 does provide that: “MySpace.com reserves the right, in its sole discretion . . . to
 13 restrict, suspend, or terminate your access to all or part of the services at any time, for
 14 any or no reason, with or without prior notice, and without liability.” Exhibit 3 at 2.
 15 However, there is no provision which expressly states that a breach of the MSTOS
 16 automatically results in the termination of authorization to access the website. Indeed,
 17 the MSTOS cryptically states: “you are only authorized to use the Services . . . if you
 18 agree to abide by all applicable laws and to this Agreement.” Id. at 1 (emphasis
 19 _____

20 ²⁷ An arbitration clause is considered to be “broad” when it contains language to the effect that
 21 arbitration is required for “any” claim or dispute which “arises out of” the agreement. Fleet Tire Service v.
 22 Oliver Rubber Co., 118 F.3d 619, 621 (8th Cir. 1997); see also Schoendube Corp. v. Lucent Technologies,
 23 Inc., 442 F.3d 727, 729 (9th Cir. 2006). Where a broad arbitration clause is in effect, “even the question of
 24 whether the controversy relates to the agreement containing the clause is subject to arbitration.” Fleet Tire
 25 Service, 118 F.3d at 621. Moreover, “[a]n agreement to arbitrate ‘any dispute’ without strong limiting or
 26 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 (1986).

27 ²⁸ According to the MSTOS, “If there is any dispute about or involving the Services, you agree that the
 28 dispute shall be governed by the laws of the State of California without regard to conflict of law provisions
 . . .” Exhibit 3 at 7.

1 added).

2 **3. The Absence of Minimal Guidelines to Govern Law Enforcement**

3 Treating a violation of a website's terms of service, without more, to be
4 sufficient to constitute "intentionally access[ing] a computer without authorization or
5 exceed[ing] authorized access" would result in transforming section 1030(a)(2)(C)
6 into an overwhelmingly overbroad enactment that would convert a multitude of
7 otherwise innocent Internet users into misdemeanor criminals. As noted in Section
8 IV(A) above, utilizing a computer to contact an Internet website by itself will
9 automatically satisfy all remaining elements of the misdemeanor crime in 18 U.S.C.
10 §§ 1030(a)(2)(C) and 1030(c)(2)(A). Where the website's terms of use only
11 authorizes utilization of its services/applications upon agreement to abide by those
12 terms (as, for example, the MSTOS does herein), any violation of any such provision
13 can serve as a basis for finding access unauthorized and/or in excess of authorization.

14 One need only look to the MSTOS terms of service to see the expansive and
15 elaborate scope of such provisions whose breach engenders the potential for criminal
16 prosecution. Obvious examples of such breadth would include: 1) the lonely-heart
17 who submits intentionally inaccurate data about his or her age, height and/or physical
18 appearance, which contravenes the MSTOS prohibition against providing
19 "information that you know is false or misleading"; 2) the student who posts candid
20 photographs of classmates without their permission, which breaches the MSTOS
21 provision covering "a photograph of another person that you have posted without that
22 person's consent"; and/or 3) the exasperated parent who sends out a group message
23 to neighborhood friends entreating them to purchase his or her daughter's girl scout
24 cookies, which transgresses the MSTOS rule against "advertising to, or solicitation
25 of, any Member to buy or sell any products or services through the Services." See
26 Exhibit 3 at 4. However, one need not consider hypotheticals to demonstrate the
27 problem. In this case, Megan (who was then 13 years old) had her own profile on
28 MySpace, which was in clear violation of the MSTOS which requires that users be

1 “14 years of age or older.” Id. at 2. No one would seriously suggest that Megan’s
2 conduct was criminal or should be subject to criminal prosecution.

3 Given the incredibly broad sweep of 18 U.S.C. §§ 1030(a)(2)(C) and
4 1030(c)(2)(A), should conscious violations of a website’s terms of service be deemed
5 sufficient by themselves to constitute accessing without authorization or exceeding
6 authorized access, the question arises as to whether Congress has “establish[ed]
7 minimal guidelines to govern law enforcement.” Kolender, 461 U.S. at 358; see also
8 City of Chicago v. Morales, 527 U.S. 41, 60 (1999). Section 1030(a)(2)(C) does not
9 set forth “clear guidelines” or “objective criteria” as to the prohibited conduct in the
10 Internet/website or similar contexts. See generally Posters ‘N’ Things, Ltd., 511 U.S.
11 at 525-26. For instance, section 1030(a)(2)(C) is not limited to instances where the
12 website owner contacts law enforcement to complain about an individual’s
13 unauthorized access or exceeding permitted access on the site.²⁹ Nor is there any
14 requirement that there be any actual loss or damage suffered by the website or that
15 there be a violation of privacy interests.

16 The Government argues that section 1030(a)(2)(C) has a scienter requirement
17 which dispels any definitional vagueness and/or dearth of guidelines, citing to United
18 States v. Sablan, 92 F.3d 865 (9th Cir. 1996). The Court in Sablan did observe that:

19 [T]he computer fraud statute does not criminalize other-
20 wise innocent conduct. Under the statute, the Government
21 must prove that the defendant intentionally accessed a
22 federal interest computer without authorization. Thus,
23 Sablan must have had a wrongful intent in accessing the
24 computer in order to be convicted under the statute. This
25 case does not present the prospect of a defendant being
26 convicted without any wrongful intent as was the situation
27 in [United States v.] X-Citement Video [513 U.S. 64, 71-73
28 (1994)].

Id. at 869. However, Sablan is easily distinguishable from the present case as it: 1)

²⁹ Here, the prosecution was not initiated based on a complaint or notification from MySpace to law enforcement officials.

1 did not involve the defendant's accessing an Internet website;³⁰ 2) did not consider the
2 void-for-vagueness doctrine but rather the *mens rea* requirement; and 3) dealt with a
3 different CFAA subsection (i.e. 18 U.S.C. § 1030(a)(5)) and in a felony situation.

4 The only scienter element in section 1030(a)(2)(C) is the requirement that the
5 person must "intentionally" access a computer without authorization or "intentionally"
6 exceed authorized access. It has been observed that the term "intentionally" itself can
7 be vague in a particular statutory context. See, e.g., American Civil Liberties Union
8 v. Gonzales, 478 F.Supp.2d 775, 816-17 (E.D. Pa. 2007), aff'd, 534 F.3d 181, 205
9 (3rd Cir. 2008), cert. denied, 129 S.Ct. 1032 (2009).

10 Here, the Government's position is that the "intentional" requirement is met
11 simply by a conscious violation of a website's terms of service. The problem with
12 that view is that it basically eliminates any limiting and/or guiding effect of the
13 scienter element. It is unclear that every intentional breach of a website's terms of
14 service would be or should be held to be equivalent to an intent to access the site
15 without authorization or in excess of authorization. This is especially the case with
16 MySpace and similar Internet venues which are publically available for access and
17 use. See generally BoardFirst, 2007 U.S. Dist. LEXIS 96230 at *43. However, if
18 every such breach does qualify, then there is absolutely no limitation or criteria as to
19 which of the breaches should merit criminal prosecution. All manner of situations
20 will be covered from the more serious (e.g. posting child pornography) to the more
21 trivial (e.g. posting a picture of friends without their permission). All can be
22 prosecuted. Given the "standardless sweep" that results, federal law enforcement
23
24

25 ³⁰ In Sablan, the defendant was a bank employee who had been recently fired for circumventing its
26 security procedures in retrieving files. Early one morning, she entered the closed bank through an unlocked
27 door and, using an unreturned key, went to her former work site. Utilizing an old password, she logged onto
28 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.

1 entities would be improperly free “to pursue their personal predilections.”³¹ Kolender,
2 461 U.S. at 358 (citing Smith v. Goguen, 415 U.S. 566, 575 (1994)).

3 In sum, if any conscious breach of a website’s terms of service is held to be
4 sufficient by itself to constitute intentionally accessing a computer without authori-
5 zation or in excess of authorization, the result will be that section 1030(a)(2)(C)
6 becomes a law “that affords too much discretion to the police and too little notice to
7 citizens who wish to use the [Internet].” City of Chicago, 527 U.S. at 64.

8 **V. CONCLUSION**

9 For the reasons stated above, the Defendant’s motion under F.R.Crim.P. 29(c)
10 is GRANTED.

11
12 DATED: This 28th day of August, 2009

13
14 

15 _____
16 GEORGE H. WU
17 United States District Judge
18
19
20
21
22
23
24
25

26
27 ³¹ In comparison, the felony violation of 18 U.S.C. § 1030(a)(2)(C) contains effective scienter elements
28 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 crime or tortious act
which, in turn, will normally contain additional scienter and/or wrongful intent conditions.