United States v. Drew, CR 08-0582-GW

This case raises the issue of whether (and/or when will) violations of an Internet website's terms of service constitute a crime under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030.

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 agreed to intentionally access a computer used in interstate commerce without (and/or in excess of) authorization inorder 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. 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. 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. On or about October 7, 2006, the conspirators had "Josh" inform Megan that he was moving away. 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 her in it." Later on that same day, after learning that Megan had killed herself, Drew caused the Josh Evans MySpace account to be deleted.

MySpace is a "social networking" website where members can create "profiles" and interact with other members. 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. In addition, the individual had to check on the box indicating that "You agree to the MySpace Terms of Service and Privacy Policy" ("MSTOS").
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…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…
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.

The MSTOS prohibited the posting of a wide range of content on the website including (but not limited to) material that: "provides information that you know is false or misleading or promotes illegal activities or conduct that is abusive, threatening, obscene, defamatory or libelous"; "includes a photograph of another person that you have posted without that person's consent"; or "involves commercial activities and/or sales without our prior written consent." Further, MySpace was allowed to unilaterally modify the terms of service, with such modifications taking effect upon the posting of notice on its website.

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 worldwide. "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.

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 history) which indicates that Congress intended for them to have specialized meanings. As delineated in Webster's New World Dictionary at 92, to "authorize" ordinarily means "to give official approval to or permission for …" 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. Nor can it be doubted that the owner can relay and impose 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.

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, and while public policy considerations might in turn limit enforcement of particular restrictions, 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.

In Kolender v. Lawson, 461 U.S. 352, 357-58 (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 guidelines to govern law enforcement…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."

The pivotal issue herein is whether basing a CFAA misdemeanor 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 because of actual notice deficiencies.

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. Thus, while "ordinary people" might expect to be exposed to civil liabilities for violating a contractual provision, they would not expect criminal penalties.

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. 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.

Third, by utilizing violations of the terms of service as 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. 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.

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 misdemeanant criminals.

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 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."

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." No one would seriously suggest that Megan's conduct was criminal or should be subject to criminal prosecution.

If every such breach [of the a site's Terms of Service] 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.

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 much discretion to the police and too little notice to citizens who wish to use the [Internet]."

For the reasons stated above, the Defendant's motion [to dismiss] is GRANTED.