CINDY A. COHN (California Bar No. 145997)
cindy@eff.org
JENNIFER STISA GRANICK (California Bar No. 168423)
jennifer@eff.org
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x134
Fax: (415) 436-9993 (fax)

Attorney for *Amicus Curiae*
Electronic Frontier Foundation

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

FACEBOOK, Plaintiff, v. POWER VENTURES, Defendant.	Case No. 5:08-cv-05780 JW **BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT POWER VENTURES' MOTION FOR SUMMARY JUDGMENT ON CAL. PENAL CODE 502(C)** Date: June 7, 2010 Time: 1:30 p.m. Dep't: Hon. Judge James Ware

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

STATEMENT OF INTEREST OF *AMICUS CURIAE*

Amicus Electronic Frontier Foundation's interest in this case is the sound and principled interpretation and application of the California computer crime statute, California Penal Code § 502(c). *Amicus* believes that this brief may assist the Court in its consideration of consumer interests in this matter, as well as the proper scope of section 502(c).

Electronic Frontier Foundation ("EFF") is a non-profit, member-supported digital civil liberties organization. As part of its mission, EFF has served as counsel or *amicus* in key cases addressing user rights to free speech, privacy, and innovation as applied to the Internet and other new technologies. With more than 14,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age, and publishes a comprehensive archive of digital civil liberties information at one of the most linked-to web sites in the world, www.eff.org.

I. INTRODUCTION AND FACTS

A. Summary Of The Argument

Power Ventures sought to provide Facebook users with a tool that could, at the users' direction, aggregate their Facebook inbox messages, friend lists and other data with messages and lists from other social networks the individual patronizes, such as Orkut or LinkedIn. Power's product allowed Facebook users to view all of their different social network data in one place. Facebook users benefited from the choice Power offered them in how to access and use their social network data across several different social networks.

Facebook argues that by offering these enhanced services to users, Power violated California's computer crime law. It grounds its claim in the fact that Facebook's terms of service prohibit a user from having automated access to a user's own information and that Power continued to offer the service to Facebook users even after Facebook sent Power a cease and desist letter demanding that it stop. Yet merely providing a technology to assist a user in accessing his or her own data in a novel manner cannot and should not form the basis for criminal liability.

To hold otherwise, as Facebook asks this court to do, will create a massive expansion of the scope of California criminal law, hinging liability on arbitrary and often confusing terms chosen by private parties in the contracts of adhesion they present to users. This creates both legal uncertainty and the risk of capricious enforcement. It will also hobble user choice and interfere with follow-on innovation, in part by creating a barrier to Facebook users who wish to move their data from Facebook to a competing service.

While users who choose services such as Power's may breach Facebook's terms of use (if those terms are otherwise enforceable), breaches of these sorts of private contracts should not be turned into criminal conduct. Indeed, if Facebook's proposed construction of section 502(c) in this case is correct, millions of otherwise innocent Internet users are potentially violating criminal law through routine online behavior. Similarly, allowing a private party to define criminal conduct puts far too much power in the hands of business entities that are not necessarily acting in the public interest.

For these reasons, *amicus* urges the Court to grant summary judgment in favor of Power on Facebook's section 502(c) claims.

B. Facebook's Service.

Social networks are Internet-based services that enable individuals to share their personal information and to communicate with friends, family and acquaintances. Facebook, like other social networks, allows its users to store their own information on Facebook's servers using Facebook's web interface for uploading and viewing the information. The tools allow Facebook users to make lists of friends, publish status updates, post photographs, and create common interest groups.[1]

Facebook has been wildly successful at acquiring users. The service claimed over 400 million active users[2] and 134 million unique visitors in the month of January 2010 alone.[3] In February 2010, Facebook had 49.62% of the US market share of visits to social-networking websites and forums.[4] In March 2010, Facebook was the single most visited website in the United States.[5] Facebook reports that people spend over 500 billion minutes per month on the service.[6] By the company's CEO's favored measure of success, if Facebook were a country it would be the third largest in the world.[7]

Importantly, Facebook users own the information they store with the company. The company's terms of service confirm this and it is not subject to dispute here.[8] Moreover, ownership

---

[1] Facebook Factsheet, http://www.facebook.com/press/info.php?factsheet (last visited Apr. 30, 2010).

[2] Facebook Statistics, http://www.facebook.com/press/info.php?statistics (last visited Apr. 30, 2010.)

[3] Aaron Prebluda, We're Number Two! Facebook Moves Up One Big Spot in the Charts (Feb. 17, 2010), http://blog.compete.com/2010/02/17/we%25e2%2580%2599re-number-two-facebook-moves-up-one-big-spot-in-the-charts/.

[4] Marketing Charts, Top 10 Social-Networking Websites & Forums (Feb. 2010), http://www.marketingcharts.com/interactive/top-10-social-networking-websites-forums-february-2010-12248/.

[5] Heather Dougherty, Facebook Reaches Top Ranking in US (March 15, 2010), http://weblogs.hitwise.com/heather-dougherty/2010/03/facebook_reaches_top_ranking_i.html.

[6] Facebook Statistics, *supra*, note 2.

[7] John D. Sutter, Facebook Gives Itself a Birthday Face-Lift (Feb. 5, 2010), http://www.cnn.com/2010/TECH/02/05/facebook.birthday/index.html.

[8] Facebook's Statement of Rights and Responsibilities confirms: "You own all of the content and information you post on Facebook" and "[f]or content that is covered by intellectual property rights, like photos and videos ("IP content"), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-

and control are extremely important to Facebook users, as the company learned in February of 2009 when it modified its terms of use to give Facebook the right to continue to use content indefinitely even after a user attempted to delete it or leave the service entirely. After a huge outcry, the company backpedaled, and reinstituted the old terms that allowed users to delete their content from the site.[9]

As part of its business model, Facebook has also been steadily increasing the amount of information about its users and their activities it offers to third parties. Through changes to its terms of service and the functionality of its Application Programming Interface or API, through which third parties can see Facebook user's information and activities, Facebook now offers to certain third parties and advertisers as much information about any particular user and his or her friends as that user themselves could access using Power's service.[10] Thus, by continuing to press for Power to be liable under criminal law, Facebook's actions appear to be aimed not at protecting users from the sharing of their information, but at ensuring their own control (and the corresponding ability to monetize) user information, even against the users themselves.

C. Power's Service

Power's service allows individuals with valid accounts on social networks to aggregate their information stored with each service, giving them the ability to view their data and friends lists, as well as other information, across multiple services on a single screen. The user can then click through the Power interface to go to any of her social networks, including Facebook, and thereafter interact with them through that network's user interface. Power's service is a follow-on innovation to social networking platforms, giving the user more options to view their own information posted to such services. For instance, Power's service allows a user to see all of their

---

licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ("IP License"). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it." Facebook Statement of Rights and Responsibilities § 2 (Apr. 22, 2010), http://www.facebook.com/facebook?ref=pf#!/terms.php?ref=pf.

[9] Bill Meyer, Facebook Data-Retention Changes Spark Protest (Feb. 17, 2010), http://www.cleveland.com/nation/index.ssf/2009/02/facebook_dataretention_changes.html.

[10] *See*, *e.g.*, Erick Schonfeld, Microsoft Taps Into Facebook's Open Graph to Launch Docs.com (Apr. 21, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/04/21/AR2010042103128.html; Matt Rosoff, Pandora and Facebook Get Social Music Right (Apr. 22, 2010), http://news.cnet.com/8301-13526_3-20003210-27.html.

friends and contacts in a single list, regardless of which social network they use. Power also offers users a tool by which users can easily export their information social networks into a spreadsheet format, thus aiding users who might want to move their information from one social network to another.

D. Facebook's Section 502(c) Claims

Facebook's argument that Power has violated California Penal Code section 502(c) is essentially (1) that the network's terms of service prohibit automated access to a user's information, and (2) that the network sent Power a cease and desist letter demanding that it stop providing its service to users.[11]

First, Facebook relies on two of its Terms of Service that provide:

> 3.2. You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our permission.
>
> and
>
> 3.5. You will not solicit login information or access an account belonging to someone else.[12]

Facebook's Complaint asserts that Power:

> 43. "use[s] other users' accounts to access Facebook's computer systems," …
>
> 49. "use[s] automated scripts to collect information from or otherwise interact with the |Facebook's website or to access Facebook's computers for the purpose of scraping user data from Facebook and displaying it on Power.com.

In other words, Facebook claims that Power commits a crime when Facebook users choose to use Power's tool, or any other tool, to automatically access the information they store at Facebook. *See* Facebook's Mot.n for J. on the Pleadings or In The Alternative Partial Summ. J., Dkt. 56 (hereinafter "Facebook's MJOP") at 6 ("Power's actions were indisputably without permission because they exceeded the terms of use."). On Facebook's theory, then, the users also commit a crime when they use Power's service, or any other automated means, to access their Facebook

[11] Facebook also complains that Power continued to find ways to provide access to users even after Facebook implemented simple technological means to block Power's service from accessing its servers, but this does not appear to be a separate basis for its section 502(c) claim. *See* Facebook Reply at 5-6.

[12] Facebook Statement of Rights and Responsibilities, *supra*, note 8.

accounts since that also violates Facebook's the terms of service.

Second, Facebook claims that Power violated criminal law when it continued to provide its service even after Facebook sent Power a cease and desist letter asking it to stop allowing Facebook users to access their data through Power. *See* Facebook Reply ISO Mot. For J. On The Pleadings or Partial Summ. J. and Opp. To Mot. for Summ. J., Dkt. 66 (hereinafter "Facebook Reply"), at 5-6 ("[O]n December 1, 2008 Facebook notified Power that 'Power.com's access of Facebook's website and servers was unauthorized and violated Facebook's rights.'").

II. CRIMINAL LAW IS NOT VIOLATED WHEN FACEBOOK USERS CHOOSE TO USE UNAPPROVED "AUTOMATED MEANS" TO GAIN ACCESS TO THEIR OWN INFORMATION.

When a person is authorized to access certain information, as Facebook users unquestionably are here, mere use of an unapproved technology to access that information cannot constitute a criminal act under California Penal Code section 502(c). The plain language of the Section 502 prohibits access to computers or information that the user does not have permission to access; it does not prohibit all undesirable uses of computers or information that the user is *authorized* to obtain. Moreover, section 502(c)'s federal corollary, the Computer Fraud and Abuse Act (CFAA)), has the same limitation. Here, Facebook users have the authority to access their own information stored with Facebook.

Enforcement of this Facebook's argument here -- that it can render otherwise lawful access criminal if it is accomplished contrary to its policies or its claims in a cease and desist letter -- would be especially problematic. For instance, since Facebook prohibits all "automated means," of access, a user who uses the universal web browser feature that stores login information and automatically logs users in to various websites would violate criminal law if she used that feature to access her Facebook account.

Even if the Court agrees that Facebook can contractually prevent users from using automation technology to assist them in accessing their own information, such violations amount, at most, to breaches of contract.

A. Section 502(c) Does Not Criminalize Power's Enabling A User To Gain Permissive Access to Her Own Data, Even Through Unapproved Means.

Power provides tools that allow users to access and manipulate their own data stored with Facebook. Facebook users have permission to access their data -- which they unquestionably own -- and Power does not allow users access to any additional information, like other users passwords or Facebook's proprietary data, beyond what each individual Facebook user is entitled to access. Power's service acts solely with the user's *permission*, at the user's behest and in the user's interest.

Section 502(c) penalizes one who, in relevant part:

> (1) Knowingly accesses and *without permission* alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.
>
> (2) Knowingly 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.
>
> (3) Knowingly and *without permission* uses or causes to be used computer services.
>
> (4) Knowingly accesses and *without permission* adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
>
> …
>
> (7) Knowingly and *without permission* accesses or causes to be accessed any computer, computer system, or computer network. (Emphasis added).

None of the sparse case law arising from section 502(c) supports its extension to authorized user-directed access, such as Power's conduct here. To the contrary, courts have rejected the application of section 502(c) to criminalize the behavior of persons who have permission to access a computer or computer system, but who use that access to do things that violate the rules applicable to the system. Courts have so held even when there is undisputed damage or disruption of services resulting from the access, which is not the situation here.

For instance, in *Mahru v. Superior Court*, 191 Cal. App. 3d 545, 549 (1987), the court rejected the application of section 502(c)(4) to a director of a data processing company who, in a dispute over the termination of a service contract with a customer, had instructed his employee to alter the names of certain files on a system the company operated on behalf of the customer, a

credit union. Despite finding that the director had actually disrupted the operation of the computer system, and that he had done so maliciously, the court held that section 502(c) was not applicable because the data processor had full rights to access the computer. "Section 502(c) cannot be properly construed to make it a public offense for an employee, with his employer's approval, to operate the employer's computer in the course of the employer's business in a way that inconveniences or annoys or inflicts expense on another person." *Id.*

Similarly, in *Chrisman v. City of Los Angeles*, the court rejected application of section 502(c)(7) to a police officer who had violated police procedures by accessing the police computer system for purposes unrelated to work, such as searching information about celebrities. 155 Cal. App. 4th 29, 32 (2007). The court found that the officer had engaged in professional misconduct but was not guilty of criminal unauthorized access. *Id.* at 34-35. The key difference was that the officer was authorized to *access* the police computer system, even though his particular *purpose* in doing so was clearly unauthorized. *Id.* Thus, "appellant's computer queries seeking information that the department's computer system was designed to provide to officers was misconduct if he had no legitimate purpose for that information, but it was not hacking the computer's 'logical, arithmetical, or memory function resources,' as appellant was entitled to access those resources."

The court in *Chrisman* distinguished that police officer's behavior from that of the defendant in *People v. Lawton,* 48 Cal. App. 4th Supp. 11, 15 (1996). In *Lawton*, the defendant was a member of the public who used computer terminals at the local library to display employee passwords and other information not accessible to patrons. That defendant, the *Chrisman* court said, had accessed the computer "to 'bypass security and penetrate levels of software not open to the public,' and his offense lay in such bypassing and penetration." 155 Cal. App. 4th at 35 (quoting *Lawton*, 48 Cal. App. 4th Supp. 11, 12 (1996)). By contrast, the police officer in *Chrisman* merely "used [the police computer system] to get information to which he was entitled when performing his job, but retrieved it for non-work-related reasons." *Id.* As a result, section 502(c) did not apply.

As in *Mahru* and *Chrisman*, Power's users are also Facebook users, permitted to access Facebook computers to obtain or manipulate their own data stored there. Power does not give users

-- or itself -- access to any information other than what the particular user is allowed to access as a Facebook user. Facebook may not like the *means* the users choose to employ, or users' *purpose* in aggregating their Facebook information with information stored with other social networks. Facebook may even terminate such users under its terms of use. But so long as Power and its users only access information they are already allowed to access, no computer crime is committed. This conclusion is especially true here, where there was no harm to Facebook's servers as a result of Power's provision of service. *See, e.g., Intel v. Hamidi*, 30 Cal. 4th 1342, 1348 (2003) (former employee who sent mass emails to former colleagues on employer's email system not liable for trespass to chattels because the "tort … may not, in California, be proved without evidence of an injury to the plaintiff's personal property or legal interest" and the claimed injury was disruption or distraction caused to recipients by the contents of the e-mail message, not impairment to the functioning of the computer system.).[13]

Unlike the defendant in *Facebook, Inc. v. ConnectU LLC,* 489 F. Supp. 2d 1087 (N.D. Cal. 2007), Power's service only accesses the user's own information and only makes use of that information as the user herself directs. In contrast, ConnectU accessed Facebook user accounts for the purpose of automated collection of a large number of email addresses of non-ConnectU customers, so that the company could send unsolicited commercial email to those persons and try to get them to sign up for ConnectU's service. *Id*. at 1089. In other words, ConnectU accessed email addresses and other information from Facebook users who had not given that company permission to do so, and used that information for their own commercial purposes. In rejecting ConnectU's argument that section 502(c) does not prevent access to Facebook users' email addresses because those customers made them available on Facebook, the court found that Facebook users are "entitled to disclose their email addresses for selective purposes," which presumably did not include receiving commercial solicitations from ConnectU. *Id.* at 1091 n. 5.

[13] In *eBay, Inc. v. Bidder's Edge, Inc.,* 100 F. Supp. 2d 1058, 1066 (N.D. Cal. 2000), the Court did allow a preliminary injunction on a trespass claim against auction aggregator based on concern that denial of preliminary injunctive relief would encourage an increase in the complained of activity, and such an increase would present a strong likelihood of irreparable harm. Unlike the situation here, Bidder's Edge aggregated information from eBay without user consent; yet even without that key difference *amicus* submits that *Hamidi* is the better reasoned analysis.

Here, in contrast, Power's tool serves Facebook's users, not Power. It allows Facebook users to access the user's own information and only manipulates that information as the user desires. Facebook's attempts to extend *ConnectU* to the case where users are choosing to access their own data through a third party automated service like Power's should fail.

Power's users are authorized Facebook users accessing their own data that they have full permission to access. When Power's service accesses that data at the user's behest, Power violates no law and commits no crime.

B. Similarly, Section 502(c)'s Federal Corollary, The Computer Fraud And Abuse Act, Prohibits Trespass And Theft, Not Mere Violations Of Terms Of Use.

Courts interpreting the meaning of section 502(c) have looked to the federal corollary, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (CFAA) for guidance. *See e.g. Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc*., 556 F. Supp. 2d 1122, 1131-32 (E.D. Cal. 2008) (Because section 502(c) "has similar elements to § 1030" and both parties had "incorporate[d] by reference their arguments regarding § 502 into the arguments regarding § 1030, " the court considered the two claims in tandem.); *In re Apple & AT&T Mobility Antitrust Litigation*, 596 F. Supp. 2d 1288, 1309 (N.D. Cal. 2008) (court's decision on section 502(c) relied on the exact same "reasons discussed in those prior sections" about the plaintiffs' section 1030 claims).

The most recent cases interpreting the CFAA have held that if a user is authorized to access a computer and information stored there, then doing so is not criminal, even if that access is in violation of a contractual agreement or non-negotiated terms of use. For example, in *Int'l Ass'n of Machinists and Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479 (D.Md. 2005), the plaintiff argued that the defendant, a union officer, exceeded her authorization to use the union computer when she violated the terms of use to access a membership list with the purpose to send it to a rival union, and not for legitimate union business. *Id*. at 495-96. The defendant had signed an agreement promising that she would not access union computers "contrary to the policies and procedures of the [union] Constitution." *Id*. The district court rejected the application of section 1030, holding that even if the defendant breached a contract, that breach of a promise not to use

information stored on union computers in a particular way did not mean her access to that information was unauthorized or criminal:

> Thus, to the extent that Werner-Masuda may have breached the Registration Agreement by using the information obtained for purposes contrary to the policies established by the [union] Constitution, it does not follow, as a matter of law, that she was not authorized to access the information, or that she did so in excess of her authorization in violation of the [Stored Communications Act] or the CFAA. . . . Although Plaintiff may characterize it as so, the gravamen of its complaint is not so much that Werner-Masuda improperly accessed the information contained in VLodge, but rather what she did with the information once she obtained it. . . . Nor do [the] terms [of the Stored Communications Act and the CFAA] proscribe authorized access for unauthorized or illegitimate purposes.

Id. at 499 (citations omitted).[14]

Subsequent cases have followed the reasoning of *Werner-Masuda* based on either plain language or legislative history. In *Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322 (N.D. Ga. 2007), the district court similarly rejected a CFAA claim against an employee who violated an employment agreement by using his access to his employer's computer system to steal data for a competitor. The defendant had transferred information from password-protected computer drives to his new employer while still employed with the former company, in violation of a confidentiality agreement. *Id.* at 1327-31. Correctly identifying the narrower interpretation of "exceeding authorized access" as "the more reasoned view," the court held that "a violation for accessing 'without authorization' occurs only where initial access is not permitted. And a violation for 'exceeding authorized access' occurs where initial access is permitted but the access of certain information is not permitted." *Id*. at 1343.

In *Shamrock Foods v. Gast*, 535 F. Supp. 2d 962 (D.Ariz. 2008), the district court relied on *Davidson* and *Werner-Masuda* to hold that the defendant did not access the information at issue "without authorization" or in a manner that "exceed[ed] authorized access." *Id.* at 968. The

[14] The *Werner-Masuda* court similarly interpreted the same language in the Stored Communications Act, 18 U.S.C. § 2701(a) ("SCA"). It found that the SCA "prohibit[s] only unauthorized access and not the misappropriation or disclosure of information." It continued: "there is no violation of section 2701 for a person with authorized access to the database no matter how malicious or larcenous his intended use of that access." (quoting *Educ'al Testing Service v. Stanley H. Kaplan, Educ'al Ctr., Ltd.*, 965 F. Supp. 731, 740 (D. Md. 1997) ("[I]t appears evident that the sort of trespasses to which the [SCA] applies are those in which the trespasser gains access to information to which he is not entitled to see, not those in which the trespasser uses the information in an unauthorized way"). *Werner-Masuda,* 390 F. Supp. 2d at 496.

defendant had an employee account on the computer he used at his employer, Shamrock, and was permitted to view the specific files he allegedly emailed to himself. The CFAA did not apply, even though the emailing was for the improper purpose of benefiting himself and a rival company in violation of the defendant's Confidentiality Agreement.

In *LVRC Holdings, LCC v. Brekka,* 581 F.3d 1127 (9th Cir. 2009), the defendant was a marketing contractor for a residential treatment center for addicts. While so employed, and during negotiations for *Brekka* to take an ownership interest in the facility, he emailed several of the facilities' files to himself. *Id.* at 1130. Subsequently, after the talks had terminated unsuccessfully and *Brekka* was no longer working for the facility, he used his login information to access the center's website statistics system. *Id.* The company discovered his access, disabled the account and sued *Brekka*, alleging that he violated 18 U.S.C. §§ 1030(a)(2) and (a)(4) by emailing files to himself for competitive purposes and for accessing the statistics website. *Id.* The Ninth Circuit upheld summary judgment in favor of *Brekka*. "For purposes of the CFAA, when an employer authorizes an employee to use a company computer subject to certain limitations, the employee remains authorized to use the computer even if the employee violates those limitations." In other words, "[a] person uses a computer 'without authorization' under [section 1030(a)(4) only] when the person has not received the permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." *Id*. at 1135.

The plaintiff in *Brekka* had pointed to the Seventh Circuit case of *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), arguing that an employee can lose authorization to use a company computer when the employee resolves to act contrary to the employer's interest. The Ninth Circuit explicitly rejected that interpretation because section 1030 is first and foremost a criminal statute that must have limited reach and clear parameters under the rule of lenity and to comply with the void for vagueness doctrine. *Brekka*, 581 F. 3d at 1134, citing *United States v. Carr*, 513 F.3d 1164, 1168 (9th Cir. 2008). As described further in Section IV, *infra,* Section 502(c) is also a criminal statute and must be narrowly drawn for the same reason.

Following the decision in *Brekka*, Judge Patel of this Court reconsidered her earlier ruling

applying section 1030 in *United States v. Nosal*, 2010 WL 934257 (N.D. Cal. Jan. 6, 2010). The court reversed itself, holding that no CFAA violation occurred when co-conspirators employed with an executive search placement firm accessed and downloaded firm trade secrets because those co-conspirators were at the time both employed and permitted to access the firm database "in the form of valid, non-rescinded usernames and passwords." *Id*. at *6. The court further held that neither Nosal's employment agreement, nor an express policy Nosal and his co-conspirators signed indicating that the accessed material was proprietary, nor a notice stating that the computer system and information therein were confidential, altered the result. Rather, "[a]n individual only "exceeds authorized access" if he has permission to access a portion of the computer system but uses that access to "*obtain* or *alter* information in the computer that [he or she] is not entitled so to obtain or alter." *Id*. at *7, citing 18 U.S.C. § 1030(e)(6) (emphasis in original).[15]

The cases discussed above contrast with and reject earlier decisions, most importantly the Washington District Court decision in *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc*., 119 F. Supp. 2d 1121 (W.D. Wash. 2000), which Facebook cites in support of its Motion. Facebook MJOP at 8. In *Shurgard*, the District Court denied a motion to dismiss a CFAA claim brought by an employee who took employer information from the computer system with him to his next job. *Id*. at 1129. The court relied on the Restatement (Second) of Agency, §112 (1958), to hold that when the plaintiff's former employees accepted new jobs with the defendant, the employees "lost their authorization and were 'without authorization' [under the CFAA] when they allegedly obtained and sent [the plaintiff's] proprietary information to the defendant via e-mail." *Shurgard*, 119 F. Supp. 2d at 1125. The *Shurgard* approach has troubling and potentially unconstitutional results, most notably criminalizing employee disloyalty or other transgressions against the mere preferences of a private party.

In sum, the better-reasoned and more recent cases in the Ninth Circuit and elsewhere explicitly reject *Shurgard* and the notion that a terms of service violation could create federal

[15] For additional cases rejecting criminal liability under the CFAA when the defendant had authorization to access the system or data in question, but misused that authority, see also *Lockheed Martin Corp. v. Speed*, 2006 WL 2683058 (M.D. Fla. Aug. 1, 2006); *Brett Senior & Assocs., P.C. v. Fitzgerald*, 2007 WL 2043377 (E.D. Pa. July 13, 2007).

criminal liability. To the extent that the federal cases are influential on this Court's interpretation of California Penal Code § 502(c), they weigh in favor of Power.

III. IMPOSING CRIMINAL LIABILITY BASED ON TERMS OF SERVICE OR CEASE AND DESIST LETTERS WOULD BE AN EXTRAORDINARY AND DANGEROUS EXTENSION OF CRIMINAL LAW

Many web sites or web-based services post their terms behind a "legal notices" or "terms of service" hyperlink which users can only access by scrolling to the bottom of the page and clicking on the link. Nothing about the links indicate that they are exceptionally important, much less that failure to click on it and read the underlying terms could subject the user to criminal penalties. Moreover, many terms of service, including Facebook's, contain clauses which state that the website owner can unilaterally change the terms at any time, and that continued use of the website implies acceptance of the new terms.[16]

Facebook's own terms of service provisions contain items that are likely routinely violated, thus converting possibly millions of Facebook users into federal criminals. For instance, Facebook's terms of use provide:

- You will not provide any false personal information on Facebook,
- You will not use Facebook if you are under 13.
- You will keep your contact information accurate and up-to-date.

Terms, *supra*, note 8.

On Facebook's view, if a user shaves a few years off of her age in her profile information, or asserts that he is single when he is in fact married, or seeks to hide or obfuscate her current physical location, hometown or educational history for any number of legitimate reasons, she commits a computer crime. A user who is twelve years old violates the criminal law every time she uses Facebook. And if a user changes jobs or addresses, she would need to immediately tell

[16] *See also, e.g., West Terms of Use,* http://west.thomson.com/about/terms-of-use/default.aspx?promcode=571404 (last visited July 28, 2008) ("By accessing, browsing, or using this website, you acknowledge that you have read, understood, and agree to be bound by these Terms. We may update these Terms at any time, without notice to you. Each time you access this website, you agree to be bound by the Terms then in effect."); *AOL Terms of Use,* http://about.aol.com/aolnetwork/aolcom_terms (last visited July 28, 2008) ("You are responsible for checking these terms periodically for changes. If you continue to use AOL.COM after we post changes to these Terms of Use, you are signifying your acceptance of the new terms.")

Facebook or run the risk that her continued use of the site could lead to criminal sanctions.[17]

Nor are Facebook's provisions unique. Google bars use of its services by minors – probably to protect itself against liability and to try to ensure its terms were binding in the event of a litigated dispute. Google Terms of Service, 2.3 ("You may not use the Services and may not accept the Terms if (a) you are not of legal age to form a binding contract with Google, or (b) you are a person barred from receiving the Services under the laws of the United States or other countries including the country in which you are resident or from which you use the Services."). Surely the company does not mean – or imagine – that tens of millions of minors in fact would never use its services to obtain information or would do so at the risk of criminal liability. In another example, YouTube's Community Guidelines, expressly incorporated into the site's terms of use, prohibit "bad stuff." YouTube Community Guidelines, http://www.youtube.com/t/community_guidelines (last visit July 28, 2008). Uploading "bad stuff" would violate YouTube's terms that, under Facebook's theory here, would constitute access without permission to the site. Surely YouTube did not draft the "bad stuff" prohibition with criminal liability in mind. Whatever the validity of holding such contracts enforceable for purposes of contract law,[18] the terms cannot define the line between lawful conduct and criminal violations.

For the same reasons cited above, Power's continued provision of aggregation services to Facebook users even after its receipt in Facebook's cease and desist letter does not trigger criminal liability. Facebook users who chose to use Power were still accessing their own data, that they had full rights and permission to access, even if Facebook did not like how or why they did it. No

---

[17] It is of no import that law enforcement might not bring these cases. The inability of a reader to distinguish in a meaningful and principled way between innocent and criminal computer usage is the constitutional harm. *Humanitarian Law Project v. Mukasey*, 509 F.3d 1122, 1133 (9th Cir. 2007). *See also*, Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act, Minnesota Law Review* (Forthcoming 2010) at 17, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1527187. ("Courts must adopt a meaning of unauthorized access that does not let the police arrest whoever they like. This means that courts must reject interpretations of unauthorized access that criminalize routine Internet use or that punish common use of computers.")

[18] *See* Mark A. Lemley, *Terms of Use*, 91 Minn. L. Rev. 459, 465, 475-76 (2006) (observing that in civil cases "in today's electronic environment, the requirement of assent has withered to the point where a majority of courts now reject any requirement that a party take any action at all demonstrating agreement to *or even awareness of terms* in order to be bound by those terms.") (emphasis added). This lax approach simply cannot provide "fair notice" in the criminal context.

California cases support the claim that a cease and desist letter or other direct notice to a follow-on innovator creates criminal liability when that innovator is merely facilitating otherwise authorized access to user data. Just as with terms of service violations, the computer owner's use preferences do not trigger criminal liability so long as the user has authorized access to the data in question.

Register.com, Inc. v. Verio, Inc., cited by Facebook is not to the contrary. (*See* Facebook's MJOP at pp. 7, 9). There, the court enjoined automatic searching of the registrant contact information contained in domain registry database after lawyers specifically objected to the defendant's use and sent out a terms of use letter to the defendant. *Register.com, Inc. v. Verio*, *Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000), *aff'd in part as modified by Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393 (2d Cir. 2004) (reversing the trial court's CFAA finding on the basis that there was insufficient likelihood of showing the $5,000 damage threshold necessary for private claims, but upholding a trespass to chattels claim). The defendant did not have the registrants' permission to access their contact information. Here, Power has the permission of the Facebook user to access her own data.[19]

For these reasons, this Court should view with caution Judge Fogel's decision denying Power's Motion to Dismiss Facebook's copyright circumvention claim, in which the court determined that, for purposes of a claim of copyright circumvention, the Facebook terms of service deny users the right to authorize circumvention of Facebook's technological protection measures. *Amicus* questions whether this analysis is correct for purposes of a civil copyright circumvention claim. In any event, at this stage of the litigation, it is clear that even if the terms of service are theoretically relevant to a civil copyright circumvention claim, they cannot serve here as a basis for criminal liability for Facebook users, or their agents, who seek to access to information that the users own.

If Facebook's proposed construction of section 502(c) in this case is correct, millions of

[19] Facebook's assertion that allowing user permission to serve as the basis for authorized access to a user's own data would be akin to allowing a third party to break into a bank in order to retrieve a user's deposits is both unfounded and hyperbolic. *See* Facebook Reply at 6. More correctly, Facebook's argument would allow a bank to make it a crime for a bank customer to use certain technology to assist her in making an otherwise legitimate deposit or withdrawal from her own account during regular business hours.

otherwise innocent internet users would potentially be committing frequent criminal violations of the law through ordinary, indeed routine, online behavior. Similarly, allowing a private party to define criminal conduct merely by sending a letter complaining about a competitor's computer usage puts far too much power in the hands of private entities that in doing so may or may not have consumer rights and the public interest at heart.

IV. THE RULE OF LENITY REQUIRES THIS COURT TO INTERPRET CRIMINAL LAWS, INCLUDING SECTION 502(C), NARROWLY

While this is a civil dispute, the Court's ruling here will influence the interpretation of section 502(c), which is first and foremost a criminal statute. See *Leocal v. Ashcroft*, 543 U.S. 1, 11 n. 8 (2004) (holding that where a statute has both criminal and noncriminal applications, courts should interpret the statute consistently in both criminal and noncriminal contexts). Therefore, this Court must apply the rule of lenity and interpret this statute narrowly, so as to exclude terms of service violations and disregard of cease and desist letters.

Grounding criminal liability under section 502(c), as Facebook seeks to do here, on whether a person has fully complied with Facebook's terms of service or has disregarded a cease and desist letter creates constitutional problems and renders the statute void for vagueness. Pinning criminal liability on the vagaries of privately created, frequently unread, generally lengthy and impenetrable terms of service would strip the statute of adequate notice to citizens of what conduct is criminally prohibited and render it hopelessly vague. *See United States v. Drew*, 259 F.R.D. 449, 465 (C.D. Cal. 2009), ("utilizing violations of the terms of service as the basis for the section 1030(a)(2)(C) crime improperly makes the website owner the party who ultimately defines the criminal conduct"). And pinning criminal liability on whatever counsel chooses to put into an individual cease and desist letter is even worse; such letters are even more likely to be arbitrary and discriminatory than general terms of use.

The Supreme Court has stated:

> "[i]t 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). A criminal statute is therefore 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)."

United States v. Batchelder, 442 U.S. 114, 123 (1979); see also *Grayned v. Rockford*, 408 U.S. 104, 108-09 (1972) ("Vague laws may trap the innocent by not providing fair warning. Second, if arbitrary and discriminatory enforcement is to be prevented, laws must provide explicit standards for those who apply them. A vague law impermissibly delegates basic policy matters to policemen, judges, and juries for resolution on an ad hoc and subjective basis, with the attendant dangers of arbitrary and discriminatory application. Third, but related, where a vague statute 'abut(s) upon sensitive areas of basic First Amendment freedoms,' it 'operates to inhibit the exercise of (those) freedoms.' (citations omitted)."). A plurality of the Supreme Court has further specified that "[v]agueness may invalidate a criminal law for either of two independent reasons. First, it may fail to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits; second, it may authorize and even encourage arbitrary and discriminatory enforcement." *Chicago v. Morales*, 527 U.S. 41, 56 (1999) (Stevens, J., plurality opinion).

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) (quoting *Nunez v. City of San Diego*, 114 F.3d 935, 940 (9th Cir. 1997)). "Vague statutes are invalidated for three reasons: '(1) to avoid punishing people for behavior that they could not have known was illegal; (2) to avoid subjective enforcement of laws based on 'arbitrary and discriminatory enforcement' by government officers; and (3) to avoid any chilling effect on the exercise of First Amendment freedoms.'" *Humanitarian Law Project v. Mukasey*, 509 F.3d 1122, 1133 (9th Cir. 2007) (quoting *Foti v. City of Menlo Park*, 146 F.3d 629, 638 (9th Cir. 1998)).

Given that courts must adopt a narrow construction of a criminal statute to avoid vagueness and other unconstitutional infirmities, Facebook's proposed view of section 502(c) must be rejected. *See Zadvydas v. Davis*, 533 U.S. 678, 689 (2001); *Coates v. City of Cincinnati*, 402 U.S. 611, 614 (1971) (law disallowing three people to congregate if it is annoying to others was unconstitutionally vague).

For this reason, Professor Orin Kerr has argued thoughtfully and persuasively that

"unauthorized access" should not include access to a computer in violation of a contract or terms of service. Professor Kerr observes that doing so would:

> threaten a dramatic and potentially unconstitutional expansion of criminal liability in cyberspace. Because Internet users routinely ignore the legalese that they encounter in contracts governing the use of websites, Internet Service Providers (ISPs), and other computers, broad judicial interpretations of unauthorized access statutes could potentially make millions of Americans criminally liable for the way they send e-mails and surf the Web.

Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1599 (2003). Consider the remarkable and disturbing results that a contract-based approach to criminalizing computer access can create:

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

Id. at 1650-51. This outcome is unacceptable regardless of whether the site owner's objection is lodged in a terms of service or sent in a cease and desist letter.

Section 502(c), like the CFAA, offers no guidance on the meaning of access or use "with permission." As Kerr argues with regard to the CFAA, "The core difficulty is that access and authorization have a wide range of possible meanings. … Is it unauthorized if the computer owner tells the person not to access the computer? Is it unauthorized if the access is against the interests of the computer owner? Is it unauthorized if the access violates a contract on access? Presently the answer is remarkably unclear." Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act, Minnesota Law Review* (Forthcoming 2010) at 17, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1527187.

Yet, Facebook's interpretation of section 502(c) means the statute will rely for its essential meaning on the existence and clarity of separate contractual terms or demand letters drafted for a variety of reasons that have nothing to do with preventing the sort of unauthorized hacking, misuse, trespass or theft of private data with which the computer crime law is properly concerned.

To make sense and to avoid fatal vagueness problems, section 502(c) must be limited to

clear, proper purposes consistent with the statute's goals, and not whatever commercial or personal purpose motivates a site owner to draft a provision in a terms of service document, or a cease and desist letter.

V. IMPOSING CRIMINAL LIABILITY IN THIS CASE WOULD CREATE A RULE THAT HOBBLES USER-CHOICE, COMPETITION, AND INNOVATION

Enforcing private web site operators' preferences with criminal law puts immense coercive power behind terms and conditions that may be contrary to the interests of consumers or the public.[20] Many web site terms of service contain conditions that are vague, arbitrary or even fanciful. They are not written by their private drafters with the precision and care that would be expected – indeed required – of operative provisions in a criminal statute. Nor are they necessarily written with the public interest in mind. To the contrary, they may seek to undermine the public interest in competition by creating barriers to entry for competitors or barriers to exit for their users. In ruling on this motion, this Court should be especially careful not to suggest criminal liability applies when a user or user-directed service violates a term or condition that seeks to, or effectively does, prohibit competing or follow-on innovation, as appears to be the case here.

Generally, companies garner and keep customer loyalty by providing a quality product. If the product is substandard or something better comes along, customers can vote with their feet and shop somewhere else. The ability to choose what services to use and how to use them is good for customers and healthy for businesses. Here, the specific terms Facebook relies on, as applied to users who choose to use Power's enhanced services, prevents users from adopting follow-on innovation by third parties. Thus, enforcement of those terms runs the very serious risk of excluding competition and limiting users to only the innovation that Facebook chooses to allow. More worrisome, since one of the services Power provides its users is the ability to export their social network data into a format that can be easily read by other social networks, Facebook's argument would allow it to facilitate user lock-in. By stopping users from engaging the assistance

[20] *Amicus* here takes no position on Power's antitrust or anticompetitive counterclaims. Nonetheless, in determining whether to accept Facebook's interpretation of section 502(c), we believe it is important for the court to consider how Facebook's broad interpretation would hurt consumers and the market by limiting follow-on innovation and creating a barrier to users who wish to move their data out of Facebook.

of third parties and automated systems like Power's to access and remove their data, Facebook increases the cost to consumers of switching social networking services.

Facebook's urged interpretation of section 502(c), therefore, would harm the market forces that would otherwise allow users to freely leave the service if, for example, they dislike changes in Facebook's terms of use or privacy policies. These concerns are not merely hypothetical. Facebook has recently sparked a storm of protest and concern due to changes to its terms of use and practices that make the personal data that its users store with Facebook increasingly accessible to third parties, including advertisers.[21] Additionally, Facebook has changed its policies with regard to certain user content. For example, in mid 2009, Facebook blocked some images from breastfeeding groups.[22] Whatever the propriety of such changes under contract law, the imposition of criminal liability for users attempting to easily move their data out of Facebook poses unacceptable risks to consumers and innovators. Consumer choices would then be limited due not to natural competition, but to a social network's privately imposed – but publicly enforced -- barriers. Furthermore, the penalty for non-compliance would be unacceptably steep.

VI. CONCLUSION

Based upon the foregoing, *amicus* respectfully requests that this Court grant summary judgment in favor of Power on Facebook's section 502(c) claims.

DATED: May 3, 2010

By */s/Jennifer Stisa Granick*
Jennifer Stisa Granick (California Bar No. 168423)

ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x134
Facsimile: (415) 436-9993

[21] Miguel Helft, *Senators Ask Facebook for Privacy Fixes*, New York Times Bits Blog (April 27, 2010), *available at* http://bits.blogs.nytimes.com/2010/04/27/senators-ask-facebook-for-privacy-fixes/; MoveOn's Facebook Privacy Petition, *available at* http://civ.moveon.org/facebookprivacy/.

[22] MSNBC, *Facebook nudity policy angers nursing moms -- Rules say no nipples, but mothers contend breast-feeding is not obscene* (Jan. 1, 2009), *available at* http://www.msnbc.msn.com/id/28463826/.