CINDY A. COHN (California Bar No. 145997)
cindy@eff.org
JENNIFER STISA GRANICK (California Bar No. 168423)
jennifer@eff.org
MARCIA HOFMANN (California Bar No. 250087)
marcia@eff.org
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x134
Fax: (415) 436-9993 (fax)

Attorneys 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. Facebook further grounds its claim that Power violated criminal law on Power's decision to continue to provide its service to users even after Facebook implemented a simple measure, Internet Protocol address blocking, to stop Power's tool from working for Facebook users.

Amicus believes that merely providing a tool to assist an authorized 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 urges 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 websites in the contracts of adhesion they present to users or in their cease and desist letters, thus giving these private parties immense power to decide when criminal liability attaches. This creates both legal uncertainty and the risk of capricious enforcement.

These problems are not mitigated simply by looking to whether the server owner adopted, and the user evaded, some technological barrier. The IP blocking used by Facebook here was a crude attempt to enforce its choice of means by which authorized users could access the website; it was not aimed at distinguishing between authorized and unauthorized users. Power's efforts to ensure that Facebook's authorized users could continue to access their own data on Facebook's

servers despite Facebook's attempts to control the means of access should not trigger criminal liability. Imposing such sanctions here 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.

Perhaps the most important fact in this case is that Power's servers only connect with Facebook servers *at the behest of a Facebook user*, who must provide her own valid username and password to obtain access to Facebook and her own social networking data. Power did not connect to Facebook except as an agent of an authorized user. It is true that the user is choosing automation, despite Facebook's terms of 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 become criminal conduct, for either the user or for the provider of the automation tool. This is especially the case when Facebook has breach of contract remedies available to it, including termination of a misbehaving user's credentials. Were Facebook's proposed construction of section 502(c) in this case correct, millions of otherwise innocent Internet users are violating criminal law through routine online behavior. Furthermore, 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]

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

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 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 altogether. After a huge outcry, the company backpedaled, and reinstituted the old terms that allowed users to delete their content from the site.[9]

---

[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-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),

As part of its business model, Facebook has also steadily increased the amount of information about its users and their activities it offers to third parties. Facebook has an Application Programming Interface, or API, through which third parties can see the information and activities of Facebook's users. Through controversial changes to its terms of service and the functionality of its API, Facebook now offers to certain third parties and advertisers as much information about any particular user and his or her friends as that user personally could have accessed 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 with third parties, but at ensuring Facebook's 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 friend 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 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 her own information posted to such services. For instance, Power's service allows a user to see all of her friends and contacts in a single list, regardless of which social networks they use. Power also offers the user a tool by which she can easily export her information from social networks into a spreadsheet format, thus aiding users who might want to move their information from one social network to another. Power stopped providing its service to Facebook users at some point during this legal dispute.

D. Facebook's IP Blocking Effort

In December 2008, Facebook and Power conferred about Power's implementation of user

---

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.

access to Facebook accounts. Apparently Facebook wanted Power to use Facebook's API rather than connect a user directly to her account information so that Facebook would have more control over how stored data was accessed and manipulated, but Power felt that the API did not allow the full functionality Power wanted to bring to its customers.[11] During these negotiations, Facebook blocked the Internet Protocol (IP) address of Power's server, "so that users attempting to access their Facebook accounts through Power's browser would be denied access." Declaration of Steve Vachani ISO Power's Opp. to Mot. for J. On The Pleadings or Partial Summ. J. at ¶ 9, Dkt. 65; *see also* Exhibit A to Declaration of Julio C. Avalos ISO Facebook's Mot. for J. on the Pleadings or In The Alternative Partial Summ. J., Dkt. 57. As described in detail below, IP blocking is simply a method of preventing a computer with one IP address from connecting to another. This technique has no bearing on computers associated with any other IP address or individual users who connect to the Internet using different machines or access points. If the person originally using the blocked IP address changes to a different IP address for any reason, the block will not affect her any longer. Facebook does not claim that Power disabled its IP blocking, or did any damage to Facebook's servers, but merely that the company changed IP addresses so that its servers would not be blocked and Power users could continue to choose to access their Facebook accounts through the Power interface. Compl. ¶ 58-59.

E. Facebook's Section 502(c) Claims

Facebook's argument that Power has violated California Penal Code section 502(c) is based on three elements: (1) that the network's terms of service prohibit automated access to a user's information, (2) that the network sent Power a cease and desist letter demanding that it stop providing its service to users, and (3) that Power continued to find ways to provide access to users even after Facebook implemented IP blocking to keep Power from accessing its servers.[12]

---

[11] *Amicus* expresses no preference between the two sides of this debate. Facebook may have valid reasons for wanting application developers to go through its API, and Power and its users may have valid reasons for wanting the ability to exercise more control over users' data. Two businesses can have valid but competing views about which tools will be valuable to their user bases, which is another reason why applying criminal liability is wholly inappropriate in these kinds of disputes.

[12] While avoiding IP blocking does not appear from the papers to be a separate basis for

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.[13]

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.

Power's liability theoretically derives from giving a Facebook user the choice of using an automated tool contrary to the terms of service. 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 with Facebook. *See* Facebook's Mot. 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."). Importantly, while individuals were not sued here, under Facebook's theory the *users* also commit a crime when they use Power's service, or any other automated means, to access their Facebook accounts since that also violates Facebook's the terms of service.

Second, Facebook claims that Power independently violated criminal law when it continued to provide its service even after Facebook implemented IP blocking and 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

---

Facebook's section 502(c) claim, *see* Facebook Reply at 5-6, at the June 7, 2010 hearing on these motions, it became clear that this evasion was at least one factor the company offered in support of the claim.

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

violated Facebook's rights.'").

II. FACEBOOK USERS WHO CHOOSE TO USE "AUTOMATED MEANS" TO GAIN ACCESS TO THEIR OWN INFORMATION IN CONTRAVENTION OF THE FACEBOOK TERMS OF SERVICE DO NOT VIOLATE CRIMINAL LAW.

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 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. In other words, Section 502 punishes unauthorized *access* or *use* of information, but generally not authorized access through unapproved *means*.[14] Moreover, section 502(c)'s federal corollary, the Computer Fraud and Abuse Act (CFAA), has the same limitation. Facebook users have the authority to *access* and *use* their own information stored with Facebook, so under either statute they commit no crime when they do exactly that through automated or other disfavored means.

Adoption of Facebook's argument here -- that otherwise lawful access is criminal if it is accomplished contrary to any of Facebook's policies or claims in a cease and desist letter -- would create absurd results. For example, as described in more detail in Section III, *infra*, since Facebook requires users to keep their contact information current and to use accurate information, someone who lies about her age or fails to update her current city after a move would violate criminal law. Even closer to the facts here, Facebook's prohibition on all "automated means" of access could make it criminal for a user to take advantage of the universal web browser feature that stores login information and automatically logs users in to various websites, if she uses 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 should amount, at most, to breaches of contract.

[14] Of course, providing a means of access that disrupts access to Facebook's servers would violate sections 502(c)(5) and (6).

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

Power provides a tool that allows users to access and manipulate their own data stored with Facebook. Facebook users have permission to access their data -- which they undisputedly 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 and the data stored there, 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 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." *Id.*

The court in *Chrisman* distinguished the 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*, the access challenged here is by *authorized* users, who are permitted to access Facebook computers to obtain or manipulate their own data stored there, albeit by directing their queries through the Power browser. Power does not give any user -- or itself -- access to information other than what she is already 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' accounts under its terms of use. But so long as Power and its users only access information they are already allowed to access and do not misuse that data, 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.).[15]

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

[15] 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 an auction aggregator based on concern that denial of preliminary injunctive relief would encourage an increase in the disputed 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 and the court's analysis turned on the likely future actual harm to eBay's servers, which is not demonstrated here; yet even without those key differences *amicus* submits that *Hamidi* is the better reasoned analysis.

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. Here, in contrast, Power's tool is controlled by and serves Facebook's users, not Power. It allows a Facebook user to access her own information and only manipulates that information as the user desires. Facebook's attempts to extend *ConnectU* to this 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, which 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. 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 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, 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 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).[16]

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 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. Identifying the narrower interpretation of "exceeding authorized access" as "the more reasoned view," the court held that "a violation for accessing 'without authorization'

[16] 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.

occurs only where initial access is not permitted. Further, 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 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 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." *Id.* at 1133. 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).[17]

The cases discussed above contrast with and reject earlier decisions, most importantly *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

[17] 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).

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 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 websites or web-based services post their terms behind a "legal notices" or "terms of service" hyperlink that 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 them 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.[18]

Facebook's own terms of service 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.

[18] *See also, e.g., West Terms of Use,* http://west.thomson.com/about/terms-of-use/default.aspx?promcode=571404 (last visited June 21, 2010) ("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 June 21, 2010) ("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.")

- You will not use Facebook if you are under 13.
- You will keep your contact information accurate and up-to-date.
- You will not share your password . . . [or] let anyone else access your account[.]

Terms, *supra*, note 8.

In Facebook's view, if a user shaves a few years off of her age in her profile information, or asserts that she is single when she 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 criminal law every time she uses Facebook. And if a user changes jobs or moves to another city, she must immediately inform Facebook or run the risk that her continued use of the site could lead to criminal sanctions.[19] Moreover, a politician or other high-profile user who communicates through Facebook with the general public violates the terms of service if he delegates his password to employees or volunteers to maintain the page. *See, e.g., Barack Obama's Facebook Page,* http://www.facebook.com/barackobama (last visited June 20, 2010) (prominently noting that the page is "run by Organizing for America, the grassroots organization for President Obama's agenda for change.").

These problems are not specific to Facebook because Facebook's terms of service provisions are not unique. Google bars use of its services by minors – probably to protect itself against liability and to try to ensure its terms are 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

[19] It is of no import that law enforcement might not choose to 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. *Foti v. City of Menlo Park*, 146 F.3d 629, 638 (9th Cir. 1998). *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.").

mean -- or imagine -- that tens of millions of minors in fact will never use its search engine or other services, or do so only at the risk of criminal liability. In another example, YouTube's Community Guidelines, expressly incorporated into the site's terms of use, prohibit posting videos that show "bad stuff." YouTube Community Guidelines, http://www.youtube.com/t/community_guidelines (last visited June 18, 2010). Uploading "bad stuff" would not only violate YouTube's terms of service, but under Facebook's theory here, also 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,[20] 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 receipt of Facebook's cease and desist letter does not trigger criminal liability. Facebook users who chose to use Power were still accessing their own data, which they had full rights and permission to access, even if Facebook did not like how or why they did it. No California case supports 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.

The relatively early case of *Register.com, Inc. v. Verio, Inc.*, cited by Facebook, is not to the contrary. *See* Facebook's MJOP at 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

[20] *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.

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 particular Facebook users to access their own data.[21]

If Facebook's proposed construction of section 502(c) in this case were correct, millions of 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 may or may not have consumer rights and the public interest at heart.[22]

IV. EVASION OF A TECHNOLOGICAL MEASURE PUT IN PLACE TO ENCOURAGE COMPLIANCE WITH TERMS OF SERVICE OR CEASE AND DESIST LETTERS, WITHOUT MORE, DOES NOT INCUR CRIMINAL LIABILITY

At oral argument, Facebook added an additional basis for its claim that Power violated section 502: Power's alleged evasion of Facebook's IP address blocking effort. Yet if the failure to abide by contractual limits on means of access is insufficient to create criminal liability, ignoring or bypassing technological limits that attempt to create those same limits must also be insufficient to create criminal liability. To understand why, it is necessary to explain IP address blocking and how users or entities avoid it to demonstrate (1) that there are many legitimate reasons for changing your IP address to avoid blocking, so the practice should not be categorically discouraged, and (2)

---

[21] 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.

[22] 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.

IP blocking does not necessarily provide computer security or data privacy, and did not in this case, so this evasion of IP blocking is outside the scope of the computer crime law.

A. IP Address Allocation

An "IP address" is a numeric value used to identify a computer or set of computers on the Internet. Internet routers use the IP address to decide where to send communications addressed to a particular computer.[23] The address is normally written as four numbers separated by periods.[24] For example, one of the web servers operated by *amicus* uses the address 64.147.188.11, while this Court's web server uses 207.41.19.17.[25]

IP addresses are allocated to Internet service providers (ISPs) in chunks of consecutive addresses out of a worldwide pool of around four billion possible addresses through geographically-based non-profit organizations known as regional Internet registries.[26] ISPs can further delegate these addresses to smaller entities such as a business, an Internet café, or a smaller ISP.[27] ISPs can also assign an IP address directly to an individual computer. This assignment process is frequently automated and the assignment can be short- or relatively long-term.[28]

Because IP addresses are allocated in this way, they can convey approximate and general information about a computer's location, how the computer is connected to the Internet or what individual or entity is using that computer to connect.[29] But it is equally true that the IP address used by a particular computer can change over time, that individual users connect through different

---

[23] *See* Declaration of Seth Schoen ("Schoen Dec'l") at 2, citing Eric A. Hall, *Internet Core Protocols: The Definitive Guide*, 37-40 (O'Reilly and Associates, 2000).

[24] *See* Schoen Dec'l at 2, citing Radia Perlman, *Interconnections Second Edition*, 199 (Addison Wesley Longman, 2000).

[25] *See* Schoen Dec'l at 2.

[26] *See* Schoen Dec'l at 3, citing American Registry for Internet Numbers, "Internet Number Resource Distribution," available at https://www.arin.net/knowledge/distribution.pdf.

[27] *See* Schoen Dec'l at 3, citing Hall, *supra*, at 40-41.

[28] *See* Schoen Dec'l at 3, citing Wikipedia, "IP Address: Static vs dynamic IP addresses," version of June 17, 2010, available at http://en.wikipedia.org/w/index.php?title=IP_address&oldid=368588938#Static_vs_dynamic_IP_addresses.

[29] *See* Schoen Dec'l at 4, citing Kevin F. King, "Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies," *available at* http://ssrn.com/abstract=1622411 (cited here for its clear description of the relationship between IP address and geolocation, but not for its legal conclusions).

IP addresses depending on where they are, and that multiple users can connect to the Internet through a single IP address.[30]

For instance, a laptop will receive a different IP address when it connects to the Internet from different locations.[31] If a laptop's owner uses the machine from her workplace in the morning, a café in the afternoon, and her home in the evening, she will present three different IP addresses over the course of a single day. A traveler who brings a laptop to a different city and goes on-line there will receive an IP address unrelated to the IP address he used at home. So will an Internet user who chooses to change residential broadband providers -- for example, by switching from Comcast to AT&T. Even a home Internet user may encounter an IP address that changes over time, since some ISPs vary the address that they assign to a particular computer on different occasions.[32] America Online, for instance, provides a different, randomly-selected IP address to every user with each new telephone modem dial-up session.[33]

Some common Internet technologies such as tunnels, virtual private networks ("VPN"s), and proxy servers will also change the apparent IP address that a user appears to be connecting from. Users have many legitimate reasons to use technologies that will change their apparent IP addresses. [34]

---

[30] *See* Schoen Dec'l at 4, citing Yinglian Xie *et al.*, "How Dynamic Are IP Addresses?," in *Proceedings of the 2007 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, available at http://www.sigcomm.org/ccr/drupal/files/fp179-xie.pdf, and Jeff Tyson, "How Network Address Translation Works," available at http://computer.howstuffworks.com/nat.htm/printable.

[31] *See* Schoen Dec'l at 5, citing University of Illinois Campus Information Technologies and Educational Services, "Network Access While Traveling", available at http://www.cites.illinois.edu/network/access/travel.html.

[32] *See* Schoen Dec'l at 5, citing Whatismyipaddress.com, "Dynamic IP Addressing," available at http://whatismyipaddress.com/dynamic-static, and Xie *et al.*, note 7, supra.

[33] *See* Schoen Dec'l at 5, citing Wikimedia Foundation, "Why are AOL users often blocked?," *available at* https://en.wikipedia.org/wiki/Wikipedia:AOL#Why_are_AOL_users_often_blocked.3F, and AOL, "AOL Outbound Mail Server Hostnames and IPv4 Addresses," *available at* http://postmaster.aol.com/Postmaster.OMRs.html.

[34] *See generally* Testimony of Seth Schoen before the United States Sentencing Commission (March 17, 2009), http://www.ussc.gov/AGENDAS/20090317/Schoen_testimony.pdf (describing use of proxy servers and virtual private networks for computer security and privacy reasons, and as a means of proving entitlement to access subscription-based resources).

B. IP Address Blocking

Most network routers, firewalls, and Internet server software provide simple, straightforward "IP blocking" features.[35] That is, a computer or network can be configured to discard or ignore all communications from a particular IP address. A server operator could use this as a way to reduce unwanted Internet traffic based on the server operator's belief that particular IP addresses are associated with a greater likelihood of undesired activity, such as spam email.[36] The operator could choose to use this ability to refuse communications with a particular computer, with a particular ISP, or with an entire geographic area, such as a country.[37] If a computer has been configured to "block" an IP address or addresses, it will either return an error in response to communications from those addresses (for instance, stating that a website is unavailable), or simply ignore those communications entirely, making no reply to them.[38]

Because it is so easy for a user to change her IP address, system administrators know that this kind of blocking is a rather rough and easily ignored tool for limiting Internet connections.[39] Requiring a username and password, for example, as Facebook does, is a far more robust and direct way of distinguishing between authorized and unauthorized users.

C. Avoiding Blocking

Internet users who find their computers blocked from accessing a particular service might have many reasons to try to circumvent the restriction -- which could often mean doing something as simple as trying again from a different place. For instance, an employer might have a policy that a certain service may be accessed only from certain recognized locations. This policy could be

---

[35] *See* Schoen Dec'l at 7, citing Wikipedia, "Blacklist (computing)," version of June 13, 2010, available at http://en.wikipedia.org/w/index.php?title=Blacklist_(computing).

[36] *See* Schoen Dec'l at 7, citing dnsbl.info, "What is a DNSBL?," *available at* http://www.dnsbl.info/ (describing publicly-available blacklist databases of IP addresses alleged to have been the origin of large numbers of unwanted spam messages).

[37] *See* Schoen Dec'l at 7, citing Wikipedia, "IP blocking," version of June 10, 2010, *available at* http://en.wikipedia.org/w/index.php?title=IP_blocking&oldid=367115237.

[38] *See* Schoen Dec'l at 7, citing "Yahoo Help, IP Address Blocking," *available at* http://help.yahoo.com/l/us/yahoo/smallbusiness/store/risk/risk-17.html .

[39] *See* Schoen Dec'l at 8, citing Simson Garfinkel and Gene Spafford, *Practical Unix and Internet Security*, 484 (O'Reilly and Associates, 1996) ("Restricting a service by IP address or hostname is a fundamentally unsecure way to control access to a server.").

implemented by blocking all unknown IP addresses; an employee traveling to a new location could use a proxy or VPN service to change the apparent IP address from which the service was accessed. Or an American bank's anti-fraud measures could categorically forbid access to on-line banking services from certain foreign countries with no known customers and a high incidence of fraud; this blocking could be implemented by blocking all IP addresses associated with those countries.[40] A legitimate customer of the bank, frustrated at the inability to log on to the bank's web site during a trip, could use a proxy or VPN service to bypass the restriction by appearing to connect from a U.S.-based IP address.[41]

More trivially, an email service might refuse to accept any messages from IP addresses associated with a particular hotel, because guests staying in that hotel had previously sent large amounts of commercial email. An innocent guest could be prevented from sending legitimate email to the service as a result, but could readily avoid this restriction by using a proxy or a VPN.[42]

D. Application to This Case

The examples above illustrate that there is nothing inherently improper, never mind unlawful, about switching IP addresses and thereby avoiding IP address blocking. Any Internet user may have valid reasons for so doing, and the means of switching (going to a different location, using a VPN or proxy server, asking the ISP to allocate a different address) are common, unremarkable and in no way interfere with the proper functioning of the blocking server.

The question, then, is whether evading IP blocking to allow authorized users access to their own data through "automatic means," without causing any harm, violates section 502. The answer must be no. Section 502(c) does not and should not punish authorized *access* accomplished through disfavored but harmless *means*. Nor does it punish authorized access where the user subsequently acts contrary to the policies or preferences of the server owner. The IP blocking here did nothing more than roughly attempt to control the manner in which legitimate users accessed their data.

---

[40] *See* Schoen Dec'l at 9 citing Wikipedia, "IP blocking," version of June 19, 2010, *available at* http://en.wikipedia.org/w/index.php?title=IP_blocking&oldid=368931563 (suggesting that some services may forbid all access to Nigerian IP addresses because of high rates of fraud associated with Nigeria).

[41] *See generally* Schoen Dec'l at 9.

[42] *See generally* Schoen Dec'l at 10.

Sidestepping that blocking is not criminal for the same reasons that utilizing automation in violation of terms of service is not criminal: users have permission to access their data, and they have authorized Power to access it on their behalf.

This is not to say that section 502 could never prohibit evasion of IP address blocking. If a provider implemented blocking to prevent access by unauthorized persons, and an unauthorized person evaded that block as part of gaining access, that person may well have violated section 502(c)(3) or (7). Similarly, if a third party like Power evaded IP blocking to help that unauthorized individual, section 502(c)(6) could apply.

The benefit of *amicus'* approach is that it neither approves nor disapproves particular technologies, but looks to the purpose and language of section 502 and the effect of a technological barrier to determine whether evading that barrier is trespass or a privacy invasion. If a particular technological restriction seeks to control access to or use of data, then evasion of it is almost certainly criminal. But if the restriction merely seeks to impose owner preferences or terms of service on otherwise authorized users, as the IP blocking here did, than it is not. Holding otherwise would essentially give website owners the power to criminalize any term of service that could be implemented in code, regardless of whether the user was authorized or the term imposed a type of restriction or condition that criminal law should not be used to enforce.

V. 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 narrowly interpret this statute.

Grounding criminal liability under section 502(c) on whether a person has fully complied with Facebook's terms of service, disregarded a cease and desist letter, or avoided a technological measure meant to force those terms or litigation demands on users creates constitutional problems and renders the statute void for vagueness and overbreadth. Criminal punishment cannot be based

on the vagaries of privately created, frequently unread, generally lengthy and impenetrable terms of service, which fail to give adequate notice to citizens of what conduct is criminally prohibited. Interpreting section 502 otherwise would make 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"). 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) As the *Batchelder* Court stated:

> 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.'" *Foti v. City of Menlo Park*, 146 F.3d 629, 638 (9th Cir. 1998).

Similarly, "the overbreadth doctrine permits the facial invalidation of laws that inhibit the exercise of First Amendment rights if the impermissible applications of the law are substantial when judged in relation to the statute's plainly legitimate sweep." *See City of Chicago v. Morales*, 527 U.S. 41, 52, 56 (1999) (quotations omitted). Basing criminal liability on mere notice from the server owner runs afoul of this doctrine by granting computer owners the power to criminalize speech, as well as competition.

For these reasons, George Washington Law 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.

Under Facebook's interpretation of Section 502(c), the statute must 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. Given that courts must adopt a narrow construction of a criminal statute to avoid vagueness, overbreadth 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).

Section 502 liability is not sufficiently narrowed by looking to whether a user or a tool-provider changed her IP address to avoid blocking. Here, the IP blocking did no more than attempt to enforce through technological means the otherwise non-criminal provision of automation technology to the public. A lawful act is not necessarily made unlawful because one uses a different IP address to accomplish it. Here, the avoidance of IP blocking did not enable anyone to access data that she is not authorized to access.

In *Cybercrime's Scope*, Kerr critiques a contract-based approach to criminal liability and advocates that courts only impose such sanctions for the circumvention of certain code-based restrictions. The example Kerr gives throughout the article is requiring a username and password limiting the user's privileges on the machine. Certainly evading a username and password to gain access to a server or other people's data would violate the law. But requiring a password is a very different kind of technological security measure than IP blocking. Requiring a password actually

defines the user's authority to access the machine and/or data stored thereon. It is a *barrier* to access, not a *means* of access. Blocking Power's IP address does not restrict anyone's rights or ability to access their Facebook data. It was merely a crude attempt to remove a legitimate user's option of utilizing the Power tool. In other words, the IP blocking here was more like a speed bump than a wall. *Amicus* agrees with Kerr that courts should reject mere contract- or notice-based theories of criminal liability in favor of code-based restrictions. But not all code-based restrictions fit section 502's definitions of access without permission. Thus, evasion of a code-based restriction is only unlawful if it fits the statutory language and purpose of section 502 by restricting access and use, and not merely by imposing some limitation on the means used to effectuate lawful access.

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 cease and desist letter, or to attempt to block a particular computer from connecting to its server when the user is otherwise permitted to access her data stored there.

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

Enforcing private website operators' preferences with criminal law puts immense coercive power behind terms and conditions and technological measures that may be contrary to the interests of consumers and the public.[43] Many terms of service contain conditions that are vague, arbitrary or even fanciful. Terms of use are not written by their drafters with the precision and care that would be expected -- indeed required -- of operative provisions in a criminal statute. Nor are such terms necessarily written with the public interest in mind.

Technological measures like IP blocking are even more imprecise since they give the user no understanding of why they have been implemented. For example, technological means are

[43] *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.

commonly used to help repressive government regimes keep their citizens from accessing "undesirable" content. The Chinese government uses such means -- including IP blocking -- to keep people within China from accessing certain content on the Internet, and also legally requires private companies doing business in China to implement censorship measures.[44] Google for several years refrained from offering certain services and filtered search results on http://www/google.cn at the insistence of the Chinese government.[45] Other companies, including Microsoft and Yahoo, continue to comply with the Chinese government's requirements.[46] If service providers censor content or block certain users under pressure from other governments, then anyone within such a country – including visitors from the U.S. -- who obscures her location to obtain uncensored content or access "unapproved" websites would risk criminal penalties under U.S. law.

Technological speed-bumps may also 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 attaches 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. For example, if Facebook were to reach an agreement with

---

[44] *See* Amnesty International, *Undermining Freedom of Expression in China: The Role of Yahoo!, Microsoft and Google* (July 2006), http://www.amnestyusa.org/business/Undermining_Freedom_of_Expression_in_China.pdf.

[45] Andrew McLaughlin, *Google in China* (Jan. 27, 2006), http://googleblog.blogspot.com/2006/01/google-in-china.html. Google only recently decided not to comply with China's censorship demands any longer. *See* David Drummond, *A New Approach to China* (March 23, 2010), http://googlepublicpolicy.blogspot.com/2010/03/new-approach-to-china-update.html.

[46] *See* Undermining Freedom of Expression in China, *supra* note 25; *Gates Backs China in Google Censorship Spat* (Jan. 27, 2010), http://www.theregister.co.uk/2010/01/27/gates_backs_china_google_censorship ("Gates shrugged off China's repressive online policies as simply part of doing business in a foreign country;" also noting that Gates told ABC, "[F]ortunately the Chinese efforts to censor the Internet have been very limited. You know, it is easy to go around it.").

Internet Explorer that allowed only that browser to connect with Facebook, and Facebook blocked all other browsers from accessing the site, users who wanted to access their accounts with Safari, Chrome, Firefox or any other browser could face criminal liability, which would chill their use of those competing browsers.

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 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) would therefore interfere with 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 recently sparked a storm of protest and concern due to changes to its terms of use and practices that made users' personal data increasingly accessible to third parties, including advertisers.[47] Facebook has also changed its policies with regard to certain user content. For example, in mid 2009, Facebook blocked some images from breastfeeding groups.[48] While Facebook may have the right to make these changes, its users certainly have the right to leave if they do not like the changes. The imposition of criminal liability for users selecting a tool that could easily move their data out of Facebook poses unacceptable risks to consumers and

[47] 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/.

[48] 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/.

innovators. Consumer choice would be limited not by natural competition, but a social network's privately imposed -- but publicly enforced -- terms, the penalty for non-compliance with which would be unacceptably steep.

VII. 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: June 21, 2010

ELECTRONIC FRONTIER FOUNDATION

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

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