

1 I. NEEL CHATTERJEE (STATE BAR NO. 173985)  
 nchatterjee@orrick.com  
 2 JULIO C. AVALOS (STATE BAR NO. 255350)  
 javalos@orrick.com  
 3 ORRICK, HERRINGTON & SUTCLIFFE LLP  
 1000 Marsh Road  
 4 Menlo Park, CA 94025  
 Telephone: +1-650-614-7400  
 5 Facsimile: +1-650-614-7401

6 JESSICA S. PERS (STATE BAR NO. 77740)  
 jpers@orrick.com  
 7 Orrick, Herrington & Sutcliffe LLP  
 The Orrick Building  
 8 405 Howard Street  
 San Francisco, CA 94105-2669  
 9 Telephone: +1-650-614-7400  
 Facsimile: +1-650-614-7401

10 THOMAS GRAY (STATE BAR NO. 191411)  
 tgray@orrick.com  
 11 Orrick, Herrington & Sutcliffe LLP  
 4 Park Plaza, Suite 1600  
 12 Irvine, CA 92614-2558  
 Telephone: +1-949-567-6700  
 13 Facsimile: +1-949-567-6710

14 Attorneys for Plaintiff  
 15 FACEBOOK, INC.

16 UNITED STATES DISTRICT COURT  
 17 NORTHERN DISTRICT OF CALIFORNIA  
 18 SAN JOSE DIVISION

20 FACEBOOK, INC.,  
 21 Plaintiff,  
 22 v.  
 23 POWER VENTURES, INC. a Cayman Island  
 Corporation; STEVE VACHANI, an  
 24 individual; DOE 1, d/b/a POWER.COM,  
 DOES 2-25, inclusive,  
 25 Defendants.  
 26

Case No. 5:08-cv-05780 JW (HRL)

**FACEBOOK, INC.’S REPLY TO  
 AMICUS CURIAE ELECTRONIC  
 FRONTIER FOUNDATION’S BRIEF  
 IN SUPPORT OF DEFENDANT  
 POWER VENTURES’ MOTION FOR  
 SUMMARY JUDGMENT**

27  
 28

**TABLE OF CONTENTS**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

	<b>Page(s)</b>
I. INTRODUCTION .....	1
II. ARGUMENT .....	2
A. Power Has Violated 502(c)'s Plain Language .....	2
B. Facebook Suffered "Damage" or "Loss" Sufficient to Warrant Injunctive Relief .....	4
C. Injunctive Relief Here Is Consistent With Statutory Intent and Sound Public Policy .....	5
D. The Case Law Confirms that Power's Actions Violated Section 502(c).....	7
E. Power's Efforts to Circumvent Facebook's Technical Measures to Block Power Confirm That Its Unauthorized Access to Facebook's Servers was Undertaken Knowingly .....	10
F. A Finding of Liability Against Power Would Not Be Unconstitutional.....	11
III. CONCLUSION .....	12



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**TABLE OF AUTHORITIES  
(Cont.)**

**STATE CASES**

**Page(s)**

*Chrisman v. City of Los Angeles*,  
155 Cal. App. 4th 29 (2007) ..... 9

*Intel Corp. v. Hamidi*,  
30 Cal. 4th 1342 (2003) ..... 10

*Leader v. State of California*,  
182 Cal. App. 3d 1079 (1986)..... 13

*Mahru v. Superior Court of the Los Angeles County*,  
191 Cal. App. 3d 545 (1987)..... 9

**STATUTES**

SEC Rule 10b-5 ..... 13

California Penal Code § 502(c)..... *passim*

1 **I. INTRODUCTION**

2 The Electronic Frontier Foundation’s (“EFF”) *amicus curiae* brief (“EFF Br.”) misses the  
3 point of Facebook’s motion, ignores the plain language and legislative history of 502(c) and, most  
4 fundamentally, ignores the facts of the case before the Court. This is not a case against a  
5 Facebook user for violating Facebook’s Terms of Service (“Terms”), nor does the case require the  
6 Court to assess the relative significance of various technical means website providers can employ  
7 to block access. Rather, this case raises a narrow, uncontroversial issue: whether a commercial  
8 entity that repeatedly and knowingly obtains user data from private computer servers in defiance  
9 of the server-owner’s repeated statement that the entity’s access was without permission violates  
10 California Penal Code 502(c). EFF ignores this question and, by focusing instead on parade-of-  
11 horribles hypotheticals about whether users could be punished criminally for violating  
12 Facebook’s Terms, fights a battle that is not raised by this action.

13 This case arose because *Power* (not its users) accessed Facebook’s servers and systems to  
14 take information without agreeing to safeguards designed to protect user data, even after  
15 Facebook specifically told Power to stop. Indeed, Power not only accessed and took data of users  
16 who signed up for Power’s service, but also of the Facebook friends of those users, who had not  
17 consented to the transfer. What is more, when Facebook implemented technical security  
18 measures to block Power’s unauthorized access, Power, by its own admission, “circumvented”  
19 them, thus confirming that it *knew* that its access was unauthorized. Nowhere in its brief does  
20 EFF acknowledge, much less address, these undisputed facts. Under the clear language of the  
21 statute as well as its legislative history, Power has violated Penal Code 502(c).

22 Although EFF claims that granting summary judgment for Facebook will hobble  
23 “competition, and innovation,” the opposite is true. Facebook has created a highly competitive  
24 system through Facebook “Connect,” which, as even EFF acknowledges, permits third parties to  
25 access Facebook’s servers and systems to provide applications for Facebook users – including the  
26 type of “aggregation” application Power claims to have developed – provided only that the third  
27 parties agree to terms designed to safeguard users’ privacy and data. Hundreds of thousands of  
28 other application developers have agreed to those terms, and they are providing hundreds of

1 thousands of applications that Facebook users enjoy every day. Power, however, does not want  
 2 to play by the same rules: it refuses to adhere to the safeguards that apply to all other developers,  
 3 yet seeks unbridled access to Facebook user data, including the data of users who have *not* agreed  
 4 to use Power's service. Facebook made abundantly clear that such access was without permission  
 5 and raised privacy and other concerns, and Facebook also made clear that it had established  
 6 Connect precisely so that Power, like other third-party developers, could interact with Facebook  
 7 while still respecting user privacy. Yet Power, after acknowledging as much, accessed  
 8 Facebook's servers and system without permission and through unauthorized means anyway.  
 9 Under the plain terms of the statute, Power's actions violated Section 502(c).

## 10 **II. ARGUMENT**

### 11 **A. Power Has Violated 502(c)'s Plain Language.**

12 Penal Code 502(c) provides, in relevant part, that any person who commits any of the  
 13 following acts violates the statute:

14 (2) Knowingly accesses and without permission takes, copies, or makes  
 15 use of any data from a computer, computer system, or computer network.

16 (3) Knowingly and without permission uses or causes to be used computer  
 17 services.

18 (7) Knowingly and without permission accesses or causes to be accessed  
 19 any computer, computer system, or computer network.

19 Power's own pleadings in this case establish the following:

- 20 • "Defendants developed computer software and other automated  
 21 devices and programs to access and obtain information from the  
 Facebook website for aggregating services." Dkt. 54 ¶ 74.
- 22 • Power "creates temporary cached copies of the Facebook website in  
 23 order to display it through the Power browser." *Id.* ¶ 75.
- 24 • Facebook told Power to stop accessing Facebook's servers, both through a  
 25 cease and desist letter and through e-mail and telephone conversations. *Id.* ¶  
 57.
- 26 • Following these communications from Facebook, Power first agreed to cease  
 27 its illegal activities but subsequently "'made the business decision" to continue  
 28 to access Facebook's servers without permission. Dkt. 57-1, Ex. A at 15.
- Upon learning that Power was renegeing on its agreement to stop illegally  
 accessing Facebook's computers, Facebook implemented technical measures

1 to block Power from accessing Facebook's servers. Dkt. 54 ¶ 63. As  
2 summarized by Power's own counsel, Power then "'did circumvent that  
3 barrier,' as 'established by the pleadings.'" Declaration of Julio C. Avalos In  
4 Support of Facebook's Reply to EFF Amicus Curiae Brief ("Avalos Decl."),  
5 Ex. A at 30:13-15.

6 These admissions are plainly sufficient to establish a violation of Section 502(c).  
7 Facebook specifically advised Power that its access to Facebook's servers was without  
8 permission, and it specifically directed Power to stop. By its own admission, Power ignored  
9 those communications and continued to access Facebook's servers, and it continued to make  
10 copies of the user data stored there, including data of users who had not signed up for Power's  
11 service. Power thus "knowingly access[ed] and without permission . . . cop[ied] or ma[de] use of  
12 . . . any data from a computer, computer system, or computer network," Penal Code 502(c)(2); it  
13 "[k]nowingly and without permission us[ed] or cause[ed] to be used computer services," *id.*,  
14 502(c)(3), and it "[k]nowingly and without permission accesse[d] or cause[d] to be accessed any  
15 computer, computer system, or computer network," *id.*, 502(c)(7). The case could hardly be  
16 simpler.

17 EFF asserts that "Power's service only accesses the user's own information and only  
18 makes use of that information as the user herself directs," and it claims as a result that Power's  
19 access to Facebook's servers was authorized. EFF Br. at 11:18-19. In fact, Power took from  
20 Facebook not only the information of its "own" users, but also of those users' friends, who had  
21 not signed up for Power's service. At least as important, there is nothing in the record to support  
22 the assertion that Power "only makes use of the user's information as the user herself directs."  
23 This case arose only because Power was unwilling to agree to Facebook's Terms, applicable to all  
24 developers, that would safeguard user privacy and otherwise limit Power's ability to engage in  
25 unacceptable actions with user data. If Power wanted to make use of user information only "as  
26 the user herself directs," presumably it would have been willing to agree to the same terms that  
27 bind all other developers.

28 More fundamentally, EFF's theory – that a third-party developer is as a matter of law  
entitled to unrestricted access to Facebook's servers because a user says so – is demonstrably  
incorrect. An individual's permission to access his or her own data cannot trump Facebook's

1 explicit directive to Power *not* to access its servers and take user data, any more than a bank  
2 account holder can authorize a third-party developer to hack into a bank’s servers and direct wire  
3 transfers in defiance of the bank’s express refusal to allow such access.<sup>1</sup> Indeed, Judge Fogel has  
4 already ruled as much in this very case, explaining that Facebook users may not authorize third-  
5 parties to access Facebook’s servers without Facebook’s permission. *See* Dkt. 38 at 7:24-28  
6 (“[t]his argument relies on an assumption that Facebook users are authorized to use Power.com or  
7 similar services to access their user accounts. The Terms of Use negate this argument . . . Users  
8 may have the right to access their own content, but conditions have been placed on that access.”).

9 **B. Facebook Suffered “Damage” or “Loss” Sufficient to Warrant Injunctive**  
10 **Relief.**

11 At the June 7, 2010 hearing, Power claimed that Facebook lacked standing to object to  
12 Power’s unauthorized access to Facebook’s servers, purportedly because Facebook had not  
13 suffered any “injury” or established “victim expenditures.” In fact, civil remedies are available  
14 under the statute to any “owner or lessee of the computer, computer system, computer network,  
15 computer program, or data who suffers *damage or loss* by reason of a violation of any of [the  
16 nine] provisions of subdivision (c).” Penal Code 502(e)(1) (emphasis added). Power’s  
17 protestations notwithstanding, this standing requirement does not use the terms “injury” or  
18 “victim expenditure.” Nor does the section exclude from the term “damage or loss” the time and  
19 expense of Facebook’s internal investigation or responsive actions (such as imposing technical  
20 blocking measures) – categories that are documented here and which Power does not dispute.  
21 *See, e.g.*, Dkt. 54 ¶¶ 57-58, 60, 63-64. And, despite Power’s arguments, the statute does not  
22 require Facebook to establish that its actions were “reasonable and necessary.” That language is  
23 from a provision related to the recovery of compensatory damages, which Facebook is not

---

24 <sup>1</sup> EFF claims that a bank customer should be permitted to “to use certain technology to assist her  
25 in making an otherwise legitimate deposit or withdrawal from her own account during regular  
26 business hours.” EFF Br. at 19:20-23, n. 21. Even if EFF were correct – and presumably bank  
27 owners would resist the notion that a third party application provider should have free rein to  
28 access their servers in any manner it wishes, provided an account holder gives the green light – it  
would have no bearing on this case. Power’s user information “withdrawal” from Facebook’s  
servers was in no sense “otherwise legitimate,” because it was undertaken in defiance of  
Facebook’s express direction that it was unauthorized.

1 seeking here, not injunctive relief. *See* Penal Code 502(e)(1) (“[C]ompensatory damages shall  
2 include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that  
3 a computer system, computer network, computer program, or data was not altered damaged, or  
4 deleted by the access.”).

5 C. **Injunctive Relief Here Is Consistent With Statutory Intent and Sound Public**  
6 **Policy.**

7 EFF argues that, irrespective of the statutory text, a finding in Facebook’s favor here  
8 would be “an extraordinary and dangerous extension of criminal law.” EFF Br. at 16:10-12. But  
9 EFF can make this claim only by distorting the issue presented. As noted at the outset, this case  
10 is not about whether a user who fails to adhere to a website’s terms when accessing his own  
11 account can be found liable under section 502(c), and it therefore does not invite the Court to  
12 address the parade of horrors featured in EFF’s brief. Rather, this case involves a third-party  
13 that, by its own admission, repeatedly accessed Facebook’s servers in order to obtain user data  
14 (including the data of Facebook users who had not authorized its service), after receiving and  
15 acknowledging express communications from Facebook directing it to stop. Far from  
16 “extraordinary and dangerous,” liability in these circumstances is consistent with legislative intent  
17 and commanded by sound public policy.

18 From its inception, 502(c) (previously Assembly Bill No. 2551) was designed to guard  
19 against any access to computer systems that occurred without permission of the computer system  
20 owner. The original bill was introduced in 1984 by California State Assemblyman Sam Farr,  
21 Chairman of the Assembly Committee of Economic Development and New Technologies, to  
22 close a perceived loophole in California’s computer trespass statute.<sup>2</sup> At the time, Penal Code  
23 502 already criminalized the “malicious” use of another’s computer. In response to a  
24 questionnaire asking “What problem or deficiency under existing law does the bill seek to  
25

---

26 <sup>2</sup> Notably, these amendments were introduced and passed two years prior to Congress’s enactment  
27 of the Computer Fraud and Abuse Act (“CFAA”) in 1986. Though EFF is correct that “[c]ourts  
28 interpreting section 502(c) have looked to ... the [CFAA] ... for guidance,” EFF Br. at 15-16, the  
statutes are not identical and the language of California’s broader, earlier-passed legislation  
should govern this case.

1 remedy?” Assemblyman Farr answered: “Non-malicious, but unauthorized, access of computers  
2 is currently not a crime, although such access can result in loss of personal privacy and costs to  
3 system owners to correct any damages or to assess whether or not damage to the system occurred  
4 as a result of the unauthorized access.” Avalos Decl., Ex. B.

5         Though both EFF and Power argue that Facebook is seeking to misapply a 1980s statute  
6 to a modern context, the interests Facebook seeks to vindicate here fall squarely within the  
7 interests the legislature sought to protect. Even apart from Assemblyman Farr’s explanation –  
8 which makes abundantly clear that 502(c) was designed to address precisely the sort of conduct at  
9 issue here – the statute’s original January 1984 preamble provides that “[t]he Legislature  
10 recognizes that the computer has now become an integral part of society. Because of this  
11 pervasiveness, the Legislature recognizes the need to protect the rights of owners and legitimate  
12 users of computer systems, as well as the privacy interests of the general public, from those who  
13 would abuse these systems.” *Id.*, Ex. C (emphasis added). The preamble continued:

14             The Legislature finds that with the increased availability and use of computers by  
15 private individuals and by both public and private sectors, there has been a  
16 corresponding increase in the incidence of misuse and intrusions by unauthorized  
17 individuals. In order to discourage “browsing,” which has led to destruction of  
18 property and numerous instances of invasion of privacy, as well as to punish the  
19 more serious offenders, it is the intent of the Legislature to establish a range of  
20 penalties to correspond with the level of culpability of individuals who abuse  
21 computer systems.

22             In an effort to protect the rights of the general public and the rights of legitimate  
23 users of computer systems, the Legislature hereby declares its intent to establish  
24 sanctions against unauthorized intrusions into computer systems which are not  
25 intended for general public use or for which access is limited by the owner or  
26 lessee.

27 *Id.* (emphasis added).

28         The California legislature, in short intended to capture exactly the sort of conduct that  
occurred here: Power’s “business decision” (Dkt. 57-1, Ex. A at 15) to knowingly access  
Facebook’s servers and to obtain data in the face of numerous express communications from  
Facebook over the course of a month directing Power to stop.

Nor is it the case, as EFF wrongly contends, that finding Power liable under the plain  
terms of the statute would inhibit competition and innovation. EFF Br. at 28:16-31:3. EFF

1 asserts that, by seeking to block Power from accessing its servers, Facebook is attempting to  
2 “prevent[] users from adopting follow-on innovation by third parties.” *Id.* at 30:5-6. As  
3 Facebook has emphasized throughout – and as Power itself has acknowledged, *see* Dkt. 54 ¶ 28  
4 Facebook created its “Connect” program specifically to enable third-party developers to develop  
5 “follow-on innovation,” and it makes that program available to providers *for free*. At the same  
6 time, in order to protect the user experience and safeguard user privacy, Facebook requires  
7 developers that use Connect to agree to Facebook’s Terms, and hundreds of thousands of  
8 developers do so without complaint. If, as EFF claims, Facebook is legally proscribed from  
9 enforcing those terms, it will inhibit Facebook’s ability to make Connect widely available and  
10 severely curtail the ability of third-party developers to create the “follow-on innovation” EFF  
11 claims to value.<sup>3</sup>

12 **D. The Case Law Confirms that Power’s Actions Violated Section 502(c).**

13 EFF contends that finding liability here would conflict with numerous cases interpreting  
14 section 502(c) and the analogous Computer Fraud and Abuse Act. *See* EFF Br. at 9-16. In fact,  
15 the case law uniformly establishes that where, as here, a third party accesses a website’s servers  
16 without permission for the purpose of scraping user data, the third party is liable under 502(c).

17 Thus, for example, in *Facebook, Inc. v. ConnectU*, 489 F. Supp. 2d 1087, 1091 (N.D. Cal.  
18 2007), the court found that Facebook had adequately stated a 502(c) violation against the  
19 ConnectU defendants based on their unauthorized access to Facebook’s servers. In so doing, the  
20 court specifically rejected the argument – which both EFF and Power press here – that the  
21 permission of Facebook *users* was enough to authorize the defendants’ access to Facebook’s  
22 servers. The court held that the statute required defendants to obtain *Facebook’s* permission prior  
23 to accessing *Facebook’s* servers. *Id.*

24 ///

25 \_\_\_\_\_  
26 <sup>3</sup> That EFF would seek to prevent Facebook from limiting what applications providers can do  
27 with user data is surprising, given EFF’s aggressive complaints elsewhere that Facebook is too  
28 permissive in enabling developers to obtain user data. *See, e.g.*, Electronic Frontier Foundation,  
“Open Letter to Facebook: More Privacy Improvements Needed,” [http://www.eff.org/press/  
archives/2010/06/16](http://www.eff.org/press/archives/2010/06/16) (last visited July 4, 2010).

1 Similarly, one of the most recent 502(c) cases found defendants liable when they copied  
2 files from the plaintiff's computer systems without the plaintiff's permission and despite the fact  
3 that such copying did not damage the plaintiff's servers. *Joseph Oat Holdings, Inc. v. RCM*  
4 *Digesters, Inc.*, 665 F. Supp. 2d 448, 455-56 (D. N.J. 2009) (applying California law).<sup>4</sup> In this  
5 District, Judges Hamilton and James also recently reaffirmed the application of 502(c) to cases of  
6 unauthorized access to computer servers and websites. *See Craigslist, Inc. v. Naturemarket, Inc.*,  
7 No. C 08-05065 PJH (MEJ), 2010 U.S. Dist. LEXIS 19992, at \*5-6 (N.D. Cal., Jan. 28, 2010),  
8 *adopted by Craigslist, Inc. v. Naturemarket, Inc.*, No. C 08-05065 PJH, 2010 U.S. Dist. LEXIS  
9 19977 (N.D. Cal., Mar. 5, 2010) ("*Craigslist*"). In a direct analog to the present case, the  
10 *Craigslist* defendants were found to have violated 502(c) by offering an automated service that  
11 permitted their users to post or remove advertisements on the Craiglist.com website in violation  
12 of Craigslist's terms of use and in circumvention of Craigslist's security measures. *Id.* at \*5-6; *see*  
13 *also Oracle Corp. v. SAP AG*, No. C 07-1658 (PJH), 2008 U.S. Dist. LEXIS 103300 (N.D. Cal.,  
14 Dec. 15, 2008) (denying motion to dismiss 502(c) claim based on the defendants' improper  
15 copying of software and support materials in violation of Oracle's license terms). Further,  
16 numerous cases have found liability under the CFAA on similar facts. *See, e.g., EF Cultural*  
17 *Travel BV v. Zefer Corp.*, 318 F.3d 58, 62 (1st Cir. 2003); *Southwest Airlines v. Farechase, Inc.*,  
18 318 F. Supp. 2d 435, 439-40 (N.D. Tex. 2004); *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d  
19 238, 253 (S.D.N.Y. 2000) ("*Register.com*").

20 EFF's attempts to marginalize this well-established precedent fail. For example, EFF  
21 mischaracterizes *Register.com*, stating that the appellate court there reversed "the trial court's  
22 CFAA finding on the basis that there was insufficient likelihood of showing the \$5000 damage  
23 threshold necessary for private claims." EFF's Br. at 19-20. In fact, the appellate court affirmed  
24 the trial court's finding of computer trespass liability. *Register.com*, 126 F. Supp. 2d at 253.

25 \_\_\_\_\_  
26 <sup>4</sup> The *Joseph Oat* court found a 502(c) violation despite the defendants' claims that they were  
27 accessing the plaintiff's computers for a legitimate, worthwhile purpose (discovery preservation).  
28 *Id.* at 456 ("Plaintiff's copying . . . was done to protect their business interests, not to gain a  
litigation advantage in this case."). Similarly, Power's pretext of Internet "liberation" – and  
EFF's espousal of that pretext – does not disturb the commercial nature of Power's unauthorized  
access nor the illegal nature of that access.

1 Similarly, in its attempt to distinguish *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d  
2 1058 (N.D. Cal. 2000), EFF emphasizes that Power obtained Facebook users' consent to access  
3 their Facebook accounts. In *eBay*, however, in finding the defendant did not have authorized  
4 access to the plaintiff's servers for a claim of trespass, the court stated "[plaintiff's] servers were  
5 private property, conditional access to which [plaintiff] grants the public. [Plaintiff] does not  
6 generally permit the type of automated access made by [defendants]." The same is true here. As  
7 in *eBay*, Facebook's servers are private property, and Power had no authority to use them in the  
8 face of express communications demanding that it cease doing so.

9 EFF also cites a string of cases that it claims exonerate conduct akin to Power's, such as  
10 *Mahru v. Superior Court of the Los Angeles County*, 191 Cal. App. 3d 545, 549 (1987) and  
11 *Chrisman v. City of Los Angeles*, 155 Cal.App.4th 29 (2007), and a handful of CFAA cases.  
12 Even on EFF's own reading, these cases are beside the point here. As EFF explains it, these  
13 opinions stand only for the proposition that, when a user has permission to access servers and  
14 systems, exceeding the approved permission does not violate 502(c) or the CFAA. Even if this  
15 were correct, it has nothing to do with this case. Power had *no permission* from Facebook to  
16 access Facebook's computer servers, or the data contained thereon, at all. The record consistently  
17 establishes that Facebook repeatedly notified Power of this fact.

18 EFF also relies upon *United States v. Drew*, 259 F.R.D. 449, 465 (C.D. Cal. 2009), a civil  
19 spin-off of the infamous Lori Drew "cyber-bullying" matter, where a fourteen year old girl  
20 committed suicide due to the cyber-bullying of a peer's mother (Drew) who was pretending to be  
21 a fellow high school student on MySpace.com. As the *Drew* court summarized, "the only basis  
22 for finding that [defendant] Drew intentionally accessed MySpace's computer/servers without  
23 authorization and/or in excess of authorization was her and/or her co-conspirator's violations of  
24 the MSTOS [MySpace Terms of Service] by deliberately creating the false Josh Evans profile,  
25 posting a photograph of a juvenile without his permission and pretending to be a sixteen year  
26 old." *Id.* at 461. Unlike *Drew*, this is not a situation where a Facebook user merely disregarded  
27 Facebook's Terms and *unknowingly* violated section 502(c) because he or she did not understand  
28 the terms. Again, Facebook specifically told Power it had no permission to access Facebook's

1 servers. Knowing that, Power nonetheless made a “business decision” to access Facebook’s  
2 servers and obtain user data. That defiant conduct is far afield from the conduct at issue in *Drew*.

3 Finally, EFF incorrectly relies upon *Intel Corp. v. Hamidi*, 30 Cal.4th 1342, 1346 (2003).  
4 *Hamidi* involved allegations of nuisance and trespass to chattels, not 502(c) or the CFAA, and in  
5 any case involved nothing more than a former employee emails on the plaintiff’s e-mail system.  
6 The case is self-evidently besides the point.

7 **E. Power’s Efforts to Circumvent Facebook’s Technical Measures to Block**  
8 **Power Confirm That Its Unauthorized Access to Facebook’s Servers was**  
9 **Undertaken Knowingly.**

10 At the conclusion of the June 7, 2010 hearing, the Court invited the parties to address the  
11 relevance of the technical measures Facebook put in place to block Power’s access to its servers.  
12 Consideration of those measures is not necessary to dispose of this case: Power’s conduct – in  
13 particular, its continued access to Facebook’s servers to obtain user data even after Facebook  
14 specifically advised Power that its actions were without permission and directed Power to stop –  
15 violated section 502(c) even apart from Power’s circumvention of the technical blocking  
16 Facebook put in place to stop Power’s unauthorized access. But if there were any doubt on that  
17 question, Power’s efforts to circumvent Facebook’s technical measures confirm that Power acted  
18 knowingly when it accessed Facebook’s servers without permission.

19 As explained above, Power’s own admissions establish that it continued to access  
20 Facebook’s servers to obtain user data even after Facebook specifically advised Power that its  
21 access was unauthorized and directed it to stop. This alone is sufficient to establish 502(c)  
22 knowledge requirements. But if the Court were to require more, the mens rea here is further  
23 established by Power’s admission that it circumvented the “IP blocking” measures implemented  
24 by Facebook after Power was told to stop and refused to do so. *See* Dkt. 54 ¶ 63 and Avalos  
25 Decl., Ex. A. As Power’s own counsel explained to the court, the pleadings establish that, when  
26 Facebook put in place a “barrier[]” to prevent Power’s access, Power “did circumvent that  
27 barrier.” Avalos Decl., Ex. A at 30:13-15. In light of that admission, there can be no dispute that  
28 Power acted with the requisite mens rea to establish a violation of section 502(c).

1           Indeed, EFF admits as much. In its own words, “[i]f a provider implemented blocking to  
2 prevent access by unauthorized persons, and an unauthorized person evaded that block as part of  
3 gaining access, that person may well have violated section 502(c)(3) or (7).” EFF Br. at 24:4-7;  
4 *see id.* at 24:11-13. This is precisely the case before the Court.

5           To be sure, EFF adds that not *all* conduct that results in evading an IP block is culpable  
6 under 502(c), because changing one’s IP address is a simple and often innocent gesture. EFF Br.  
7 at 19:10-24:17. That may be so, but it has nothing to do with this case. Here, there is no dispute  
8 that Power circumvented the IP blocking Facebook put in place not because it changed its address  
9 or was seeking to avoid censorship by the Chinese government, *see* EFF Br. at 29:2-10, but  
10 because it wanted to continue accessing Facebook’s servers in order to obtain user data even after  
11 Facebook specifically directed it to stop. That admitted fact further confirms that Power  
12 knowingly accessed Facebook’s servers without permission to obtain user data, in violation of  
13 Section 502(c).<sup>5</sup>

14           **F. A Finding of Liability Against Power Would Not Be Unconstitutional.**

15           EFF’s final argument is that a finding of liability against Power would render 502(c)  
16 unconstitutionally vague or overbroad. According to EFF, as a private party, Facebook may not  
17 define what is or is not criminal under the statute. EFF Br. at 24:24-25:8. But it was the  
18 Legislature, not Facebook, that defined what behavior is actionable under 502(c). In *ConnectU*,  
19 Judge Seeborg rejected this exact theory, finding that “ConnectU’s argument that a private party  
20 cannot define what is or is not a criminal offense by unilateral imposition of terms and conditions  
21 of use is not persuasive. The *statute* defines the criminal offense: taking, copying, or using data  
22 ‘without permission.’ The fact that private parties are free to set the conditions on which they will  
23

---

24  
25 <sup>5</sup> Power’s suggestion that there is factual uncertainty here because the parties were “in  
26 negotiations” while the blocking was put in place is a red herring. There were no “negotiations”  
27 with Power—Facebook told Power that if it wanted to access Facebook, it needed to do so  
28 through Facebook Connect. *See* Dkt. 57-1 at pp. 2-15. Power agreed but soon reneged on the  
agreement. *Id.* at p. 15. Subsequently, Facebook blocked Power’s IP address and Power  
promptly circumvented that block. Dkt. 54 ¶ 63; Avalos Decl., Ex. A at 30:13-15. Nothing more  
is necessary to establish that Power acted knowingly and without permission.

1 grant such permission does not mean that private parties are defining what is criminal and what is  
2 not.” *ConnectU*, 498 F. Supp. 2d at 1091 (emphasis in original).

3 Relatedly, the Court should reject EFF’s claim that the application of a criminal statute to  
4 a civil context is somehow improper or unfair. Here again, the Legislature, not Facebook,  
5 provided for both criminal and civil remedies to 502(c) violations. Such civil/criminal schemes  
6 are common, *see, e.g., United States v. Laurienti*, No. 07-50240, 2010 WL 2473573, at \*4 (9th  
7 Cir., June 16, 2010) (observing that securities violations can give “rise to both civil liability and  
8 criminal liability”), and do not require the Court to bring any heightened caution in adjudicating a  
9 civil dispute. Nor will a finding of civil liability here translate directly into a criminal conviction  
10 against Power. In any prosecution, the government would be required to meet higher standards  
11 and burdens as compared to a civil litigant seeking damages and/or injunctive relief. *United*  
12 *States v. Selgado*, No. 98-50018, 1999 U.S. Dist. LEXIS 1319, at \*11 (9th Cir. 1999) (“a criminal  
13 proceeding requires a higher standard of proof than the proof required in the civil ... hearing”);  
14 *see also Leader v. State of California*, 182 Cal.App.3d 1079, 1087 (1986) (“The cases stress that a  
15 criminal proceeding has a higher standard of proof than a civil one; therefore it is particularly  
16 appropriate to apply a criminal conviction to a civil action, while the reverse would not be true.”).  
17 Indeed, the findings in this case would almost certainly be inadmissible to establish facts in a  
18 subsequent criminal prosecution. *See United States v. Meza-Soria*, 935 F.2d 166, 169-70 (9th  
19 Cir. 1991) (“[T]he difference in standards of proof must preclude the use of civil proceeding  
20 findings to establish facts in a criminal case.”).

### 21 **III. CONCLUSION**

22 For the foregoing reasons, Facebook requests that the Court reject the arguments set forth  
23 in EFF’s *amicus curiae* brief and grant Facebook’s motion concerning its California Penal Code  
24 502(c) claim.

25 Dated: July 6, 2010

ORRICK, HERRINGTON & SUTCLIFFE LLP

27 \_\_\_\_\_  
JULIO C. AVALOS  
Attorneys for Plaintiff,  
28 FACEBOOK, INC.