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

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

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

Attorneys for Plaintiff
FACEBOOK, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

FACEBOOK, INC.,

Plaintiff,

v.

POWER VENTURES, INC. a Cayman Island Corporation; STEVE VACHANI, an individual; DOE 1, d/b/a POWER.COM, DOES 2-25, inclusive,

Defendants.

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

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

FEDERAL CASES

Page(s)

TABLE OF AUTHORITIES
(Cont.)

STATE CASES

Page(s)

STATUTES

I. INTRODUCTION

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

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

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

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

II. ARGUMENT

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

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

> (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network.
>
> (3) Knowingly and without permission uses or causes to be used computer services.
>
> (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

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

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

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

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

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

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

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

B. Facebook Suffered "Damage" or "Loss" Sufficient to Warrant Injunctive Relief.

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

[1] EFF claims that a bank customer should be permitted to "to use certain technology to assist her in making an otherwise legitimate deposit or withdrawal from her own account during regular business hours." EFF Br. at 19:20-23, n. 21. Even if EFF were correct – and presumably bank owners would resist the notion that a third party application provider should have free rein to 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.

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

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

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

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

[2] Notably, these amendments were introduced and passed two years prior to Congress's enactment of the Computer Fraud and Abuse Act ("CFAA") in 1986. Though EFF is correct that "[c]ourts 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.

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

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

> The Legislature finds that with the increased availability and use of computers by private individuals and by both public and private sectors, there has been a corresponding increase in the incidence of misuse and intrusions by unauthorized individuals. In order to discourage "browsing," which has led to destruction of property and numerous instances of invasion of privacy, as well as to punish the more serious offenders, it is the intent of the Legislature to establish a range of penalties to correspond with the level of culpability of individuals who abuse computer systems.
>
> In an effort to protect the rights of the general public and the rights of legitimate users of computer systems, the Legislature hereby declares its intent to establish sanctions against unauthorized intrusions into computer systems which are not intended for general public use or for which access is limited by the owner or lessee.

Id. (emphasis added).

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

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

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

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

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

/ / /

[3] That EFF would seek to prevent Facebook from limiting what applications providers can do with user data is surprising, given EFF's aggressive complaints elsewhere that Facebook is too 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 (last visited July 4, 2010).

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

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

[4] The *Joseph Oat* court found a 502(c) violation despite the defendants' claims that they were accessing the plaintiff's computers for a legitimate, worthwhile purpose (discovery preservation). *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.

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

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

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

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

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

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.

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

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

Indeed, EFF admits as much. In its own words, "[i]f 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)." EFF Br. at 24:4-7; *see id.* at 24:11-13. This is precisely the case before the Court.

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

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

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

[5] Power's suggestion that there is factual uncertainty here because the parties were "in negotiations" while the blocking was put in place is a red herring. There were no "negotiations" with Power—Facebook told Power that if it wanted to access Facebook, it needed to do so 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.

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

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

III. CONCLUSION

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

Dated: July 6, 2010

ORRICK, HERRINGTON & SUTCLIFFE LLP

JULIO C. AVALOS
Attorneys for Plaintiff,
FACEBOOK, INC.