

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

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA

JOHN DOE, et al.,  
Plaintiffs,  
v.  
KAMALA D. HARRIS, et al.,  
Defendants.

NO. C12-5713 TEH  
ORDER GRANTING  
PLAINTIFFS' MOTION FOR A  
PRELIMINARY INJUNCTION

This matter came before the Court on December 17, 2012, on Plaintiffs' motion for a preliminary injunction. Plaintiffs challenge several provisions of the Californians Against Sexual Exploitation Act ("CASE Act" or "Act") that require registered sex offenders to provide certain information concerning their Internet use to law enforcement. Having carefully considered the parties' written and oral arguments, the Court now GRANTS preliminary injunctive relief for the reasons explained below.

**I. BACKGROUND**

On November 6, 2012, California voters approved the CASE Act, which appeared on the ballot as Proposition 35, with approximately 81% of the vote. Ex. D to Intervenor's Req. for Judicial Notice at 1.<sup>1</sup> Plaintiffs John Doe, Jack Roe,<sup>2</sup> and the non-profit organization California Reform Sex Offender Laws filed this action on behalf of present and future

---

<sup>1</sup>The Court GRANTS Intervenor's unopposed request for judicial notice in its entirety.

<sup>2</sup>The Court granted the two individual plaintiffs' unopposed motion to proceed anonymously during the pendency of the preliminary injunction motion on November 15, 2012.

1 California sex offender registrants the following day, when the Act was to take effect.<sup>3</sup> *See*  
2 Cal. Const. art. II, § 10(a). They contend that California Penal Code sections 290.014(b) and  
3 290.015(a)(4)-(6), as enacted by the CASE Act, violate Plaintiffs' First Amendment rights to  
4 free speech and free association. They further contend that the provisions are void for  
5 vagueness under the Fourteenth Amendment.

6 California's sex offender registration program is governed by California Penal Code  
7 section 290 *et seq.* The CASE Act added the following items to the list of information  
8 registrants must provide "upon release from incarceration, placement, commitment, or  
9 release on probation":

10 (4) A list of any and all Internet identifiers established or used  
11 by the person.

12 (5) A list of any and all Internet service providers used by the  
13 person.

14 (6) A statement in writing, signed by the person, acknowledging  
15 that the person is required to register and update the  
16 information in paragraphs (4) and (5), as required by this  
17 chapter.

18 Cal. Penal Code § 290.015(a). In addition, items (4) and (5) must be reported as part of the  
19 annual registration process. *Id.* § 290.012(a).

20 The Act defines "Internet service provider" as "a business, organization, or other  
21 entity providing a computer and communications facility directly to consumers through  
22 which a person may obtain access to the Internet," except for any "business, organization, or  
23 other entity that provides only telecommunications services, cable services, or video services,  
24 or any system operated or services offered by a library or educational institution." *Id.*  
25 § 290.024(a). "Internet identifier" is defined as "an electronic mail address, user name,  
26 screen name, or similar identifier used for the purpose of Internet forum discussions, Internet  
27 chat room discussions, instant messaging, social networking, or similar Internet  
28 communication." *Id.* § 290.024(b).

---

<sup>3</sup>California has over 75,000 registrants, excluding those who are incarcerated and those who have been deported. Cal. Dep't of Justice, *Cal. Sex Registrant Statistics* (Jan. 10, 2013), <http://www.meganslaw.ca.gov/statistics.aspx?lang=ENGLISH>.

1           The CASE Act also added a provision that requires registrants to notify law  
2 enforcement within 24 hours of any changes in the Internet information subject to  
3 registration:

4                     If any person who is required to register pursuant to the Act adds  
5 or changes his or her account with an Internet service provider or  
6 adds or changes an Internet identifier, the person shall send  
7 written notice of the addition or change to the law enforcement  
8 agency or agencies with which he or she is currently registered  
9 within 24 hours. The law enforcement agency or agencies shall  
10 make this information available to the Department of Justice.

11 *Id.* § 290.014(b). This section further requires all registrants to “immediately provide” the  
12 required information to law enforcement upon the effective date of the Act. *Id.*

13           Following a telephonic hearing, the Court granted Plaintiffs’ motion for a temporary  
14 restraining order (“TRO”) on November 7, 2012, and enjoined “Defendant Kamala Harris  
15 and her officers, agents, servants, employees, and attorneys, and those persons in active  
16 concert or participation with her . . . from implementing or enforcing California Penal Code  
17 sections 290.014(b) and 290.015(a)(4)-(6), as enacted by Proposition 35, or from otherwise  
18 requiring registrants to provide identifying information about their online speech to the  
19 government.” Nov. 7, 2012 Order at 3. Pursuant to the parties’ agreement, the Court  
20 explicitly applied this order “to all California state and local law enforcement officers and to  
21 all members of the putative class, i.e., to all persons who are required to register under  
22 California Penal Code section 290, including those whose duty to register arises after the date  
23 of this order.” *Id.*

24           On November 14, 2012, the Court entered a stipulation and order deleting the  
25 application of the TRO to “all California state and local law enforcement officers,” but  
26 providing that “the California Department of Justice and local law enforcement will not  
27 require registrants to submit the information covered by the TRO so long as the TRO remains  
28 in effect.” Nov. 14, 2012 Stip. & Order ¶ 3. The parties further agreed that the TRO would  
remain in effect “until the Court issues its ruling on Plaintiffs’ Motion for a Preliminary  
Injunction or January 11, 2013, whichever occurs first,” *id.* ¶ 4, and that “any preliminary  
injunctive relief granted by the Court will apply both to the named Plaintiffs and to all

1 persons who are required to register under California Penal Code § 290, including those  
2 whose duty to register arises during the pendency of the TRO and any preliminary injunctive  
3 relief,” *id.* ¶ 2. In addition, the parties agreed that this matter would be litigated as a facial  
4 challenge unless and until Plaintiffs provide the Attorney General with at least 45 days notice  
5 that they intend to raise an as-applied challenge. *Id.* ¶ 6.

6 Chris Kelly and Daphne Phung, the proponents of Proposition 35, moved to intervene  
7 on November 12, 2012. Although the Court did not grant the motion to intervene until  
8 January 10, 2013, Intervenors filed a written opposition and addressed the Court at oral  
9 argument. Thus, they were fully heard on Plaintiffs’ motion for a preliminary injunction.

## 11 **II. LEGAL STANDARD**

12 To obtain a preliminary injunction, Plaintiffs must establish that: (1) they are likely to  
13 succeed on the merits; (2) they are likely to suffer irreparable harm in the absence of the  
14 preliminary injunction; (3) the balance of equities tips in their favor; and (4) the issuance of  
15 the preliminary injunction is in the public interest. *Winter v. Natural Res. Def. Council, Inc.*,  
16 555 U.S. 7, 20 (2008). A stronger showing on one of these four elements may offset a  
17 weaker showing on another, but the movant must nonetheless “make a showing on all four  
18 prongs.” *Alliance for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1134-35 (9th Cir. 2011).

## 20 **III. DISCUSSION**

### 21 **A. Likelihood of Success on the Merits**

22 The Court first considers Plaintiffs’ likelihood of success on the merits. Because the  
23 Court finds Plaintiffs likely to succeed on their First Amendment speech claim for the  
24 reasons discussed below, it does not address whether Plaintiffs are likely to succeed on any  
25 of their remaining claims.

#### 26 **1. First Amendment Legal Principles**

27 This case concerns the First Amendment’s protection of the right to speak  
28 anonymously online. See *In re Anonymous Online Speakers*, 661 F.3d 1168, 1173 (9th Cir.

1 2011). It is undisputed that speech by sex offenders who have completed their terms of  
2 probation or parole enjoys the full protection of the First Amendment. Rep. Tr. at 21:11-15  
3 (Plaintiffs), 51:4-10 (government), 51:23-24 (Intervenors); *see also Simon & Schuster, Inc.*  
4 *v. Members of N.Y. State Crime Victims Bd.*, 502 U.S. 105 (1991) (striking down New York  
5 law that sought to interfere with criminals’ profiting from works describing their crimes).  
6 The provisions at issue here are not outright bans on anonymous online speech, but they may  
7 still violate the First Amendment if they impermissibly burden such speech: “[T]he  
8 distinction between laws burdening and laws banning speech is but a matter of degree . . . .  
9 Lawmakers may no more silence unwanted speech by burdening its utterance than by  
10 censoring its content.” *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 2664 (2011) (internal  
11 quotation marks and citation omitted).<sup>4</sup>

12 Plaintiffs here challenge the CASE Act as facially overbroad. Although Plaintiffs  
13 bear the burden of demonstrating a likelihood of success on the merits under the preliminary  
14 injunction standard, the government ultimately “bears the burden of proving the  
15 constitutionality of its actions” whenever it seeks to restrict speech. *United States v. Playboy*  
16 *Entm’t Grp., Inc.*, 529 U.S. 803, 816 (2000).

17 To succeed on a facial overbreadth challenge under the First Amendment, a plaintiff  
18 must demonstrate either “that no set of circumstances exists under which [the statute] would  
19 be valid,” or that “a substantial number of [the statute’s] applications are unconstitutional,  
20 judged in relation to the statute’s plainly legitimate sweep.” *United States v. Stevens*, 130 S.  
21 Ct. 1577, 1587 (2010) (internal quotation marks and citations omitted). The Court’s inquiry  
22 is not limited to the application of the challenged provisions to the particular plaintiffs before  
23 it, as “[l]itigants . . . are permitted to challenge a statute not because their own rights of free  
24 expression are violated, but because of a judicial prediction or assumption that the statute’s  
25 very existence may cause others not before the court to refrain from constitutionally

---

26 <sup>4</sup>That the challenged provisions were enacted by voter initiative does not alter the  
27 constitutional analysis. “The voters may no more violate the United States Constitution by  
28 enacting a ballot issue than the general assembly may by enacting legislation.” *Buckley v.*  
*Am. Constitutional Law Found., Inc.*, 525 U.S. 182, 194 (1999) (internal quotation marks and  
citation omitted).

1 protected speech or expression.” *Broadrick v. Oklahoma*, 413 U.S. 601, 612 (1973).

2 However, “the mere fact that one can conceive of some impermissible applications of a  
3 statute is not sufficient to render it susceptible to an overbreadth challenge.” *Members of the*  
4 *City Council of L.A. v. Taxpayers for Vincent*, 466 U.S. 789, 800 (1984).

5 Plaintiffs urge the Court to subject the challenged provisions to strict scrutiny because  
6 they discriminate against registrants as a class of speakers. However, strict scrutiny is only  
7 required where “speaker-based laws . . . reflect the government’s preference for the  
8 substance of what the favored speakers have to say (or aversion to what the disfavored  
9 speakers have to say).” *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 658 (1994). Here,  
10 the Act reflects no such preference and operates without regard to the message that any  
11 registrant’s speech conveys. The challenged provisions are therefore content-neutral, and  
12 intermediate scrutiny applies. *Id.* at 662; *see also Doe v. Shurtleff*, 628 F.3d 1217, 1223  
13 (10th Cir. 2010) (applying intermediate scrutiny to Utah reporting requirement that said  
14 “nothing about the ideas or opinions that [registrants] may or may not express, anonymously  
15 or otherwise” and were not “aimed at suppressing the expression of unpopular views”  
16 (internal quotation marks, alteration, and citation omitted)).

17 Under intermediate scrutiny, a law must “be narrowly tailored to serve the  
18 government’s legitimate, content-neutral interests.” *Comite de Jornaleros de Redondo*  
19 *Beach v. City of Redondo Beach*, 657 F.3d 936, 947 (9th Cir. 2011) (en banc), *cert. denied*,  
20 132 S. Ct. 1566 (2012) (quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 798 (1989)).  
21 “To satisfy this standard, the law need not be the least speech-restrictive means of advancing  
22 the Government’s interests”; the test is whether “the means chosen . . . burden substantially  
23 more speech than is necessary to further the government’s legitimate interests.” *Turner*, 512  
24 U.S. at 662 (internal quotation marks and citation omitted). The “essence of narrow  
25 tailoring” is to “focus[] on the source of the evils the [government] seeks to eliminate . . . and  
26 eliminate[] them without at the same time banning or significantly restricting a substantial  
27 quantity of speech that does not create the same evils.” *Ward*, 491 U.S. at 799 n.7.

28

1                                   **2.        Construing the Statute**

2            Before determining whether a challenged provision violates the First Amendment, a  
3 court must first construe the provision; “it is impossible to determine whether a statute  
4 reaches too far without first knowing what the statute covers.” *United States v. Williams*,  
5 553 U.S. 285, 293 (2008). In doing so, the Court must consider the government’s “own  
6 implementation and interpretation,” but it is “not required to insert missing terms into the  
7 statute or adopt an interpretation precluded by the plain language of the ordinance.” *Comite*,  
8 657 F.3d at 946 (internal quotation marks and citations omitted). Instead, the court may  
9 impose a limiting construction only if a provision is, on its face, “readily susceptible” to such  
10 a construction. *Reno v. ACLU*, 521 U.S. 844, 884 (1997) (internal quotation marks and  
11 citation omitted). Applying these principles to this case, the Court finds that the reporting  
12 requirements for “Internet service providers” and “Internet identifiers” are readily  
13 susceptible to the narrowing constructions discussed at oral argument and advanced by the  
14 government.<sup>5</sup>

15                                   **a.        “Internet service provider”**

16            The CASE Act defines “Internet service provider” as a “business, organization, or  
17 other entity providing a computer and communications facility directly to consumers through  
18 which a person may obtain access to the Internet,” excluding any “business, organization, or  
19 other entity that provides only telecommunications services, cable services, or video services,  
20 or any system operated or services offered by a library or educational institution.” Cal. Penal  
21 Code § 290.024(a). Pursuant to § 290.015(a)(5), a person subject to the reporting

---

22            <sup>5</sup>The government and Intervenor also suggest that, in construing the reporting  
23 requirements, the Court may look to the federal standards for state sex offender registry and  
24 notification systems developed under the Sex Offender Registration and Notification Act  
25 (“SORNA”). *See* 42 U.S.C. § 16915a(a) (providing for collection of “those Internet  
26 identifiers the sex offender uses or will use of any type that the Attorney General determines  
27 to be appropriate”); Nat’l Guidelines for Sex Offender Registration and Notification, 73 Fed.  
28 Reg. 38,030-01 at 38,055 (July 2, 2008) (U.S. Attorney General guidelines for state  
registries to include “all designations used by sex offenders for purposes of routing or  
self-identification in Internet communications or postings”). The Court does not find it  
necessary to rely on SORNA for this purpose because, as discussed below, it finds the  
construction of the statutes proposed by the government and Intervenor to be supported by  
the statutes’ plain language. Neither the government nor Intervenor argue that SORNA  
affects the Court’s analysis on any other issue.

1 requirements must, upon registration, provide to law enforcement “[a] list of any and all  
2 Internet service providers used by the person.” At oral argument, the government stated that  
3 the plain language of the Act limits this requirement to only “Internet service providers with  
4 which the registrant has an open account at the time of the registration.” Rep. Tr. at 48:2-15;  
5 *cf. id.* at 49:2-5 (noting Intervenors’ agreement). Plaintiffs acknowledged that it would be  
6 permissible for the Court to construe the statute in this manner, *id.* at 17:15-18:1, and the  
7 Court now does so. Reading section 290.015(a)(5) to exclude providers that are only  
8 accessed or used by the registrant, as opposed to those with which the registrant has an  
9 account, is consistent with both the common understanding of “Internet service provider” and  
10 California Penal Code section 290.014(b), which requires a registrant to update law  
11 enforcement only when he or she “adds or changes his or her *account* with an Internet  
12 service provider” (emphasis added).

13 **b. “Internet identifier”**

14 The CASE Act’s definition of “Internet identifier” – “an electronic mail address, user  
15 name, screen name, or similar identifier used for the purpose of Internet forum discussions,  
16 Internet chat room discussions, instant messaging, social networking, or similar Internet  
17 communication” – is also readily susceptible to a construction that avoids many of the  
18 potential problems suggested by Plaintiffs. *Id.* § 290.024(b).<sup>6</sup> The Act may be reasonably  
19 interpreted to require reporting only of Internet identifiers actually used to post a comment,  
20 send an email, enter into an Internet chat, or engage in another type of interactive  
21 communication on a website, and not identifiers a registrant uses solely to purchase products  
22 or read content online. *See* Rep. Tr. at 63:8-16 (Intervenors suggesting this rule); *id.* at  
23 64:22-24 (government focusing on “interactive communications” as the test for whether an  
24 Internet identifier must be reported); *id.* at 37:5-8 (Plaintiffs saying that it would be

---

25  
26  
27 <sup>6</sup>Plaintiffs expressed fear that law enforcement may subsequently decide to require  
28 registrants to report the websites associated with their Internet identifiers. However, as  
Plaintiffs acknowledge, the Act’s language requires the reporting only of Internet identifiers  
and not associated websites. Mot. at 22-23.

1 reasonable to interpret the Act to “count[] once you actually use that account to post  
2 something”).<sup>7</sup>

3 This interpretation raises the question of when a registrant must report an Internet  
4 identifier that could potentially be used for interactive communication but that the registrant  
5 initially uses only to view content or make a purchase online. At oral argument, the  
6 government assured the Court that it would not require a registrant to report such an  
7 identifier upon creating it, but that a registrant would have to report the identifier within 24  
8 hours of first using the identifier to engage in interactive communication. Rep. Tr. at 65:21-  
9 66:11. The Court finds this construction to be reasonable.

10 Consistent with the above discussion, the Court construes the challenged provisions  
11 as requiring registrants to report: (1) “Internet service providers” with which the registrant  
12 has a current account at the time of registration or with which the registrant later creates an  
13 account, and (2) “Internet identifiers” that are actually used by the registrant to engage in  
14 interactive communication with others, within 24 hours of the registrant’s first use of the  
15 identifier for interactive communication.

### 16 3. Narrow Tailoring

17 The Court now turns to whether Plaintiffs are likely to succeed in showing that the  
18 challenged provisions, as just construed, fail to satisfy the First Amendment under  
19 intermediate scrutiny. This requires the Court to determine whether the provisions are  
20 “narrowly tailored to serve the government’s legitimate, content-neutral interests.” *Comite*,  
21 657 F.3d at 947 (internal quotation marks and citation omitted).

22 The CASE Act’s stated purposes include “combat[ing] the crime of human  
23 trafficking” and “strengthen[ing] laws regarding sexual exploitation, including sex offender  
24 registration requirements, to allow law enforcement to track and prevent online sex offenses

---

25  
26 <sup>7</sup>The government suggested that blog usernames need not be reported as long as the  
27 blog did not permit interactive comments. Rep. Tr. at 63:17-19. The Court declines to  
28 interpret the statute in this fashion since the government has not explained why a registrant’s  
use of his or her own non-interactive blog to comment should be distinguished from his or  
her posting the same comment on a different website. However, this deviation from the  
government’s proposed construction is not material to the Court’s First Amendment analysis.

1 and human trafficking.” CASE Act § 3(1), (3). The Act’s text also expresses an interest in  
2 “deter[ring] predators from using the Internet to facilitate human trafficking and sexual  
3 exploitation.” *Id.* § 2(6). Plaintiffs do not dispute that these are legitimate government  
4 interests. *Cf., e.g., Doe v. Jindal*, 853 F. Supp. 2d 596, 805 (M.D. La. 2012) (“There can be  
5 no doubt that the state has a wholly legitimate interest in protecting children from sex  
6 offenders online.”).

7 It is not difficult to imagine situations in which having registrants’ Internet identifiers  
8 would advance these interests. For instance, if a registered sex offender used a social  
9 networking site to recruit victims for human trafficking, being able to match the Internet  
10 identifier used to do the recruiting against a database of registered Internet identifiers could  
11 help to identify the perpetrator.<sup>8</sup> *Cf.* Bock Decl. ¶ 10 (describing trafficking case of twin  
12 girls recruited through a social networking site). Likewise, a database of Internet identifiers  
13 could be used to identify the perpetrator of a sex offense – assuming that the person were a  
14 registrant<sup>9</sup> – who used an anonymous Internet account to make contact with his or her  
15 victim. *Cf. id.* ¶ 11 (describing case of a person who raped four women he contacted via  
16 Craigslist, including a teenage victim “whose pimp had been trafficking her”). Although the  
17 government has not presented any real-life examples involving the use of Internet  
18 information in a sex offender registry to prevent or solve a crime,<sup>10</sup> the Court finds that the  
19 challenged provisions could conceivably advance the legitimate purposes of the Act. It now  
20 turns to the question of whether they are narrowly tailored to achieving those purposes.

---

21  
22  
23 <sup>8</sup>This assumes that the re-offending registrant complied with the Internet reporting  
requirements enacted by the CASE Act.

24 <sup>9</sup>Plaintiffs’ unchallenged statistics suggest that “most online predators” –  
25 approximately 96% – “are not registered offenders and have no prior record.” Finkelhor  
Decl. ¶ 18.

26 <sup>10</sup>The government argues that it cannot provide such examples from California  
27 because the challenged provisions have not yet gone into effect. However, neither the  
28 government nor Intervenors responded to Plaintiffs’ observation that data from other  
jurisdictions where Internet registration requirements are in effect could shed light on the  
potential impact of such requirements in California.

1 Defendants and Intervenors assert that *Shurtleff*, 628 F.3d 1217, in which the Tenth  
2 Circuit upheld a reporting requirement in Utah, is persuasive authority that the CASE Act  
3 should survive scrutiny under the First Amendment. In *Shurtleff*, the challenged statute  
4 required a registrant “to provide all ‘Internet identifiers and the addresses [he] uses for  
5 routing or self-identification in Internet communications or postings.’” *Id.* at 1221 (footnote  
6 omitted) (alteration in original) (quoting Utah Code Ann. § 77-27-21.5(14)(i) (West 2008)).  
7 An Internet identifier was defined as “‘any electronic mail, chat, instant messenger, social  
8 networking, or similar name used for Internet communication.’” *Id.* at 1221 n.1 (quoting  
9 Utah Code Ann. § 77–27–21.5(1)(j)). The district court found that the original statutory  
10 scheme violated the First Amendment because it “‘contained no restrictions on how the  
11 [state] could use or disseminate registrants’ Internet information, implicating protected  
12 speech and criminal activity alike.” *Doe v. Shurtleff*, Case No. 1:08-CV-64-TC, 2009 WL  
13 2601458, at \*1 (D. Utah Aug. 20, 2009).

14 The Utah legislature subsequently amended the statute to limit state officials’ use of  
15 the information to “investigating kidnapping and sex-related crimes, and . . . apprehending  
16 offenders. . . .” *Shurtleff*, 628 F.3d at 1221 (internal quotation marks omitted) (quoting Utah  
17 Code Ann. § 77-27-21.5(2) (West Supp. 2010)). The legislature simultaneously amended  
18 the state’s public records act “to designate certain information provided by an offender,  
19 including internet identifiers, as private.”<sup>11</sup> *Id.* (citing Utah Code Ann. § 63G-2-302(1)(m)).  
20 This meant that the information could “only be disclosed in limited circumstances such as  
21 when requested by the subject of the record, or pursuant to a court order or legislative  
22 subpoena,” and could be shared “between different government entities and their agents”  
23 only if the entity receiving the record placed “the same restrictions on disclosure of the  
24 record as the originating entity.” *Id.* at 1221 n.4 (internal quotation marks omitted) (citing  
25 Utah Code Ann. §§ 63G-2-201(5), 63G-2-202, and quoting Utah Code Ann. § 63G-2-206).  
26 The Tenth Circuit “read this language, as did the district court, as only allowing state actors

---

27  
28 <sup>11</sup>The legislature also amended the statute to remove “any requirement that offenders  
disclose their passwords.” *Shurtleff*, 628 F.3d at 1221.

1 to look beyond the anonymity surrounding a username in the course of an investigation after  
2 a new crime has been committed,” and further interpreted the statute “as permitting sharing  
3 only among law-enforcement agencies, not the public at large.” *Id.* at 1225. The court  
4 consequently found no First Amendment problem: “Although this narrow interpretation  
5 may still result in the disclosure of Mr. Doe’s online identifiers to state officials,” the court  
6 reasoned, “such identification will not unnecessarily interfere with his First Amendment  
7 freedom to speak anonymously.” *Id.*

8 In California, sex offender registration statements are not subject to “inspection by the  
9 public or by any person other than a regularly employed peace officer or other law  
10 enforcement officer,” Cal. Penal Code § 290.021, but a law enforcement entity may disclose  
11 registrants’ information to the public “by whatever means the entity deems appropriate,  
12 when necessary to ensure the public safety based upon information available to the entity  
13 concerning that specific person,” *id.* § 290.45(a)(1). With any such disclosure, the entity  
14 must include “a statement that the purpose of the release of information is to allow members  
15 of the public to protect themselves and their children from sex offenders.” *Id.*  
16 § 290.45(a)(2). These California statutes do not contain the safeguards present in the  
17 amended Utah statutes and are closer to the pre-amendment Utah statutes initially found  
18 unconstitutional by the district court in *Doe v. Shurtleff*, Case No. 1:08-CV-64-TC, 2008 WL  
19 4427594 (D. Utah Sept. 25, 2008).

20 They are also similar to a Georgia statute – struck down by the district court in *White*  
21 *v. Baker*, 696 F. Supp. 2d 1289 (N.D. Ga. 2010) – that permitted disclosure of registrants’  
22 Internet information “to law enforcement agencies for law enforcement purposes” and to the  
23 public as “necessary to protect the public” without any other limitations. *Id.* at 1309  
24 (quoting O.C.G.A. § 41-1-12(o)). This Court agrees with the *White* court, which found the  
25 lack of statutory protections on disclosure to be troubling:

26 It is conceivable, if not predictable, that a person in law  
27 enforcement might determine that Internet Identifiers for  
28 offenders ought to be released so that the public can search for  
and monitor communications which an offender intends to be

1 anonymous. That these anonymous communications might well  
2 be on a matter of public policy, political speech, or other  
3 protected speech squarely implicates the First Amendment. . . .  
The prospect that Internet Identifiers, as currently defined, may  
be released to the community has an obvious chilling effect.

4 *Id.* at 1310-11.<sup>12</sup>

5 While the government asserted at oral argument that there has to be “some kind of  
6 nexus” between the use of an Internet identifier and criminal activity before law enforcement  
7 can access information related to a registrant’s Internet identifier, Rep. Tr. at 54:23-55:15,  
8 the Court “cannot simply presume the [government] will act in good faith and adhere to  
9 standards absent from the [statute’s] face.” *Comite*, 657 F.3d at 946-47 (internal quotation  
10 marks, alteration, and citation omitted). Here, Plaintiffs have no guarantee that their  
11 pseudonyms will be safeguarded from public dissemination because neither the CASE Act  
12 nor any other California statute requires the nexus asserted by the government at the hearing.  
13 Their right to speak anonymously will therefore be chilled.

14 This chilling effect is heightened because, unlike in the Utah or Georgia cases, the  
15 disclosure of a registrant’s identity – at least to law enforcement, and potentially to the  
16 public as well – will occur either before he or she speaks or, at maximum, within 24 hours  
17 after speaking and potentially while the speech is ongoing. *Cf. Shurtleff*, 628 F.3d at 1225  
18 (finding that disclosure “would generally occur, if at all, at some time period following  
19 Mr. Doe’s speech and not at the moment he wished to be heard”); *White*, 696 F. Supp. 2d at  
20 1294 (noting that the Georgia statute required registrants to provide updated information  
21 within 72 hours). A contemporaneous disclosure requirement poses a greater burden on  
22 speech than an after-the-fact disclosure requirement because it “connects the speaker to a  
23 particular message directly.” *ACLU v. Heller*, 378 F.3d 979, 991-92 (9th Cir. 2004). When  
24 a California registrant wants to speak online, he or she must use either a previously reported  
25 Internet identifier – in which case the disclosure to law enforcement would have occurred

26 <sup>12</sup>The Georgia statute defined “Internet Identifier” as “E-mail addresses, usernames,  
27 and user passwords,” and further defined “username” as “a string of characters chosen to  
28 uniquely identify an individual who uses a computer or other device with Internet capability  
to gain access to e-mail messages and interactive online forums.” *White*, 696 F. Supp. 2d at  
1295 (quoting O.C.G.A. § 42-1-12(a)(16)(K) & (a)(21.1)).

1 prior to the speech – or a new identifier that must be reported within 24 hours, regardless of  
2 whether any conversation using the identifier has concluded. Because it results in a risk of  
3 more contemporaneous disclosure, this reporting requirement is even more problematic than  
4 the 72-hour reporting requirement found to be unconstitutional in *White*. It likewise creates  
5 a far greater chilling effect on anonymous speech than the statute upheld in *Shurtleff*,  
6 especially when combined with the lack of statutory protections on the information’s  
7 disclosure to other law enforcement agencies and the public.

8 Registrants’ speech may also be chilled because failure to comply with sex offender  
9 registration requirements, including the Internet provisions, is punishable by up to three  
10 years in state prison. Cal. Penal Code § 290.018(a)-(c). This potential punishment may  
11 deter registrants from speaking at all if they are uncertain about whether they have to report a  
12 particular Internet identifier to law enforcement and, if so, whether they will be able to file  
13 any such report within the required 24-hour period. *See NAACP v. Button*, 371 U.S. 415,  
14 433 (1963) (“The threat of sanctions may deter the[] exercise [of First Amendment rights]  
15 almost as potently as the actual application of sanctions.”). The uncertainty surrounding  
16 what registrants must report – and the resultant potential chilling effect – is greater in this  
17 case because the Court’s interpretation of the Act is not definitive guidance to registrants  
18 about what they must report. While the Court construed the Act’s provisions for purposes of  
19 determining whether they violate the First Amendment, this Court’s interpretation is not  
20 binding on state courts, where the registrants would face prosecution for failure to register.  
21 *See Cal. Teachers Ass’n v. State Bd. of Educ.*, 271 F.3d 1141, 1146 (9th Cir. 2001) (“[I]t is  
22 solely within the province of the state courts to authoritatively construe state legislation.”).

23 The CASE Act provisions’ chilling effect might be justifiable if the provisions were  
24 narrowly tailored, but – at least at this stage of the proceedings – the government has not  
25 persuaded the Court that they are. For the reasons discussed below, the Court finds that the  
26 provisions apply both to more speakers and more speech than is necessary to advance the  
27 government’s legitimate purposes.

28

1 First, the Court is not persuaded that burdening the anonymous speech rights of all  
2 75,000 registered sex offenders is narrowly tailored to the government’s interest in fighting  
3 online sex offenses. The government already classifies registrants using a risk-assessment  
4 tool known as Static-99. Using this instrument, the State has classified the majority of  
5 registrants released on parole after 2005 as posing a “low” or “moderate-low” risk of  
6 re-offending. Abbott Decl. ¶ 9. The government has not sufficiently explained why these  
7 individuals ought to be treated differently from non-registrants who are not required to report  
8 Internet-identifying information to authorities. This fact is not altered by Intervenors’  
9 reliance on Plaintiffs’ data that “[p]edophiles who molest boys and rapists of adult women  
10 have recidivism rates of 52% and 39% respectively,” or that the overall average recidivism  
11 rate for registrants in all risk categories is between 14% and 20%. *Id.* ¶ 15. The issue is not  
12 whether registrants recidivate, which Plaintiffs do not dispute. Instead, the problem is that  
13 the government has not explained why the collection of Internet-identifying information  
14 from registrants who present a low or moderately low risk of re-offending, and a potentially  
15 even lower risk of re-offending online,<sup>13</sup> is narrowly tailored to the Act’s purposes. Based  
16 on the State’s own existing risk assessments, the uniform application of the CASE Act  
17 appears overbroad.<sup>14</sup>

18 At oral argument, the government asserted that Static-99 cannot be used to limit the  
19 number of registrants who must report Internet-identifying information because the CASE  
20 Act’s “Internet identifier registration requirements serve[] a different purpose” than  
21 Static-99’s purpose of “estimat[ing] the risk that a person might pose when they are released

---

22  
23 <sup>13</sup>No party or intervenor presented any evidence concerning the rate by which  
24 registered sex offenders re-offend using the Internet. The only statistical evidence presented  
25 on the prevalence of Internet use in the commission of sex offenses was from a national study  
of 2006 arrests, which indicated that only approximately 1% of sex offenses against children  
involved the Internet or other technology. Finkelhor Decl. ¶ 12.

26 <sup>14</sup>Even if the Act were applied only to the registrants deemed to pose a higher risk by  
27 the State’s Static-99 tool, this, too, could still be insufficiently tailored because it considers  
28 only the risk of re-offending, not the risk of committing a sex offense online – which is the  
CASE Act’s stated focus. However, the challenged provisions currently apply to all  
registrants, regardless of risk, and the Court therefore need not and does not decide this  
question.

1 to the community.” Rep. Tr. at 76:19-77:1. The purpose of the CASE Act’s new  
2 registration requirements is, according to the government, “to be able to find somebody if we  
3 need to.” *Id.* at 77:1-2. However, the government has not explained how being able to find  
4 all registered sex offenders using Internet identifiers – regardless of the registrants’ risk of  
5 re-offending as determined by the government’s own assessment tool – is narrowly tailored  
6 to achieving the Act’s legitimate interest in combating online sex offenses or human  
7 trafficking.

8 In addition, even as to registrants who may legitimately be required to register  
9 Internet-identifying provisions based on their risk of recidivism, the challenged provisions  
10 appear to extend to too much speech. When asked at oral argument what kinds of  
11 communications it would be “most helpful for law enforcement to be able to monitor,” the  
12 government referred to *White v. Baker*, stating that the court there said that “Internet chatting  
13 and social networks and chat rooms . . . were the most helpful, that mostly involved the  
14 exploitation of children.” Rep. Tr. at 75:1-8. Indeed, the *White* court found that online  
15 solicitation for sexual exploitation “generally do[es] not occur in communications that are  
16 posted publicly on sites dedicated to discussion of public, political, and social issues.” 696  
17 F. Supp. 2d at 1310. The government has not shown the utility of requiring registration of  
18 Internet identifiers used for this type of public commentary.

19 Nonetheless, the CASE Act provisions extend to all such websites, and registrants are  
20 likely to be chilled from engaging in legitimate public, political, and civic communications  
21 for fear of losing their anonymity. As a Nebraska district court forcefully stated, a  
22 requirement that sex offenders report to the government all communications on blogs and  
23 websites “puts a stake through the heart of the First Amendment’s protection of anonymity  
24 [and] surely deters faint-hearted offenders from expressing themselves on matters of public  
25 concern.” *Doe v. Nebraska*, Case No. 8:09CV456, 2012 WL 4923131, at \*28 (D. Neb.  
26 Oct. 17, 2012); *see also White*, 696 F. Supp. 2d at 1310 (concluding that a requirement was  
27 overbroad because it included communications that did not “reasonably present a vehicle by  
28 which a sex offender can entice a child to have illicit sex”). This Court agrees. Applying the

1 registration requirements to all Internet forums, even those types that have not been shown to  
2 pose any reasonable risk of leading to an online sex offense or human trafficking, creates a  
3 significant chilling effect on Plaintiffs' protected speech.<sup>15</sup>

4 In short, at this preliminary stage of the proceedings, the government, with the  
5 Intervenors' support, has failed to show that the CASE Act's reporting requirements are  
6 narrowly tailored to serve its legitimate interests. The challenged provisions have some  
7 nexus with the government's legitimate purpose of combating online sex offenses and  
8 human trafficking, but "[t]he Government may not regulate expression in such a manner that  
9 a substantial portion of the burden on speech does not serve to advance its goals." *Ward*,  
10 491 U.S. at 799. On the current record, the Court concludes that Plaintiffs are likely to  
11 establish that the challenged provisions, when combined with the lack of protections on the  
12 information's disclosure and the serious penalty registrants face if they fail to comply with  
13 the reporting requirements, create too great a chilling effect to pass constitutional muster.  
14 While the government may be able to demonstrate narrow tailoring in subsequent  
15 proceedings, it has not done so here. Accordingly, the Court concludes that Plaintiffs are  
16 likely to succeed on their First Amendment free speech claim.

#### 17

#### 18 **B. Remaining Preliminary Injunction Factors**

19 To warrant injunctive relief, Plaintiffs must also show that they are likely to suffer  
20 irreparable harm in the absence of an injunction and demonstrate that the public interest and  
21 balance of equities weigh in their favor. As discussed below, the Court finds that Plaintiffs  
22 have sufficiently established all of these factors.

23 First, neither the government nor Intervenors dispute that Plaintiffs are likely to suffer  
24 irreparable harm in the absence of an injunction. Indeed, the Supreme Court long ago

---

25  
26 <sup>15</sup>The Court recognizes that, like the challenged provisions here, the Utah statutes  
27 upheld by the Tenth Circuit in *Shurtleff* applied broadly to all Internet forums and all  
28 registered sex offenders. However, as discussed above, the chilling effect of the Utah statute  
was diminished, if not eliminated, by the statutory restrictions on disclosure and the lack of a  
relatively contemporaneous reporting requirement.

1 explained that “[t]he loss of First Amendment freedoms, for even minimal periods of time,  
2 unquestionably constitutes irreparable injury.” *Elrod v. Burns*, 427 U.S. 347, 373 (1976).

3 Second, the Ninth Circuit has “consistently recognized the ‘significant public  
4 interest’ in upholding free speech principles,” *Klein v. City of San Clemente*, 584 F.3d 1196,  
5 1208 (9th Cir. 2009), and has further observed that “it is always in the public interest to  
6 prevent the violation of a party’s constitutional rights,” *Melendres v. Arpaio*, 695 F.3d 990,  
7 1002 (9th Cir. 2012) (internal quotation marks and citation omitted).

8 Third, based on the present record, the government has not demonstrated that the  
9 CASE Act’s impact on public safety is sufficient to overcome the interest – both to Plaintiffs  
10 and to the public – in avoiding infringement of Plaintiffs’ First Amendment rights. As the  
11 Supreme Court has explained, “[t]he prospect of crime . . . by itself does not justify laws  
12 suppressing protected speech,” nor may the government “prohibit speech because it increases  
13 the chance an unlawful act will be committed at some indefinite future time.” *Ashcroft v.*  
14 *Free Speech Coal.*, 535 U.S. 234, 245, 253 (2002) (internal quotation marks and citation  
15 omitted). In this case, the government has not provided any evidence regarding the extent to  
16 which the public safety might be enhanced if the additional registration requirements went  
17 into effect. Plaintiffs’ evidence – as yet undisputed – indicates that only 1% of arrests for sex  
18 crimes against children are for crimes facilitated by technology, Finkelhor Decl. ¶ 12, and  
19 that registered sex offenders are involved in only 4% of these arrests, *id.* ¶ 18. While the  
20 Court does not minimize the significance of any single crime, the record at this stage of the  
21 proceedings suggests that the potential usefulness of the Internet registration information is  
22 limited to a very small portion of the universe of sex offenses and online sex offenses.  
23 Moreover, enjoining the Internet registration requirements enacted by the CASE Act would  
24 not prevent the government from investigating online sex offenses, as it could still employ  
25 other mechanisms to do so. *See, e.g., Doe v. Shurtleff*, 2008 WL 4427594, at \*9 (noting that,  
26 even in the absence of an Internet registration requirement, “investigators of internet crime  
27 already have tools to unmask anonymous internet suspects, such as investigative  
28 subpoenas”). Against the government’s weak showing of the utility of registrants’ Internet

1 information if the Act is not enjoined, the Court must weigh the likely and substantial  
2 chilling of Plaintiffs’ First Amendment rights discussed above. Having done so, the Court  
3 concludes that both the balance of equities and the public interest weigh in favor of granting  
4 injunctive relief.

5  
6 **C. Application of Injunction to Local Law Enforcement**

7 Finally, the Court must address whether any injunctive relief binds local law  
8 enforcement officials in California or only the Attorney General. The parties agreed that  
9 local law enforcement officials would not enforce the challenged provisions during the  
10 pendency of the temporary restraining order, but the government now argues that an  
11 injunction against the Attorney General cannot bind local law enforcement agencies or  
12 personnel. For support, the government cites a single California appellate case from seventy  
13 years ago for the proposition that “the California Constitution does not contemplate absolute  
14 control and direction of sheriffs” by the Attorney General. Gov’t Opp’n at 9 (citing *People*  
15 *v. Brophy*, 49 Cal. App. 2d 15, 28 (1942)).

16 The government’s argument is beside the point. Federal Rule of Civil Procedure  
17 65(d)(2) provides that an injunction will bind the parties, as well as “the parties’ officers,  
18 agents, servants, employees, and attorneys,” and “[o]ther persons who are in active concert or  
19 participation with” these individuals. Even if the Attorney General does not have absolute  
20 control and direction over local law enforcement, it cannot be disputed that, as to the  
21 collection of sex offender registration data, local law enforcement at least acts “in active  
22 concert or participation with” the Attorney General, if not as her agent. *See, e.g.*, Cal. Penal  
23 Code § 290.015(b) (requiring local law enforcement agencies to forward registrants’  
24 information to the Department of Justice<sup>16</sup> within three days of registration); Schweig Decl.  
25 ¶ 3 (describing the collection of sex offender registration data as a “collaborative effort”  
26

27  
28 <sup>16</sup>“The Attorney General is head of the Department of Justice.” Cal. Gov’t Code  
§ 12510.

1 involving, among others, the California Department of Justice and local law enforcement  
2 agencies).

3       However, Federal Rule of Civil Procedure 65(d)(2) also provides that an injunction  
4 only binds persons “who receive actual notice of it by personal service or otherwise.” To  
5 ensure that all local law enforcement officials who are responsible for collecting registered  
6 sex offenders’ information are bound by this order, the Court will order the Attorney General  
7 to provide actual notice to all such officials. This requirement does not preclude the parties  
8 from further meeting and conferring to attempt to reach agreement that local law  
9 enforcement will not enforce the enjoined provisions as long as the Court’s order granting  
10 preliminary injunctive relief remains in effect.

11  
12 **IV. CONCLUSION**

13       The Court does not lightly take the step of enjoining a state statute, even on a  
14 preliminary basis. However, just as the Court is mindful that a strong majority of California  
15 voters approved Proposition 35 and that the government has a legitimate interest in  
16 protecting individuals from online sex offenses and human trafficking, it is equally mindful  
17 that “[a]nonymity is a shield from the tyranny of the majority,” and that Plaintiffs enjoy no  
18 lesser right to anonymous speech simply because they are “unpopular.” *McIntyre v. Ohio*  
19 *Elections Comm'n*, 514 U.S. 334, 357 (1995). The record before the Court does not establish  
20 that the Internet registration requirements enacted by the CASE Act are narrowly tailored to  
21 the Act’s legitimate purpose of combating online sex offenses and human trafficking. While  
22 the government may be able to make the necessary showing at a later stage of these  
23 proceedings, it has not yet done so, and the Court therefore concludes that Plaintiffs have  
24 demonstrated a likelihood of success on the merits of their First Amendment free speech  
25 claim.

26 //

27 //

28 //

1           Accordingly, with good cause appearing for the reasons stated in this order, Plaintiffs'  
2 motion for a preliminary injunction is GRANTED. IT IS HEREBY ORDERED that:

3           1. Defendant Kamala Harris and her officers, agents, servants, employees, and  
4 attorneys, and those persons in active concert or participation with her, are enjoined from  
5 implementing or enforcing California Penal Code sections 290.014(b) and 290.015(a)(4)-(6),  
6 as enacted by the CASE Act.<sup>17</sup>

7           2. Defendant Harris shall provide, by personal service or otherwise, actual notice of  
8 this order to all law enforcement personnel who are responsible for implementing or  
9 enforcing the enjoined statutes or from otherwise collecting registered sex offenders'  
10 information. The government shall file a declaration establishing proof of such notice on or  
11 before **January 28, 2013**. Alternatively, the parties may file on or before that date a  
12 stipulation and proposed order that local law enforcement will not enforce the enjoined  
13 provisions even in the absence of receiving actual notice.

14  
15 **IT IS SO ORDERED.**

16  
17 Dated: 01/11/13



THELTON E. HENDERSON, JUDGE  
UNITED STATES DISTRICT COURT

18  
19  
20  
21  
22  
23  
24  
25  
26           <sup>17</sup>A careful reader may observe that the Court has omitted the phrase, “or from  
27 otherwise requiring registrants to provide identifying information about their online speech to  
28 the government,” from the temporary restraining order. Nov. 7, 2012 Order at 3. This  
should not be interpreted as the Court’s permission to attempt an end run around the  
preliminary injunction entered today. The Court removed this language out of an abundance  
of caution that the scope of its injunction not reach too broadly.