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 Intervenors' Req. for Judicial Notice at 1.[1] Plaintiffs John Doe, Jack Roe,[2] and the non-profit organization California Reform Sex Offender Laws filed this action on behalf of present and future

[1]The Court GRANTS Intervenors' unopposed request for judicial notice in its entirety.

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

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

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

> (4) A list of any and all Internet identifiers established or used by the person.
>
> (5) A list of any and all Internet service providers used by the person.
>
> (6) A statement in writing, signed by the person, acknowledging that the person is required to register and update the information in paragraphs (4) and (5), as required by this chapter.

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

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

[3]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.

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

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

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

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

On November 14, 2012, the Court entered a stipulation and order deleting the application of the TRO to "all California state and local law enforcement officers," but providing that "the California Department of Justice and local law enforcement will not require registrants to submit the information covered by the TRO so long as the TRO remains 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

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

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

II. LEGAL STANDARD

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

III. DISCUSSION

A. Likelihood of Success on the Merits

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

1. First Amendment Legal Principles

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

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

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

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

[4]That the challenged provisions were enacted by voter initiative does not alter the constitutional analysis. "The voters may no more violate the United States Constitution by 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).

protected speech or expression." *Broadrick v. Oklahoma*, 413 U.S. 601, 612 (1973). However, "the mere fact that one can conceive of some impermissible applications of a statute is not sufficient to render it susceptible to an overbreadth challenge." *Members of the City Council of L.A. v. Taxpayers for Vincent*, 466 U.S. 789, 800 (1984).

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

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

2. Construing the Statute

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

a. "Internet service provider"

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

[5]The government and Intervenors also suggest that, in construing the reporting requirements, the Court may look to the federal standards for state sex offender registry and notification systems developed under the Sex Offender Registration and Notification Act ("SORNA"). *See* 42 U.S.C. § 16915a(a) (providing for collection of "those Internet identifiers the sex offender uses or will use of any type that the Attorney General determines to be appropriate"); Nat'l Guidelines for Sex Offender Registration and Notification, 73 Fed. 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 Intervenors to be supported by the statutes' plain language. Neither the government nor Intervenors argue that SORNA affects the Court's analysis on any other issue.

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

b. "Internet identifier"

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

[6]Plaintiffs expressed fear that law enforcement may subsequently decide to require 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.

reasonable to interpret the Act to "count[] once you actually use that account to post something").[7]

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

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

3. Narrow Tailoring

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

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

[7]The government suggested that blog usernames need not be reported as long as the blog did not permit interactive comments. Rep. Tr. at 63:17-19. The Court declines to 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.

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

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

---

[8]This assumes that the re-offending registrant complied with the Internet reporting requirements enacted by the CASE Act.

[9]Plaintiffs' unchallenged statistics suggest that "most online predators" – approximately 96% – "are not registered offenders and have no prior record." Finkelhor Decl. ¶ 18.

[10]The government argues that it cannot provide such examples from California because the challenged provisions have not yet gone into effect. However, neither the 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.

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

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

[11]The legislature also amended the statute to remove "any requirement that offenders disclose their passwords." *Shurtleff*, 628 F.3d at 1221.

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

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

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

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

> anonymous. That these anonymous communications might well be on a matter of public policy, political speech, or other 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.

Id. at 1310-11.[12]

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

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

[12]The Georgia statute defined "Internet Identifier" as "E-mail addresses, usernames, and user passwords," and further defined "username" as "a string of characters chosen to 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)).

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

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

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

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

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

---

[13]No party or intervenor presented any evidence concerning the rate by which registered sex offenders re-offend using the Internet. The only statistical evidence presented 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.

[14]Even if the Act were applied only to the registrants deemed to pose a higher risk by the State's Static-99 tool, this, too, could still be insufficiently tailored because it considers 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.

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

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

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

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

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

B. Remaining Preliminary Injunction Factors

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

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

[15]The Court recognizes that, like the challenged provisions here, the Utah statutes upheld by the Tenth Circuit in *Shurtleff* applied broadly to all Internet forums and all 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.

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

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

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

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

C. Application of Injunction to Local Law Enforcement

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

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

[16]"The Attorney General is head of the Department of Justice." Cal. Gov't Code § 12510.

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

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

IV. CONCLUSION

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

//

//

//

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

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

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

IT IS SO ORDERED.

Dated: 01/11/13

THELTON E. HENDERSON, JUDGE
UNITED STATES DISTRICT COURT

[17]A careful reader may observe that the Court has omitted the phrase, "or from otherwise requiring registrants to provide identifying information about their online speech to 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.