Case Nos. 13-15263, 13-15267

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

JOHN DOE, *et al*.,

PLAINTIFFS-APPELLEES,

v.

DAPHNE PHUNG, *et al*.,

INTERVENORS-APPELLANTS,

and

KAMALA D. HARRIS, Attorney General of the State of California,

DEFENDANT-APPELLANT.

On Appeal from the United States District Court
for the Northern District of California
No. 3:12-cv-05713-THE
The Honorable Thelton E Henderson, Judge

APPELLEES' OPENING BRIEF

MICHAEL T. RISHER (SBN 191627)
mrisher@aclunc.org
LINDA LYE (SBN 215584)
llye@aclunc.org
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION OF
NORTHERN CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493
Facsimile: (415) 255-8437

HANNI FAKHOURY (SBN 252629)
hanni@eff.org
LEE TIEN (SBN 148216)
tien@eff.org
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Counsel for Plaintiffs-Appellees JOHN DOE, et al.

CORPORATE DISCLOSURE STATEMENT

Pursuant to F.R.A.P. 26.1, I certify that Plaintiff-Appellee California Reform Sex Offender Laws does not have a parent corporation and that no publicly held corporation owns 10% or more of any stake or stock in it.

DATED: May 8, 2013

By: */s/ Michael T. Risher*
Michael T. Risher

Counsel for Plaintiffs-Appellees JOHN DOE, et al.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

State Cases

State Statutes

Constitutional Provisions

Legislative Materials

Other Authorities

INTRODUCTION AND ISSUES PRESENTED

The CASE Act requires all 75,000 Californians who have ever been convicted of a sex-related offense to provide the police with information about the Internet service providers ("ISPs") and Internet identifiers that they use to engage in online speech, including but not limited to anonymous online speech. This requirement applies to people convicted decades ago of misdemeanor offenses that had nothing to do with minors or the Internet, to individuals whom the State has determined pose a low risk of reoffending, and to Internet identifiers that cannot be used for improper purposes, such as identifiers used to post comments on a newspaper's website. Violations can result in years in prison.

1. Did the District Court err in holding these requirements violate the First Amendment because the government failed to meet its burden to show that they are narrowly tailored to achieve the State's interests?
2. Are the Act's definitions of ISP and Internet identifier unconstitutionally vague?
3. Did the District Court abuse its discretion in enjoining these unconstitutional provisions?

JURISDICTION

Plaintiffs agree with the government's statement of jurisdiction.

STATEMENT OF FACTS

A. The California Sex Offender Registry

California law requires every person convicted of a variety of offenses since 1944 to register as a sex offender for the rest of his life. *See* Cal. Penal Code § 290(b) (West 2012).[1] Registration is mandatory upon conviction for any of the more than 150 offenses enumerated in the statute. *See* § 290(c).[2] One of these offenses, misdemeanor indecent exposure, § 314, can encompass what this Court has described as "the conduct of pranksters with poor judgment," as well as "nude dancing at bars," exposing oneself to an undercover officer who seemed to want to engage in sex at a "cruising place," or exposing oneself during an incident of road rage. *Nunez v. Holder,* 594 F.3d 1124, 1133-38 (9th Cir. 2010) (citations omitted). In addition, registration is required upon conviction of any other offense that the court determines was committed "for purposes of sexual gratification." § 290.006; *see also* § 290.008 (juvenile registration requirements).

Registration is automatic, retroactive, mandatory, lifelong, and not subject to plea bargaining. *See People v. Kennedy*, 194 Cal. App. 4th 1484, 1491 (2011); *see also* §§ 290.007, 290.5. California has more registrants than any other state:

[1] All statutory references are to the California Penal Code unless otherwise noted.
[2] The Attorney General's website lists more than 150 distinct registerable offenses. *See* http://meganslaw.ca.gov/registration/offenses.htm (last visited May 8, 2013).

approximately 75,000, not including persons who are in custody or have been deported. *See* ER0002 n.3, 0486.

B. Newly Enacted Requirements Of CASE Act

Although California law has long required that registrants disclose basic directory information that is already widely available to the police and others, such as home address and license plate numbers, the CASE Act ("Act") now additionally requires registrants to provide the police with information about their online speech, information that the government would normally not be able to access at all, at least not without a search warrant: "[a] list of any and all Internet identifiers established or used by the person" and "[a] list of any and all Internet service providers used by the person." *See* Proposition 35, Californians Against Sexual Exploitation Act § 12, Cal. Penal Code § 290.015(a)(4), (5)). The Act defines these terms as follows:

> "Internet service provider" means 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. An Internet service provider does not include a 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.
>
> "Internet identifier" means 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.

Act § 13, § 290.024(a), (b).

Appellants have never been able to explain just what these definitions mean. In fact, even though the District Court specifically ordered all parties to address whether the Act applies to a number of specific online communications, ER0110-11, neither the government nor intervenors did so, although they did agree that registrants must turn over any identifiers that they use to post comments on websites such as the *New York Times* and Amazon.com, or that they use to maintain an interactive blog. ER0084-85; *see also* Intervenors' Br. 8, 22 (must disclose CNN.com username). They also agree that registrants would have to turn over the names of any Internet cafés that they used to access the Internet, if they had some sort of account with that café. ER0086, 0095.

Every registrant must provide this information within 24 hours after he "adds or changes his or her account with an Internet service provider or adds or changes an Internet identifier." Act § 11, § 290.014(b). In addition, registrants must provide this same information annually. *See* § 290.012(a), 290.015(a)(4), (5). "[F]orgetting … is not a defense," and a registrant who fails to register "through ordinary negligence" may be convicted and sentenced to prison. *Gonzalez v. Duncan*, 551 F.3d 875, 886 n.10 (9th Cir. 2008). Thus, a registrant who appears for his annual update and fails to list all the Internet identifiers he had previously submitted, or who lists an identifier that the police did not previously know about, could be arrested, prosecuted, and convicted.

If the individual is required to register because of a prior misdemeanor conviction and has no prior convictions for violating registration requirements, then any registration violation is a misdemeanor with a one-year maximum sentence; otherwise, a violation is a felony punishable by up to three years in state prison, a sentence that may be dramatically increased if the registrant has prior felony convictions. *See id.* at 877-79, 886; *see also* § 290.018(a)-(c); *In re Coley,* 55 Cal.4th 524 (2012) (upholding life sentence for violation).

C. The Internet Is A Forum For Expression And Association

Plaintiffs submitted an expert declaration from Professor David Post describing the Internet, how it is used, and the likely effect that the Act would have on online speech. ER0499-0520. As Professor Post explains, roughly half of Americans regularly obtain news online, including a growing number who obtain news from social networks. ER0504. Approximately 39% have engaged in some form of online civic or political activity beyond simply reading about political issues. *Id*. And millions of Americans use the Internet to work, seek work, or further their education. ER0504-05.

Americans visit millions of Internet sites that are covered by the Act because they require or permit the creation of user names, screen names, or similar identifiers to allow users to engage in various expressive activities. Many millions of web sites incorporate some form of "social networking" functionality, *e.g.*, the

ability to create a profile and post some form of content. ER0509-10. Just one of these, Facebook, now has more than one billion users worldwide, and Twitter users generate hundreds of millions of "tweets" per day. ER0503. In a typical month the average Internet user visits well over 100 distinct web sites, and many Internet users may visit far more. *Id*. Using these sites and accounts, Internet users can and do post feedback on both recently-purchased items and their sellers, collaboratively create and maintain online encyclopedia and documents, discuss local, national, and international events, and advertise for and otherwise conduct their businesses. ER0503-05, 0509-10. Even construed narrowly, the Act requires that registrants report the screen names that they use for all of these purposes. ER0508-11.

Internet users also rely on a large number of service providers to access the Internet. In particular, any person who travels is likely to use one or more new providers, such as a local cellular network or a wireless network at a hotel or café, at each destination. ER0512-14. Because these all fall within the Act's idiosyncratic definition of "ISP," even if construed narrowly, a registrant who opens an account with any such service would have to report it under the Act within 24 hours. ER0516.

D. Plaintiffs Engage In Protected Online Speech

Plaintiffs and other registrants use the Internet as do other Americans: to conduct business, communicate with friends and associates, engage in self-

expression, comment on news articles, and participate in groups with political or religious purposes. ER0488, 0552-54, 0558-59. They have and create multiple user names and similar identifiers for these activities. ER0553.

Plaintiffs John Doe and Jack Roe were both convicted of sex-related crimes more than two decades ago and have not been in trouble since then. Their crimes did not involve the Internet or a computer. ER0552, 0558.

Doe, who is 75 years old, is an activist on sex-offender issues, working with victims groups, treatment professionals, and offenders. ER0558. For years he operated websites that provided sex offenders with information and an anonymous online forum about registration requirements and recovery resources. Anonymity was key to the online discussions so that offenders would feel free to express themselves openly. ER0558-59. The Act will interfere with his ability to provide offenders with a forum to communicate with each other about sensitive subjects such as their recovery or registration requirements, because their frank discussions are made possible only by their anonymity. *Id*. In addition, the Act's burdensome reporting requirements will deter his own online speech. *Id*.

Plaintiff Roe runs an Internet-based business for which he must routinely use websites that require usernames. ER0552-53. He also anonymously maintains a blog that discusses matters of public concern; users can also comment anonymously on the blog. ER0553. Anonymity is essential to that blog because

it protects him from retaliation from those he criticizes. *Id.* Roe also comments regularly on online news articles; he does so anonymously to avoid any consequences to his business from his comments on controversial topics. ER0554.

When California first made registrant information available to the public, Roe's neighbors harassed him and his business competitors destroyed his business by publicizing his status. ER0554-55. To avoid having something similar reoccur, Roe would stop engaging in online speech if he were subject to the Act. ER0555. In fact, he has left the state because of the new law, but will return if it is held unenforceable. ER0550.

Roe's experience of retaliation is not unique. Many registrants have lost their jobs or homes when information about their offender status was publicized by law enforcement. ER0363-64.

Plaintiff California Reform Sex Offender Laws ("California Reform") is a non-profit organization that protects the rights of registrants, with some 350 members who are California registrants. ER0522. It is committed to the principles that no sexual abuse is ever acceptable, but that sex offense laws and policies should be based on sound research, not fear and animus. *Id*. California Reform maintains a website to inform its members and the public about legal and policy issues affecting registrants for the purpose of encouraging political and

social change on these issues and provides a discussion forum that allows anonymous commentary on issues affecting registrants. ER0523-24. Registrants would be chilled from commenting on this website if they were required to reveal their identities to the police; the CASE Act would thus interfere with California Reform's ability to provide a forum for registrants to express their views. ER0523-26.

Comments on the site before the November election at which the Act was adopted showed that registrants were worried that they did not understand what information the Act would require them to provide and that they would be afraid to post on the website if they had to provide information that would allow the police to connect them to their comments there. ER0524-25, 0542-47.

E. California Can And In Other Contexts Does Evaluate The Risk That Individual Registrants Will Re-Offend

Plaintiffs submitted evidence from four experts on sex crimes, sex offenders, and recidivism: Dr. Karl Hanson, a senior public-safety researcher in the Canadian government; ER0370-0414; Professor David Finkelhor, the director of the Crimes Against Children Research Center at the University of New Hampshire, ER0415-80; and two California licensed clinical psychologists who treat sex offenders, Dr. Brian Abbott, ER0481-98, and Dr. Charlene Steen, ER0362-69. This evidence, which Appellants did not contest, demonstrated that California could,

with tools it already uses, distinguish between those registrants who pose a real risk of using the Internet to commit a crime and those who do not.

1. Very Few Sex Crimes Involve The Internet, Strangers, Or Registrants

Ninety percent of sex offenses against children are committed by family members and acquaintances, not strangers, as are eighty percent of sex crimes against older victims. ER0488. Arrests for *all* technology-facilitated sex crimes against minors – including those committed by acquaintances or family members and those involving non-Internet technology – constitute only about 1% of all arrests for sex crimes against children. ER0420. Of that 1%, nearly half (46%) were for possession of child pornography. ER0423.

Registrants constitute only a small percentage of those who commit technology-facilitated crimes against children: only 4% of persons arrested for technology-facilitated crimes against youth victims were registered sex offenders, and only 2% of those arrested for soliciting undercover investigators were registered sex offenders. ER0422. Registrants primarily use the Internet for the same purposes that other people do. ER0488.

Online targeting of children is decreasing, as are sex crimes against children in general. ER0421-22. Studies show a 50% decline between 2000 and 2010 in sexual solicitation of youth on the Internet. ER0421.

2. Recidivism Rates Vary In Predictable Ways

Recidivism rates are not uniform across all sex offenders. Rather, the risk of re-offending varies based on well-known factors and can be reliably predicted by widely used risk assessment tools such as the Static-99, which classify offenders into varying risk levels. ER0371, 0375-76. In other contexts, California uses these very tools to distinguish between offenders who pose a high risk to the public and those who do not. For example, California law mandates the use of the Static-99 to determine which offenders require a high level of supervision and which do not. *See* § 290.04(b)(1); *see also* §§ 290.04-290.07, 1203(e), (f), 3008; ER0376.

Most felony sex offenders sentenced to prison and released on parole in California are classified as posing a low or moderate-low risk of re-offending under Static-99 (scores 0-3). ER0487. Less than 10% are classified as high risk. *Id*.

Most sex offenders do not re-offend after they are released. ER0377-78, 0488-89. The longer offenders remain offense-free in the community, the less likely they are to re-offend sexually. ER0373-74, 0377-81, 0489-90. On average, the likelihood of re-offending drops by 50% every five years that an offender remains in the community without a new arrest for a sex offense. ER0378-79. Eventually, persons convicted of sex offenses who remain arrest-free are *less likely* to re-offend than a non-sexual offender is to commit an "out of the blue" sexual

offence. ER378-79. At release, offenders who are classified as "low risk" pose a smaller risk of recidivism than do individuals who have never been arrested for a sex-related offense but have been arrested. ER0379. The same is true for medium-risk offenders after 10 to 14 years in the community without committing a sex offense. ER0379-80. High-risk offenders after 17 years without a new arrest for a sex-related offense pose no more of a risk than individuals who have never been arrested for a sex-related offense but have been arrested. ER0381. Ex-offenders who remain free of any arrests following their release should present an even lower risk. ER0381-82. Post-release factors such as cooperation with supervision or treatment can dramatically reduce recidivism, and monitoring these factors can be highly predictive. ER0377-78, 0381-82, 0490.

Because it is possible to distinguish sexual offenders who present a lifelong threat from those who do not, there is a point at which "resources spent tracking and supervising low-risk sexual offenders [should be] re-directed toward the management of high-risk sexual offenders, crime prevention, and victim services." ER0382.

F. The Use And Release Of Information From The Section 290 Registry

California's statutory scheme authorizes disclosure of registry information under a broad array of circumstances; and the evidentiary record affirmatively shows that law enforcement routinely discloses registrant information to the public

without any evidence the registrant has recently engaged in or is likely to engage in criminal conduct.

The statute requires the Department of Justice to "[p]rovide law enforcement agencies with full Internet access to all sex offender data," without restriction. § 290.022(4). Those agencies then may "provide information to the public about a [registrant] by whatever means the entity deems appropriate, when necessary to ensure the public safety," "[n]otwithstanding any other provision of law." § 290.45; *cf.* § 290.021 (restricting public access "except as otherwise provided by law"). The statute does not specify when disclosure is or is not "necessary to ensure the public safety," but case law and the evidence in this case show that the statute puts few real limits on disclosure. Even under a previous version of the statute that required police have reasonable suspicion before releasing information to the public and made unauthorized disclosure a crime, the police could disclose information to allow any "parent or other concerned member of the public to learn" about registrants "in the general area." *Fredenburg v. City of Fremont,* 119 Cal.App.4th 408, 421, 441 (2004). Since then, the legislature has twice weakened any protections against dissemination. First, it eliminated the requirement that police have reasonable suspicion before releasing information. *See* 2005 Cal. Legis. Serv. Ch. 722 (A.B. 1323). Then it eliminated the penalties for disclosure of registry information: although the statute originally made it a misdemeanor to

"copy, distribute, disclose, or receive" any information from the Department's sex offender records "except as authorized by law," 1996 Cal. Legis. Serv. Ch. 908 § 3 (AB 1562), a 2005 amendment to § 290.4 removed these prohibitions against disclosure. *See* 2005 Cal. Legis. Serv. Ch. 722 § 5 (A.B. 1323); *Mendoza v. ADP Screening and Selection Servs.,* 182 Cal.App.4th 1644, 1655-1658 (2010) (recounting legislative history).[3]

The evidence in this case confirms that California law enforcement agencies access and disseminate registry data to the public even when no crime has been committed or is being investigated. A 2009 survey from the California State Sex Offender Management Board ("CASOMB")[4] found that 39% of responding law-enforcement agencies had "proactively" supplied information under § 290.45 to the community by handing out flyers and other similar means, without any reason to think that a crime had occurred, sometimes with serious consequences to the registrant. *See* ER0363-364; *see* SER014, 021-22. Other evidence confirms this. *See* ER0141 (state's website: police may "notify their communities about the

[3] Similarly, a related statute authorizes use of information about registrants contained on the state's "Megan's Law" website "only to protect a person at risk," § 290.46, but California courts have refused to interpret this provision to mean that information can only be used where there is "a specific identifiable person who is in fact at risk." *Cross v. Cooper,* 197 Cal.App.4th 357, 390-91 (2011) (allowing disclosure because people moving to neighborhood "might" have children).

[4] CASOMB is the state board charged with reducing sexual crime and managing registrants. *See* § 9002; ER0485.

presence of designated" registrants); ER0145 (notifications because a registrant has "tak[en] up residence in the" jurisdiction); Gov't Br. 9 (police may disseminate information about registrants "though a law enforcement 'knock and talk' or leaflet.").

The only specific limits on police authority to use "whatever means [they] deem[] appropriate" to disseminate information to the public is that they cannot post anything on the Internet that does not already appear on the state's Megan's Law website, § 290.45(a)(1), (3), and they cannot publicize victims' names. § 290.45(b). California law thus leaves the police free to disseminate registrants' information through "'knock and talk' or leaflet," Gov't Br. 9, public service announcements on television and radio, ads in the local newspaper, and any other non-Internet means.

Thus, the District Court correctly concluded that registrants "have no guarantee that their pseudonyms will be safeguarded from public dissemination …. Their right to speak anonymously will therefore be chilled." ER0013.

G. Proceedings Below

Because the Act required registrants to provide their Internet-related information to the police "immediately" after it went into effect on November 8, 2012, Plaintiffs filed suit that same day, requesting immediate class certification and a temporary restraining order. ER0001-03. The District Court granted the

TRO, in part because the government was not ready to implement the new requirements. ER0359-61.

To ensure they and the court could fully address the merits, the parties agreed to extend the TRO to allow additional time for briefing and stipulated that any preliminary relief would apply to all registrants to avoid litigating Plaintiffs' class certification motion. SER002-03.

The District Court issued a detailed order on the preliminary injunction motion. The Court first construed several provisions of the new law narrowly, as requested by the state. ER007-08. It then determined that, even with this narrow interpretation, Plaintiffs would likely succeed on the merits of their First Amendment speech claim because the statute affected too much speech and too many speakers to pass the intermediate scrutiny that applies both to content-neutral laws that regulate speech and to laws that have an incidental effect on speech. ER0009-17. Finally, it held the other three factors set forth in *Winter v. Natural Res. Def. Council, Inc.,* 555 U.S. 7, 20 (2008) favored issuing a preliminary injunction. ER0017-19. Because it based its ruling on the First Amendment, it did not reach plaintiffs' vagueness arguments. ER0004.

SUMMARY OF ARGUMENT

The Act violates the First Amendment on its face. First Amendment scrutiny applies to all laws that are directed at speech or that have the effect of

singling out individuals engaged in expressive activity. The Act does both, because it expressly requires registration of identifiers used for "Internet communication," and it applies to registrants only when they use the Internet to speak. Moreover, by requiring registrants to provide their Internet identifiers to the police, the Act infringes on the right to anonymous speech. Thus, as every court to address similar laws has held, these requirements are subject to First Amendment scrutiny.

That scrutiny requires the government prove that the law is narrowly tailored to achieve a legitimate government interest and that the law directly furthers that interest. Although the government's interests are legitimate, the Act sweeps far too broadly because it applies to individuals convicted decades ago of misdemeanor offenses that had nothing to do with minors or the Internet, to registrants whom the State has determined pose a low risk of reoffending, and to Internet identifiers that cannot be used for improper purposes, such as identifiers used to post comments on a newspaper's website. For these reasons, the statute lacks narrow tailoring and is also overbroad.

Moreover, the government has failed to show how the Act will achieve its objectives. It has not explained how the law will prevent or detect crimes. Although 16 other states have similar laws, there is no evidence that they have ever resulted in solving a single crime, and the General Accounting Office has

found no evidence that such laws improve public safety. Those few registrants who do intend to commit an online crime will simply create new identifiers without reporting them; the Fifth Amendment may even allow them to do so without criminal liability. The most likely effect of the Act is that it will chill protected speech and result in arrest and imprisonment of registrants who failed to report Internet identifiers and ISPs that they used only for lawful, constitutionally protected speech. It may even decrease public safety by making it harder for registrants to obtain stable employment and housing.

Finally, the Act's idiosyncratic definitions of Internet identifier and ISP are unconstitutionally vague. Due Process requires statutes to provide fair warning about what is illegal, and this rule is enforced with particular vigilance when, as here, free-speech rights are involved or the law carries criminal penalties. The Act's definitions of what must be reported are both ambiguous and vague, and neither the government nor Intervenors have ever even explained what they cover. The Act is therefore facially void for vagueness.

STANDARD OF REVIEW

This Court reviews the grant of a preliminary injunction for abuse of discretion, reviewing factual determinations for clear error and legal determinations *de novo*. *Thalheimer v. City of San Diego*, 645 F.3d 1109, 1115 (9th Cir. 2010). The court construes all facts in the prevailing party's favor.

Stuhlbarg Intern. Sales Co., Inc. v. John D. Brush and Co., Inc., 240 F.3d 832, 840 (9th Cir. 2001). *See generally Valle Del Sol Inc. v. Whiting*, 709 F.3d 808 (9th Cir. 2013).

ARGUMENT

I. The Act Triggers First Amendment Scrutiny Because It Singles Out, Burdens, And Criminalizes Speech

The Act triggers First Amendment scrutiny because the challenged provisions directly regulate speech and activity that is inextricably intertwined with expression. It does so in at least three ways. First, it singles out speech by requiring registrants to report within 24 hours an "Internet identifier" "used for the purpose of … communication." Act §13, § 290.024(b). Second, it regulates activity inextricably intertwined with expression – accessing the Internet through an ISP. Act §13, § 290.024(a). Third, it restricts anonymous speech, a form of expression protected by the First Amendment.

Intervenors' argument that the Act does not trigger First Amendment review because it has a mere "incidental" impact on speech is wrong: Intervenors conflate the ultimate question of whether a law survives First Amendment scrutiny with the threshold question of whether it is subject to such scrutiny. No court has accepted this argument; to the contrary, every case addressing sex-offender online speech registration requirements has correctly held that First Amendment scrutiny applies. *See Doe v. Shurtleff,* 628 F.3d 1217, 1223 (10th Cir. 2010) (*Shurtleff III*); *Doe v.*

Nebraska, ---F.Supp.2d----, Nos. 8:09CV456, 4:10CV3266, 4:10CV3005, 2012 WL 4923131 *17 (D. Neb. Oct. 17, 2012); *White v. Baker,* 696 F.Supp.2d 1289, 1307-08 (N.D. Ga. 2010). This Court should do the same.

A. First Amendment Scrutiny Applies To Laws That Single Out Speech-Related Activity For Regulation

First Amendment scrutiny applies to laws "directed at speech itself" and also to laws that regulate "nonexpressive activity [but have] the inevitable effect of singling out those engaged in expressive activity" or that relate to "conduct with a significant expressive element." *Arcara v. Cloud Books, Inc.*, 478 U.S. 697, 706-07 (1986) (citing *United States v. O'Brien*, 391 U.S. 367 (1968) and *Minneapolis Star and Tribune Co. v. Minnesota Comm'r Of Revenue,* 460 U.S. 575, 581 (1983)); *see Texas v. Johnson*, 491 U.S. 397, 406 (1989) ("A law directed at the communicative nature of conduct must, like a law directed at speech itself" satisfy First Amendment scrutiny). Laws that "impose special obligations" or "special burdens" on people involved in expressive activities "are always subject to at least some measure of heightened First Amendment scrutiny." *Turner Broad. Sys., Inc. v. F.C.C.*, 512 U.S. 622, 636-37, 640-41 (1994) (citing *Los Angeles v. Preferred Commc'ns, Inc.,* 476 U.S. 488 (1986) and *Minneapolis Star,* 460 U.S. at 583).

"There is no *de minimis* exception" to this rule. *Lorillard Tobacco Co. v. Reilly*, 533 U.S. 525, 567 (2001).[5]

B. The Internet-Identifier Reporting Requirements Regulate Online Speech

The Act defines "Internet identifier" 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*." Act § 13, § 290.024(b) (emphasis added); § 11, § 290.014(b). As interpreted by the government, Intervenors, and the court below, a registrant need not register a screen name that he simply uses to make an online purchase, but if he uses that identifier to speak he must alert the police within 24 hours. *See* ER0009. By specifically regulating the use of Internet identifiers *for communicative purposes,* the Act singles out specific types of expressive activity for special burdens and obligations and for that reason alone implicates the First Amendment.

Intervenors' "incidental effect" argument, Intervenors' Br. 9, is therefore wrong because the Act does not incidentally affect speech; it directly regulates speech. In fact, its entire rationale is that the government hopes to prevent registrants from engaging in harmful speech with potential victims. *See Ashcroft v.*

[5] Although some of these cases involve the press, these same rules apply to all speakers. *See Citizens United v. Fed. Election Comm'n*, 558 U.S. 310, 352 (2010).

Free Speech Coalition, 535 U.S. 234, 252-53 (2002) (law intended "to keep [online] speech from children … to protect them from those who would commit other crimes" violated First Amendment); *Buckley v. Valeo*, 424 U.S. 1, 17 (1976) (First Amendment scrutiny necessary whenever government's asserted interest "arises in some measure because the communication … is itself thought to be harmful.") (quoting *O'Brien*, 391 U.S. at 382).

Intervenors in any event misapprehend the law. "Governmental regulation that has an incidental effect on First Amendment freedoms" is indeed subject to First Amendment scrutiny. *N.A.A.C.P. v. Claiborne Hardware Co*., 458 U.S. 886, 912 (1982)) (citing *O'Brien*, 391 U.S. 367); *accord Turner*, 512 U.S. at 636-37 (laws that "impose an incidental burden on speech" are subject to First Amendment scrutiny); *see, e.g., O'Brien*, 391 U.S. at 376-77; *Perry v. Los Angeles Police Dep't,* 121 F.3d 1365, 1368 (9th Cir. 1997); *Gaudiya Vaishnava Soc'y v. City & Cnty. of San Francisco,* 952 F.2d 1059, 1064 (9th Cir. 1990). The "incidental" nature of a speech restriction goes not to the threshold question of whether the First Amendment applies, but to later questions of the appropriate level of constitutional scrutiny and whether the law survives that scrutiny. *See Turner*, 512 U.S. at 636-37, 661-62; *Gaudiya,* 952 F.2d at 1065.

Thus, even if the Act's recordkeeping and 24-hour-reporting requirements were merely incidental restrictions on speech, they would implicate the First

Amendment because they mandate that any time a registrant wants to make a comment on a new newspaper website, or to send an email or access the web at a new Internet café, he must report that he has done so to the police or face a prison term. In fact, a registrant who uses a new screen name or ISP would be reckless not to *immediately* report it, lest he forget or be unable to do it later that day and face arrest. Although this type of updating may theoretically be done by mail, a registrant may reasonably fear that the post office will lose his letter or the police will not log it. A registrant who would like to comment on a newspaper article or catch up with the news online while traveling must therefore decide whether doing so is worth the burden of reporting it within 24 hours and the risk that, even if he does so, he may face arrest and prosecution because of factors beyond his control. These burdens implicate the First Amendment. *See, e.g.*, *Lamont v. Postmaster Gen.*, 381 U.S. 301, 307 (1965) (imposing "affirmative obligation" that addressee must specifically request mail burdened and violated First Amendment); *Simon & Schuster, Inc. v. New York State Crime Victims Bd.*, 502 U.S. 105, 118, 122 n.* (1991); *Am. Legion Post 7 v. City of Durham*, 239 F.3d 601, 607 (4th Cir. 2001) ("the amount of burden on speech needed to trigger First Amendment scrutiny as a threshold matter is minimal"); *cf. Hynes v. Borough of Oradell*, 425 U.S. 610, 620-22 (1976) (invalidating mail-in identification requirements for canvassers on First Amendment vagueness grounds).

Intervenors' reliance on *Arcara* is misplaced. That opinion expressly acknowledges that laws imposing incidental effects, restrictions, or limits on speech are subject to First Amendment scrutiny. *See Arcara*, 478 U.S. 702-03; *id.* at 708 (O'Connor, J., concurring). *Arcara* allowed the government to close a bookstore that was being "used as a place for prostitution" only because both the statute, a general law prohibiting prostitution, and the regulated activity, prostitution, involved "absolutely no element of protected expression." *Id.* at 705; *see id.* at 708 (O'Connor, J., concurring). Because the Act expressly and exclusively applies to online speech, *Arcara* is irrelevant. *Compare* Act § 13 ("for the purpose of … Internet communication"), *with Arcara*, 478 U.S. at 705.

Nor does *Church of Am. Knights of the Ku Klux Klan v. Kerik*, 356 F.3d 197 (2d Cir. 2004) support Intervenors' position. In that case, too, the court based its holding on a conclusion that the conduct regulated by the statute – wearing masks – was not expressive. 356 F.3d at 207-08; Intervenors' Br. 12. Even if this were correct,[6] this decision, like *Arcara*, is distinguishable from a statute specifically regulating expressive activity. In any event, the court acknowledged that "the First Amendment is implicated" by requirements such as those contained in the Act: "government efforts to compel disclosure of names." *See id.* at 209.

[6] It may well be wrong. *See Recent Cases*, 117 Harv. L. Rev. 2777-84 (2004).

Finally, Intervenors emphasize that registrants must already comply with other registration requirements, such as reporting their registered vehicles and other public information. But, as courts striking down restrictions on registrants' First Amendment rights explain, those other requirements have nothing to do with speech or with non-public information, and the cases upholding them say nothing about registrants' First Amendment rights. *See Doe v. Prosecutor, Marion Cnty., Indiana*, 705 F.3d 694, 702 (7th Cir. 2013) (invalidating restrictions on registrants' online speech)*; Doe v. City of Albuquerque*, 667 F.3d 1111, 1121 (10th Cir. 2012) (invalidating restrictions on registrants' library use). Laws affecting speech must meet a higher standard. *See City of Los Angeles v. Preferred Communications, Inc.*, 476 U.S. 488, 496 (1986); *Gaudiya*, 952 F.2d at 1063 (that city can regulate sale of fish does not mean it can regulate sale of expressive merchandise).[7]

C. The Act's ISP Reporting Requirements Regulate Access To The Internet

The Act requires reporting of any additions or changes to a registrant's account with an "Internet service provider." *See* Act § 11, § 290.014(b), § 13, § 290.024(a). Although the term is vague, *see infra* Part III, the Act defines ISP as

[7] Although Intervenors claim that a registrant must tell the police if he sends a letter to the newspaper using a penname, Intervenors' Br. 11-12, § 290.014 only requires that registrants report a name change, and there is no indication that writing such a letter would qualify; such a requirement would raise serious First Amendment concerns.

"an entity … through which a person may obtain access to the Internet." *See id.* § 13, § 290.024(a).

The Internet is a "dynamic, multifaceted category of communication [that] includes not only traditional print and news services, but also audio, video, and still images;" it allows "any person with a phone line [to] become a town crier with a voice that resonates farther than it could from any soapbox." *Reno v. Am. Civ. Liberties Union,* 521 U.S. 844, 870 (1997). All of this, and much more that occurs on the Internet, is pure speech. *See id.* at 849-53, 870 (1997); ER0503-05; *see generally* ER0502-520.

A person who wants to participate online as a speaker or listener needs access to the Internet, and to get this access a registrant must use what the Act defines as an ISP. Laws that obstruct or burden a speaker's ability to reach his audience implicate the First Amendment. *See, e.g., Preferred Commc'ns,* 476 at 488 (denial of utility-poles access to cable TV company); *Minneapolis Star,* 460 U.S. at 581 (tax on ink); *Edwards v. City of Coeur d'Alene*, 262 F.3d 856, 861-62 (9th. Cir. 2001) (ban on supports for protest signs); *Perry,* 121 F.3d at 1368 (ban on sales of goods, some of which contain expressive messages); *Gaudiya Vaishnava Soc'y,* 952 F.2d at 1064 (regulation of same). So do laws that restrict an individual's ability to receive information. *See Lamont*, 381 U.S. at 307; *City of Albuquerque*, 667 F.3d at 118-20; *see also Reno*, 521 U.S. at 874-75. Because the

ISP-reporting requirement affects a registrant's ability to get online – a necessary first step to participating in online communication – it is subject to First Amendment scrutiny.

D. The Law Triggers First Amendment Scrutiny Because It Criminalizes Anonymous Speech And Association

The unique and onerous burdens the Internet identifier and ISP registration requirements impose on *anonymous* online speech provide an additional reason that First Amendment scrutiny is essential, wholly apart from the reasons discussed above. "Under our constitution, anonymous [speech] … is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent," protected by the First Amendment. *McIntyre v. Ohio Elections Comm'n,* 514 U.S. 334, 357 (1995) (law prohibiting anonymous leafletting unconstitutional); *see Talley v. California*, 362 U.S. 60, 64-65 (1960) (same). This protection allows Americans to freely express controversial or unpopular views without having to fear governmental retaliation akin to what the Framers experienced firsthand. *See id.*; *see also John Doe No. 1 v. Reed*, 130 S.Ct. 2811, 2820 (2010). "Depriving individuals of this anonymity is therefore a broad intrusion, discouraging truthful, accurate speech by those unwilling to disclose their identities." *Washington Initiatives Now v. Rippie*, 213 F.3d 1132, 1138 (9th Cir. 2000) ("*WIN*") (citation omitted).

Thus, as even the cases that Intervenors cite for the contrary proposition recognize, laws requiring speakers to identify themselves will be upheld only when the government can justify that infringement under the First Amendment. *Compare* Intervenors' Br. 13-14, 16-17 with *Reed*, 130 S.Ct. at 2817-18, 2820-21; *Citizens United*, 558 U.S. at 366-67; *Buckley v. Am. Constitutional Law Found., Inc.*, 525 U.S. 182, 197-98 (1999) ("*ACLF*").[8] *See also Watchtower Bible and Tract Soc'y of New York, Inc. v. Village of Stratton*, 536 U.S. 150, 166-67 (2002); *Buckley*, 424 U.S. at 66-68; *N.A.A.C.P. v. Alabama*, 357 U.S. 449, 461-64 (1958); *Doe v. 2TheMart.com,* 140 F.Supp.2d 1088, 1093 (W.D. Wash. 2001). Cases applying and holding under the First Amendment that various speech restrictions were justified thus provide no support for – and indeed contradict – Intervenors' argument that the First Amendment does not apply at all. Indeed, one of the cases cited by Intervenors' specifically holds that that a statute requiring registrants to

[8] Although *ACLF* indicates that identification badges are more offensive to the First Amendment than an affidavit requirement, it does not suggest that such requirements, which were not challenged, are exempt from constitutional scrutiny. *See ACLF*, 525 U.S. at 199-200. The Tenth Circuit upheld the affidavit only because it furthered the state's "strong, often compelling, interest in preserving the integrity of its electoral system." *ACLF v. Meyer*, 120 F.3d 1092, 1099-1100 (10th Cir. 1997). The unique strength of this interest, not implicated here, is often what justifies reporting requirements. *See, e.g., Watchtower Bible*, 536 U.S. at 157; *Buckley*, 424 U.S. at 66-68 (disclosure is "essential" and "least restrictive means" to inform voters and combat corruption).

report their Internet identifiers is subject to First Amendment scrutiny. *Shurtleff III*, 628 F.3d at 1223.

These protections apply equally to online as to offline speech. *See In re Anonymous Online Speakers*, 661 F.3d 1168, 1173, 1175-78 (9th Cir. 2011) (collecting cases). Pseudonymous speech is treated as anonymous speech. *See McIntyre*, 514 U.S. at 341-44, *Talley*, 362 U.S. at 65.

The Act makes it a crime for registrants to use a pseudonymous screen name to participate in online speech without disclosing their real identity to the police within 24 hours. *See* Act § 11, § 290.014(b). As Professor Post explains, most newspaper and other websites that allow comments require commenters to have a screen name, and commenters routinely use pseudonyms to maintain their anonymity. ER0508, 0519. But under the Act, registrants cannot speak anonymously because they must turn this pseudonym over to the police. This effectively criminalizes anonymous online speech and therefore implicates the First Amendment. *Ashcroft*, 535 U.S. at 244 ("a law imposing criminal penalties on protected speech is a stark example of speech suppression").

Although Intervenors and the Government dismiss the chilling effect of the registration requirement on anonymous speech, the factual record is undisputed that the Act's burdensome and confusing registration requirements would deter Plaintiffs Doe and Roe, and members of plaintiffs California Reform from

engaging in lawful, online anonymous speech. ER523-26, 0553-55, 0558-60. Where, as here, "the record is replete with examples" of the ways in which the challenged governmental action "chilled [plaintiffs'] speech," the court applies "First Amendment scrutiny." *Conant v. Walters,* 309 F.3d 629, 638, 639 (9th Cir. 2002); *see Shelton v. Tucker*, 364 U.S. 479, 488 (1960); *WIN*, 213 F.3d at 1138.[9] Moreover, the Government's argument that California law limits disclosure of registrants' information to the public is wrong as a matter of law and contradicted by the factual record. *See supra* Statement of Facts, Part F & *infra* Part II-D-1. It is also legally irrelevant because the First Amendment is implicated by requirements that speakers disclose their identities to the government "[e]ven if there were no disclosure [of that information] to the general public," and even if the disclosure occurs long after the speech. *Shelton,* 364 U.S. at 480, 486 (statute requiring teachers to inform government of organizations to which they had belonged or contributed in preceding five years violated First Amendment);

[9] Intervenors rely on *Laird v. Tatum*, 408 U.S. 1 (1972), in support of their argument that the First Amendment does not apply. *Laird* held that individuals who claimed that military surveillance chilled their speech lacked standing because they could not show any "specific action …. against them." *Id*. at 3, 9, 13-15; Intervenors' Br. 13-14. There is no question that Plaintiffs have standing because the law is directly targeted at them and "carries an affirmative obligation" that they surrender their anonymity by reporting their online activities or face arrest. *Id*. at 12 (quoting *Lamont*, 381 U.S. at 307).

Lamont, 381 U.S. at 307 (statute requiring disclosure to government violated First Amendment; no indication of public access or dissemination).

Finally, Intervenors' argument that registrants have no absolute right to anonymity is irrelevant, because Plaintiffs do not claim such a right. Intervenors' Br. 18. The First Amendment right to speak anonymously is not absolute for anybody. *Anonymous Online Speakers*, 661 F.3d at 1173. But when the government, through the criminal law, a judicial subpoena, or some other action, threatens to infringe upon that anonymity, the party seeking disclosure must justify that infringement under the First Amendment. *See id.* at 1173. As both the government and Intervenors conceded below, "speech by sex offenders who have completed their terms of probation or parole enjoys the full protection of the First Amendment." *See* ER0005. If the government limits registrants' ability to engage in anonymous speech, the First Amendment requires it to justify those limitations.

II. The CASE Act Fails First Amendment Scrutiny Because It Is Not Narrowly Tailored And Does Not Directly Advance The Government's Goals

Laws implicating the First Amendment are generally subject either to strict or intermediate scrutiny. *See Turner*, 512 U.S. at 661-62. Strict scrutiny is likely appropriate because the Act applies only to the speech of a disfavored group of

speakers – registered sex offenders – and may discriminate by content.[10] However, because, as the District Court correctly held, the law fails even intermediate scrutiny, Plaintiffs focus on that standard.

Intermediate scrutiny requires that content-neutral statutes affecting speech "be 'narrowly tailored' to advance the interest asserted by the State." *Simon & Schuster*, 502 U.S. at 122 n.*; *see Comite de Jornaleros de Redondo Beach v. City of Redondo Beach,* 657 F.3d 936, 950-51(9th Cir. 2011) (en banc), *cert. denied*, 132 S.Ct. 1566 (2012). "To satisfy the narrow tailoring requirement, the Government bears the burden of showing that the remedy it has adopted does not burden substantially more speech than is necessary to further the government's legitimate interests." *Comite,* 657 F.3d at 948 (quoting *Turner*, 512 U.S. at 662). The government must meet this burden with actual evidence; it may rely on legislative findings only when they are "reasonable inferences based on substantial evidence." *Turner,* 512 U.S. at 666 (plurality); *Video Software Dealers Ass'n v. Schwarzenegger*, 556 F.3d 950, 962 (9th Cir. 2009). Because the Act was passed as an initiative, it does not contain any such findings. *People v. McKee*, 47 Cal.

[10] If the government and Intervenors are correct that it exempts certain types of online speech, ER083-84, the Act is content-based. Moreover, the First Amendment generally prohibits "restrictions distinguishing among different speakers, allowing speech by some but not others." *Citizens United*, 558 U.S. at 340-41; *see Sorrell v. IMS Health, Inc.*, 131 S.Ct. 2653, 2664 (2011). Laws that discriminate by content or speaker are subject to strict scrutiny. *See Citizens United*, 558 U.S. at 340; *Simon & Schuster*, 502 U.S. at 115-18.

4th 1172, 1206 (Cal. 2010). It is otherwise subject to the same scrutiny as any state statute, because "[t]he voters may no more violate the United States Constitution by enacting a ballot issue than the general assembly may …." *Buckley*, 525 U.S. at 194 (1999). Online speech receives the same scrutiny as does other types of pure speech. *See Reno*, 521 U.S. at 870.

Two federal courts have invalidated or enjoined the enforcement of laws that require sex offenders to provide the government with identifying information about their online speech, based on lack of narrow tailoring. *See Nebraska,* 2012 WL 4923131 *28 ("far too much speech is unnecessarily burdened by the requirement that Doe report to the government his daily political activity on blogs"); *White,* 696 F.Supp.2d at 1310 ("the scope of the internet identifying information required to be reported is not limited to identifiers used in the type of internet communications that enable sexual predators to entice children"). A third court invalidated a Utah statute because it did not restrict the state's use or dissemination of registrants' Internet information. *See Doe v. Shurtleff,* 1:08-CV-64 TC, 2008 WL 4427594 at *8-*9 (D. Utah, Aug. 20, 2009) ("*Shurtleff I*"). After the legislature responded by amending the statute to restrict police use and dissemination of the information "only … to investigate an Internet sex crime," the district court upheld the amended statute, *see id.*, and the Tenth Circuit affirmed. *See Shurtleff III,* 628 F.3d

1217; *Doe v. Shurtleff,* 1:08-CV-64-TC, 2009 WL 2601458 *5 (D. Utah Aug 20, 2009) ("*Shurtleff II*").

Here, the district court correctly concluded that the Act is not narrowly tailored because "the provisions apply both to more speakers and more speech than is necessary to advance the government's legitimate purposes." ER0014. The Act is also insufficiently tailored because it fails to restrict disclosure of registrants' Internet information. Finally, the Act, while burdening speech, fails to advance the government's goals of preventing sex trafficking.

A. The CASE Act Is Not Narrowly Tailored Because It Applies To Speech That Cannot Be Used To Commit A Crime

The Act's legitimate interests are clear: deterring, tracking, and preventing individuals from using the Internet to facilitate or commit human-trafficking or sex-related crimes. *See* Intervenors' Br. 20 (quoting Act's stated purposes). The only speech that it can legitimately target to further this interest is speech used to solicit, facilitate, or commit such crimes. *See Porter v. Bowen,* 496 F.3d 1009, 1023 (9th Cir. 2007). As the government admits, other speech by registrants is lawful and constitutionally protected. ER0072*; see Marion Cnty.*, 705 F.3d at 699 ("there is nothing dangerous about Doe's use of social media as long as he does not improperly communicate with minors"). The critical question is thus whether the Act burdens "substantially more speech than is necessary" to prevent or detect unlawful speech. *Comite*, 657 F.3d at 948; *see Porter*, 496 F.3d at 1023.

To satisfy this standard, a law that seeks to prevent registrants from committing new crimes should apply only to "the means by which sex offenders may communicate with [victims] and by which [victims] may respond to offenders' sexual advances," "usually, but not exclusively, interactive, and often real time" "Internet communication." *White,* 696 F.Supp.2d at 1311. But the Act instead requires registrants to disclose to the police *all* Internet identifiers, including identifiers used to comment on articles published on newspaper websites, to participate in discussion groups like that of Plaintiff California Reform pertaining to the civil rights of § 290 registrants, and to run Plaintiff Roe's anonymous blog. ER0508, 0524-26, 0553-54. Such websites "are by their nature open to the public and pose no threat to children. That sex offenders … may 'blog' threatens no child, but the government reporting requirement – that puts a stake through the heart of the First Amendment's protection of anonymity – surely deters faint-hearted offenders from expressing themselves on matters of public concern." *Nebraska,* 2012 WL 4923131 *28. The District Court specifically found that the "government has not shown the utility of requiring registration of Internet identifiers used for this type of public commentary." ER0016. Nor is there any utility in requiring registration of identifiers used for customer support, a regulation even Intervenors admit is "absurd." ER0083.

In *Marion County,* the Seventh Circuit applied intermediate scrutiny and struck down a statute banning registered sex offenders from social networking websites, holding that the law was "not narrowly tailored" because it "broadly prohibit[ed] substantial protected speech rather than specifically targeting the evil of improper communications to minors." 705 F.3d at 695. Even putting-aside newspaper and other sites that cannot be used for improper purposes, and focusing only on social networking, "illicit communication comprises a minuscule subset of the universe of social network activity. As such, the … law targets substantially more activity than the evil it seeks to redress" *id.*; *see* ER0488 (registrants primarily use the Internet for same purposes as other members of the general public). Although *Marion County* involved a prohibition rather than a registration requirement, its narrow-tailoring analysis applies equally to laws that burden speech. *See Lorillard Tobacco*, 533 U.S. at 567; *see also Sorrell*, 131 S.Ct. at 2664; *White*, 696 F.Supp.2d at 1310 (registration law that extended to "communications that are posted publicly on sites dedicated to discussion of public, political, and social issues" not narrowly tailored).[11]

[11] The distinction between a prohibition and a burden may instead be relevant to the separate prong of intermediate scrutiny that the government must also prove, that the law leaves open "ample alternative channels for the communication." *See G.K. Ltd. Travel v. City of Lake Oswego*, 436 F.3d 1064, 1074-75 (9th Cir. 2006).

C. The CASE Act Is Not Narrowly Tailored Because It Burdens Too Many Speakers

Second, the Act is woefully over-inclusive because it applies to *all* registrants, regardless of the age or the nature of the conviction and whether they are at high or low risk of re-offending.

Most sexual offenders do not re-offend; this is particularly true for those whom the state classifies, using the Static-99 and other assessments, as low or moderate-low risk upon release. *See supra* Statement of Facts, Part E; ER0376-77, 0487, 0489-90. Even looking only at the subset of California registrants who were sentenced to prison – meaning they were convicted of felonies and denied probation – 30% are classified as low risk, and an additional 38% are classified as moderate-low risk. ER0487. Thus, "it is not particularly useful to require *all* registrants to provide information about their Internet use." ER0491; *see also* ER0382 ("blanket policies … waste resources").

California cannot argue that it is infeasible to assess the risk of offenders because it currently *mandates* that *all* § 290 registrants be assessed for risk. *See* Cal. Penal Code § 290.04(a)(1), *et seq*. Nor can it claim its assessment tools are unsuitable for assessing individual risk, because it uses these same tools to decide which individuals need increased supervision or are so likely to re-offend that they

should be involuntarily committed.[12] Thus, the District Court specifically found the government failed to show why it could not use these same risk-assessment tools to exclude registrants who pose a low or moderate risk of re-offending. ER15-16.

The Act is also over-inclusive because it ignores the fact that the longer offenders remain offense-free in the community, the less likely they are to re-offend sexually. ER0373-82, 489-90. Eventually, they are *less likely* to be arrested for a sex-related offense than individuals who have never been arrested for a sex-related offense; persons originally classified as low-risk reach this point upon release. ER0377-79, 0414; *see also United States v. T.M.*, 330 F.3d 1235, 1240 (9th Cir. 2003) ("[T]hat T.M. has lived the last twenty years without committing a sex offense suggests that he no longer needs to be deterred or shielded from the public."). A large proportion of registrants – including Plaintiffs Doe and Roe – committed their offenses decades ago and have not been in trouble with the law

[12] "The rule is settled that an expert may … use statistical actuarial tools such as the Static–99, in combination with dynamic factors, to support an opinion that an individual is likely to reoffend." *People v. Jones*, B231144, 2012 WL 75628 at *8 (Cal. Ct. App. Jan. 10, 2012) (unpublished) (citations omitted). *See, e.g., People v. Aguon*, D053875, 2013 WL 175025 at *1 (Cal. Ct. App. Jan. 17, 2013) (unpublished) *review denied* (May 1, 2013) ("100 percent likelihood of reoffending"); *People v. Judge*, D054342, 2013 WL 285682 at *1 (Cal. Ct. App. Jan. 25, 2013) (unpublished), *review denied* (Apr. 10, 2013).

since then. ER0489. Nevertheless, the Act requires them to report their online speech activities forever.

Although the government touts the possibility that registrants can obtain relief though a certificate of rehabilitation and pardon, a 1998 law specifically and retroactively bars many registrants from even applying for such relief. *See People v. Ansell*, 25 Cal.4th 868, 877-78 (2001). For those who can apply, relief is completely discretionary and may be denied even if a registrant is completely rehabilitated. *See id.* at 887-88 ("there is no circumstance under which the statutory scheme requires or guarantees issuance of a certificate of rehabilitation"). This remote possibility of discretionary relief cannot save a statute that infringes First Amendment rights.

Finally, more than 99% of registrants were convicted of crimes that did *not* involve the Internet, and 80%-90% of sex crimes involve perpetrators previously known to the victim. ER0420, 0488. For this reason, too, the Act "is not narrowly tailored to target those offenders who pose a factually based risk to children through the use or threatened use of the [specified] sites or services." *Nebraska*, 2012 WL 4923131 at *19. To the contrary, it "inexplicably applies to sex offenders whose crimes did not involve the Internet or children," *Marion Cnty.*,

705 F.3d at 702 n.6,[13] and also to people who may only be "pranksters with poor judgment." *Nunez*, 594 F.3d at 1137. The state cannot justify infringing an individual's constitutional rights with "a generalized assessment based on the class of sex offenders generally, rather than on the particular sex offenses a defendant has committed or related offenses he is likely to commit." *United States v. Weber*, 451 F.3d 552, 569 (9th Cir. 2006) (invalidating supervised release condition); *see United States v. Wolf Child*, 699 F.3d 1082, 1094 (9th Cir. 2012).

The Act's gross overbreadth is unnecessary because it could have been written much more narrowly. For example, it could apply only to Internet identifiers relating to sites that could be used to commit a crime, or only to registrants who have been convicted of offenses involving the Internet, or who are at higher risk of re-offending, or even by allowing persons with very old or minor convictions or those who could otherwise demonstrate that they do not pose a risk to apply to be excluded from the new requirements.[14] Instead, it applies to all Internet identifiers and to speech by registrants who pose no more danger of

[13] Although there is no evidence in the record as to the percentage of registrants who were convicted of crimes involving minors, this lack of evidence weighs against the law's validity because the government has the burden to show narrow tailoring. *See Comite*, 657 F.3d at 948-49.

[14] California already recognizes in other contexts that registrants convicted of different offenses pose different risks; it therefore publicly discloses varying amounts of information about registrants depending on the offense of conviction, and provides a process for registrants to apply for exclusion from the publicly accessible website if they meet certain conditions. *See* § 290.46(b)-(e), ER0141.

committing a future sex crime than a typical member of the population. This "availability of obvious less-restrictive alternatives renders [the] speech restriction overinclusive." *Valle Del Sol*, 709 F.3d at 826 (citing *Comite*, 657 F.3d at 950); *see Comite,* 657 F.3d at 949-51; *Porter*, 496 F.3d at 1025 (government has burden to rebut less-restrictive alternatives suggested by plaintiffs).

The lack of narrow tailoring is exacerbated by the vagueness of the Act's definitions of what registrants must provide, combined with the serious punishment for failure to provide the correct information. Vague criminal laws regulating speech are inevitably overinclusive because the "severity of criminal sanctions may well cause speakers to remain silent rather than" risk prosecution for "arguably unlawful" activity. *Reno*, 521 U.S. at 872; *see id.* at 870-72. As discussed below, the Act's definitions of "Internet identifier" and "Internet service provider" are incomprehensible. *See infra* Part III. A registrant who would like to engage in anonymous Internet speech in a way that only "arguably" falls within the Act's purview would be reckless indeed to risk arrest and imprisonment.

Finally, the law's *mens rea* requirement is of little help, because only a foolhardy registrant could feel confident that a jury would acquit him on that basis, particularly after learning he was a convicted sex offender and had signed a statement saying he understood the registration requirements and his "duty to know them." *See* ER0331 (registration form); *cf. Gonzalez*, 551 F.3d at 886 n.10. In any

event, even if a jury might eventually acquit a registrant who claimed confusion,"[t]he chilling effect upon the exercise of First Amendment rights may derive from the fact of the prosecution, unaffected by the prospect of its success or failure." *Dombrowski v. Pfister*, 380 U.S. 479, 487 (1965).

D. The CASE Act Is Not Narrowly Tailored Because It Fails To Restrict The Government's Use Or Dissemination Of Internet Identifying Information

The district court in *White* found the registration requirement insufficiently tailored where the statute allowed "disclos[ure] to law enforcement agencies for 'law enforcement purposes.'" 696 F.Supp.2d at 1310. The court found this "permitted use [to be] undefined and extensive," and thus "not sufficiently narrowly-tailored to meet the government's compelling interest to protect children." *Id.* at 1310, 1311. Similarly, the absence of "restrictions on … [the state's] use or disseminat[ion] of registrants' internet information" led the district court in *Shurtleff I* to find the original version of Utah's statute unconstitutional. 2008 WL 4427594 *8.

The CASE Act suffers from this same flaw because California law enforcement has broad authority to disseminate registrants' Internet identifying information. Like the ill-tailored statutes in *White* and *Shurtleff I,* California permits use of registrants' information in circumstances that are "undefined and extensive." *White,* 696 F. Supp. 2d at 1310. Because the statute does not limit the

government's use or dissemination of that information, it is insufficiently tailored to the government's goals of preventing or investigating sex trafficking.

1. California Law Does Not Prohibit Dissemination Of Registrant Information

The Government's claim that the existing statutory scheme restricts disclosure of registrants' information is contrary to California law and the factual record. Gov. Br. at 15-19.

As discussed above, the Legislature has amended the registration statute so that California law now allows the police to release registrant information to the public without any reason to think a crime has occurred, and the CASOMB survey shows that the police do just this. *See supra* Statement of Facts, Part F. The only support the Government presents for its contrary claim is a citation to a legal encyclopedia that suggests that the police need reasonable suspicion to conduct some sort of "further investigation." *See* Gov't Br. 17 (citing 42A Cal. Jur. 3d Law Enforcement § 155, n.8 *see also People v. Goodson*, 106 Cal. App. 3d Supp. 5, 10 (Super. Ct. 1980)). But *Goodson* involved listening at the door of a motel room and turned on the Fourth Amendment's prohibition against unreasonable searches. *See Goodson*, 106 Cal. App. 3d Supp. at 9-10. This in no way limits the authority of law enforcement to access sex offender information in a government database or to disseminate information from that database.

The state's assurance that police will treat this information with care is insufficient. When First Amendment rights are at stake, the courts will not uphold a statute "merely because the Government promise[s] to use it responsibly" or to "adhere to standards absent from the [statute's] face." *United States v. Stevens*, 130 S.Ct. 1577, 1591 (2010); *see Comite*, 657 F.3d at 946-47. This is particularly important here because the Attorney General disclaims any authority to control local police, *see* ER19, and the "general police power" granted to California police authorizes them to take any law-enforcement action not specifically prohibited by statute or the Constitution, with no need for individualized suspicion of wrongdoing. *Ingersoll v. Palmer*, 43 Cal. 3d 1321, 1347-49 (1987).

2. *Shurtleff III* Is Distinguishable And Unpersuasive

Because California law fails to restrict the government's use and dissemination of registrants' Internet information, the district court correctly concluded that it does "not contain the safeguards present in the amended Utah statutes" upheld by the Tenth Circuit in *Shurtleff III,* and is "closer to the pre-amendment" statutes struck-down in *Shurtleff I.* ER12. The amended Utah statute permitted "sharing [of internet identifiers] only among law-enforcement agencies, not the public at large, and only for the recited law-enforcement purposes." *Shurtleff III,* 628 F.3d at 1222. Moreover, the police could only "look beyond the anonymity surrounding a username … after a new crime had been committed." *Id*.

at 1225. There was no indication that registrant information had ever been disseminated to the public under any circumstances. California law, however, allows the police to access and disseminate registrant information even when no crime has been committed, and the evidence shows they have repeatedly done just this.

Second, Utah's reporting requirements were much less burdensome than the Act's. Under the Utah statute, registrants need only report their identifiers at their semi-annual registration. *See* UT ST § 77-41-105(3) (West). The Act by contrast requires reporting within 24 hours of any addition or change to an Internet identifier or ISP. *See* Act § 11, § 290.014(b). Having to separately report every change is more burdensome than simply keeping a list of changes to provide twice a year. Moreover, *Shurtleff III* attached great weight to the fact that registrants would not have to report their identifiers until long after they had finished speaking. 628 F.3d at 1225. Here, the 24-hour requirement means registrants will likely have to report before they are done speaking. ER0013; *see also WIN*, 213 F.3d at 1138.

In any event, *Shurtleff III* is unpersuasive because, although it held that the law was subject to intermediate scrutiny, it never applied a narrow-tailoring test. The opinion contains no discussion of what websites were covered by the law, how many of those sites could be used for improper purposes, the likelihood that

different categories of registrants would use the Internet to re-offend, or how the law would advance the government's interests. Instead, the court seems to have concluded that because the law required disclosure only long after the fact and because it absolutely prohibited dissemination to the public, it imposed only a minor burden on speech such that no narrow-tailoring analysis was necessary. But the Supreme Court has expressly rejected the notion that laws imposing a "very limited" burden on speech are exempt from First Amendment scrutiny, holding instead that "[t]here is no *de minimis* exception for a speech restriction that lacks sufficient tailoring or justification." *Lorillard Tobacco*, 533 U.S. at 567 (invalidating statute under intermediate scrutiny).[15] Because *Shurtleff III* fails to engage in a meaningful analysis of whether the government had shown the Utah law to be narrowly tailored, it is unpersuasive on that question.[16]

E. The Act Fails Intermediate Scrutiny Because Government Has Failed To Show That It Furthers Its Interests In A Direct And Material Way

Finally, narrow tailoring also demands the government "demonstrate that the recited harms are real … and that the regulation will in fact alleviate these harms in

[15] The intermediate scrutiny that *Lorillard Tobacco* and *Valle Del Sol* apply to content-based burdens on commercial speech is "substantially similar" to the intermediate scrutiny at issue in this case. *Lorillard Tobacco*, 533 U.S. at 554; *Valle Del Sol* 709 F.3d at 825-26.

[16] Moreover, as discussed above, disclosure requirements impose significant burdens on First Amendment rights.

a direct and material way." *Turner*, 512 U.S. at 664 (plurality); *Video Software Dealers*, 556 F.3d at 962; *see United States v. Grace*, 461 U.S. 171, 180-81 (1983). But the Court below found that "the government has not provided any evidence regarding the extent to which the public safety might be enhanced" by the Act. ER0018. In fact, the government has not even explained – much less proved – how collecting this information will actually serve a legitimate purpose. *Cf. Marion Cnty.*, 705 F.3d at 701. The only evidence that even suggests that it will be useful is a pair of declarations from government lawyers simply concluding that the information would be useful without any real explanation of how, particularly in cases where the victim knows the offender, which comprise at least 80% of sex crimes. *See* ER253-59, 333-37. The state cannot meet its burden to show narrow tailoring with "affidavits [that are] conclusory and without sufficient support in facts." *Am. Passage Media Corp. v. Cass Commc'ns, Inc.*, 750 F.2d 1470, 1473 (9th Cir. 1985); *see Kenosha Liquor Co. v. Heublein, Inc.*, 895 F.2d 418, 420 (7th Cir. 1990) ("Expert opinions are worthless without data and reasons.").[17]

Indeed, there is no evidence that requiring offenders to report Internet information is effective. Although sixteen states and three territories have

[17] Intervenors therefore cannot complain that the District Court "ignored" their evidence, particularly in light of the standard of review. And their citation to *United States v. Cervini,* 16 Fed. Appx. 865 (10th Cir. 2001) adds nothing to their arguments; that case involved some sort of Internet news *group*, not a news site. *Id.* at 869-70.

"substantially implemented" the federal Sex Offender Registration and Notification Act, there is no evidence that implementation has improved public safety in those juridictions. *See* General Accounting Office, Sex Offender Registration and Notification Act, 13, 23-24 (2013).[18] Nor are there any examples from anywhere that Internet registration requirements have ever helped solve a crime. *See* ER10 & n.10.[19] These laws may even decrease public safety by making it harder for registrants to obtain stable employment and housing. ER0490.

Moreover, in attempting to minimize the Act's burdens on speech, the government and Intervenors[20] construe the law in a way that robs it of any possible utility. First, they assert that registrants need only disclose their actual screen-names, without any information that would allow the government to determine what website the name relates to. Intervenors' Br. at 22-23. But as Professor Post explains, because there may be hundreds of thousands of individuals who use

---

[18] *Available at* http://www.gao.gov/assets/660/652032.pdf (last visited May 8, 2013).

[19] SORNA differs from California law in a number of ways, of which Internet registration is only one. *See* CASOMB Statement of Position on Adam Walsh Act, *available at* http://www.casomb.org/docs/Adam%20Walsh%20Position%20Paper.pdf (last visited May 8, 2013). After determining that many of SORNA's provisions were ill-advised, wasteful, and incompatible with California law as well as the current research, CASOMB recommended that California not change its law to conform to SORNA (which is not mandatory), and the legislature acted accordingly. *See id.*

[20] The government joins in Intervenors' arguments. *See* Gov't Br. 1.

common Internet identifiers (*e.g.*, "Angry_User") on different websites at any particular time, reporting such names without any information about the website has no value because it cannot be used to locate anybody. *See* ER507.

Similarly, their claim that registrants can maintain anonymity by choosing to use the screen name "anonymous," even if it were correct,[21] would completely eviscerate any legitimate purpose for the requirements because the law would be completely useless at identifying anybody. And although the Act's supporters agree that it requires registrants to report opening an account with Starbucks so they can access that company's WiFi connections, they assert that a registrant could then go to "every Starbucks in America" or use a wireless network at a café that does not require an account without providing any additional information. ER086, 95. Again, if this is true, the reporting requirement becomes a completely useless burden on registrants.

The state cannot have it both ways: either the Act allows the police to locate registrants who speak on the Internet, in which case it infringes on anonymity, or it

[21] Because most websites require users adopt a *unique* login, "anonymous" or "JD" is only available to one person per site. Registrants who, for example, want to comment on a newspaper's website would necessarily have to create a more unusual identifier and then report that within 24 hours. In addition, a law that only allowed registrants to avoid the burdens of registration by using the screen name "anonymous" instead of one the user had chosen "to impart a message" (whether "Cato," "A True Patriot," or "Angry_User") would constitute a regulation of content. *See McIntyre*, 514 U.S. at 348-49; *id.* at 367-68 (Thomas, J., concurring).

does not, in which case its reporting requirements target and burden speech without furthering the government's interests.

The ease with which individuals can adopt new Internet identifiers or access public WiFi also means that these provisions are unlikely to further any legitimate goal, because a registrant who wants to commit an online crime will simply create a new identifier and then not report it. In this situation, a registrant can likely invoke the Fifth Amendment and refuse to report the incriminating information. *See Garner v. United States,* 424 U.S. 648, 651-53, 662-63 (1976) (taxpayer can refuse to provide incriminating information on tax returns). In any event, it is unlikely that a registrant who created a new identifier or account to use to commit a human-trafficking or sex crime would feel constrained to comply with the Act's reporting requirements. *See Marion Cnty.*, 705 F.3d at 701 ("if they are willing to break the existing anti-solicitation law, why would the social networking law provide any more deterrence?"); *cf. Watchtower Bible*, 536 U.S. at 168-69. This is particularly true because a quirk of California law means that a person who is convicted of a registration violation along with a more serious felony can serve at most an additional eight months for the registration violation, as opposed to the three-years (or more) that a registrant would face for failing to report an identifier or ISP used only for lawful speech. *See People v. Neely*, 176 Cal. App. 4th 787, 797-98 (2009); § 290.018(b).

It is thus not surprising that Appellants have been unable to identify a single case in which other states' laws have ever assisted in solving a crime. ER10 & n.10. But if the Act goes into effect there will undoubtedly be numerous registrants who are arrested and incarcerated for failing to report identifiers they used for lawful, constitutionally protected speech.

The Act also lacks utility because it is under-inclusive in several significant ways. First, it explicitly excludes "libraries and educational institutions" from its definition of ISPs that must be reported, despite the fact such facilities not only provide identical Internet access as do Internet cafés but may offer greater physical proximity to children. Act, ch. 8, § 13, § 290.024(a). Second, it applies only to registrants, even though the overwhelming majority of technology-facilitated sex crimes are not committed by registered sex offenders. Only 4% of persons arrested for technology-facilitated sex crimes against youth were registered sex offenders, and only 2% of those arrested for soliciting undercover investigators were registered sex offenders. ER422. Finally, it excludes instant messaging that is not transmitted over the Internet. ER511. This under-inclusivity further undercuts the government's arguments that the Act is narrowly tailored. *See Valle Del Sol*, 709 F.3d at 828.

* * *

In short, the statute is unconstitutional because it prohibits protected anonymous speech and burdens a huge amount of speech by all registrants but is not tailored to address the state's interests in preventing sex offenses and human trafficking. Even if its vague terms are construed narrowly,[22] the government has failed to prove that it is narrowly tailored to the speech or speakers that give rise to the purported dangers the statute seeks to address.

F. The Act Is Facially Invalid Both Because It Lacks Narrow Tailoring And Because It Is Overbroad

A law that lacks narrowly tailoring is facially unconstitutional. *See Comite*, 657 F.3d at 936. Similarly, a statute is facially unconstitutional if it is substantially overbroad, meaning that it "prohibit[s] or chill[s] "a substantial amount of protected speech." *Ashcroft,* 535 U.S. at 237. The standards for determining whether a law is overbroad are substantially the same used to determine whether a law is narrowly tailored under intermediate scrutiny; therefore, a law that fails that

[22] This Court cannot rewrite the statute to cure its infirmities. *See Comite,*657 F.3d at 946-47; Part III, *infra*. Nor can it "accept[] as 'authoritative' [the] Attorney General's interpretation of state law when," as here, "the Attorney general does not bind the state courts or local law enforcement authorities." *Stenberg v. Carhart,* 530 U.S. 914, 941 (2000) (citation omitted); ER0019. Third, and as the district court observed, a federal court's "interpretation is not binding on state courts, where the registrants would face prosecution for failure to register." ER0014.

test will also be overbroad. *See Bd. of Trs. of State Univ. of New York v. Fox*, 492 U.S. 469, 482-83 (1989); *Marion Cnty.*, 705 F.3d at 701-02, n.6.[23]

The Act is overbroad for the same reasons that it is not narrowly tailored: it affects an enormous amount of perfectly legal, constitutionally protected online speech that has absolutely no connection to its goals of protecting children or preventing human trafficking. It is therefore facially invalid under both doctrines.[24]

III. The Definitions Of "Internet Service Provider" And "Internet Identifier" Are Unconstitutionally Vague

The Act is unconstitutional on independent vagueness grounds. A law "is void for vagueness if its prohibitions are not clearly defined." *Hunt v. City of Los Angeles*, 638 F.3d 703, 712 (9th Cir. 2011) (citations omitted). This rule ensures that "regulated parties … know what is required of them" and also that "those enforcing the law do not act in an arbitrary or discriminatory way." *F.C.C. v. Fox Television Stations, Inc.*, 132 S.Ct. 2307, 2317 (2012); *see City of Chicago v. Morales*, 527 U.S. 41, 56 (1999) (plurality). "[W]here criminal sanctions are involved and/or the law implicates First Amendment rights such as here, a more demanding standard of scrutiny applies." *Hunt*, 638 F.3d at 712. Neither the

[23] The overbreadth doctrine differs from intermediate scrutiny in that it relaxes standing requirements. *See Fox*, 492 U.S. at 483-84.

[24] As mentioned above, the government stipulated that preliminary injunctive relief will cover all registrants. SER005.

federal courts nor the Attorney General can rewrite a vague state law to make it constitutional. *Hynes*, 425 U.S. at 622; *Stenberg*, 530 U.S. at 941-41; *see Stevens,* 130 S.Ct. at 1591-92.

A. The Act's Definition Of "Internet Identifier" Is Vague

An "Internet identifier" under the Act is "any 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 communications." Act § 13, § 290.024 (b). The initial problem with this definition is that the Act does not define "chat rooms," "instant messaging," "Internet forum discussion[s]" or "social networking," and there are multiple, and inconsistent, definitions of these terms in common use. ER507-511. For example, a simple blog could qualify as a "social networking website" under a federal definition, but not one commonly used by academics; conversely, a professional network such as LinkedIn would qualify as a "social network site" under the academic but not the federal definition. ER509-10 n.5. The lack of definitions for these terms alone means that registrants who create a screen name to engage in any number of online activities simply have no way to know whether they must report them. ER511.

Moreover, it is unclear whether "used for the purpose of" modifies all of the listed terms (email address, user-name, screen-name) or "similar identifier." If it

only modifies "similar identifier," then registrants must report *all* user-names or screen-names they use for any purpose, exacerbating the Act's overbreadth. If, however, it modifies all of the terms, then email addresses would be exempt unless the registrant uses them for one of the listed purposes, which seems to contradict the government's apparent reading of the law. ER0093-94, 354. The only way to avoid this conclusion would be to construe "similar Internet communications" to include *all* Internet communications, which would render much of the definition surplussage and would again mean that registrants would have to report essentially all user- and screen-names they use for any type of online communication.

Intervenors' and the government's attempts to clarify this definition at the preliminary-injunction hearing highlight the law's vagueness. After suggesting registration is required only for identifiers used for "interactive communications between a registrant and other members of the public" – a limitation that does not appear in the statute – they supported their claim that the law is narrowly tailored by asserting that interactive chat-room discussions with an online help service should not be covered because that would be "absurd," even though such discussion are plainly covered by the statutory language. ER083-84; *see id.* at 053-57, 509. But how are registrants supposed to know which of the Act's applications are so absurd that they can disregard them? As Professor Post makes clear, the statutory language itself is ambiguous. ER505-511. The discussion on the

California Reform website makes clear that registrants were completely unable to determine what they would have to report if the Act passed. ER542-57. Adding an absurdity exception only exacerbates this problem.

B. The Act's Definition Of "Internet Service Provider" Is Vague

The Act defines ISP as "any business, organization, or other entity providing directly to consumers a computer and communications facility through which a person may obtain access to the Internet." Act § 13, § 290.024(a). Even if, as the District Court held, the Act requires reporting only of ISPs the registrant currently has an account with, ER009, it is unconstitutionally ambiguous.

For example, it is impossible to know whether a registrant who uses his roommate's ISP account must report it. Section 290.015(a)(5) requires reporting of all ISP's "used" by a registrant, but § 290.014(a) only requires updating of the *registrant's* account. Similarly, a registrant who logs onto an Internet café's WiFi service is clearly using that café's ISP account, ER514, but the registrant himself may not have an account. ER514-15. Intervenors suggest that registrants need not report this usage. ER095. And this makes sense, because it may be impossible for a registrant to report this information. ER00513-14. But this is contrary to the statutory language, and if it were correct there would be no need for the exception for libraries, which are the functional equivalent of Internet cafés. ER514-15. And if a registrant obtains a one-time password to access a café's or hotel's Internet

connection, is that an "account" that must be disclosed? As Professor Post explains, these and other ambiguities in the Act's idiosyncratic definition of ISP make it impossible for registrants to know what they must do to comply. ER512-18.[25]

C. The Government's Proposed Solutions Cannot Cure This Problem

The government claims it will cure this vagueness by creating registration forms. ER354-55. But the Act does not require registrants merely to fill out a form; it requires them to submit "[a] list of any and all Internet identifiers" and "[a] list of any and all" ISPs. § 290.015(a)(4), (5). It also requires them to "send written notice" of any changes within 24 hours. § 290.014(b). Even if the government could develop some sort of form that would provide more concrete definitions, they have not done so yet, and no governmental form can override the statutory mandate so as to cure the vagueness problems. *See Hynes,* 425 U.S. at 622 n.6. The government's admission that it must create a form to explain what registrants must report confirms the statute's vagueness. *See Stevens*, 130 S.Ct. at 1591.

[25] That the term ISP has a widely accepted meaning is of no help because the statutory definition conflicts with that meaning. ER0516; *see Morales*, 527 U.S. at 56-67. The term "Internet identifier" has no standard definition. ER0137, 0151.

Nor can the government's suggestion that registrants talk with the police about what they must report save the statute. ER070-72. First, this is not practicable, because the 24-hour reporting requirement means that a registrant who wanted to do this would have to go to the police station every time he was considering commenting on a new website, which would require creating a new identifier, or using what might be an ISP. To get any guidance, he would then have to discuss with the police exactly what he was going to do or had done online. This would effectively mean forfeiting anonymity even if the officer decided that no reporting was necessary. Finally, this procedure would mean that the determination of whether the registrant had to turn over his identifier or ISP would depend on a single police officer's interpretation of the law, allowing precisely the possibility of "arbitrary or discriminatory" application of the law by a single officer that the vagueness doctrine guards against. *Fox Television,* 132 S.Ct. at 2317 (2012). Statutes, particularly criminal statutes affecting speech, cannot delegate "responsibilities for setting the standards of the criminal law" to the police in this way. *Smith v. Goguen*, 415 U.S. 566, 575 (1974); *see Hynes*, 425 U.S. at 622; *Hunt*, 638 F.3d at 712 & n.4. The government cannot require speakers to meet with the police to determine whether their speech will subject them to criminal liability. *See Citizens United*, 558 U.S. at 335-36; *cf. Morales*, 527 U.S. at 58-59 (police "notice" as to legality of conduct cannot cure vagueness).

In many respects, the Act is much like the ordinance at issue in *Hynes*, which required certain solicitors to provide the police with notice "for identification only." *Hynes*, 425 U.S. at 612-13. As with the Act, they could do this by mail, and they only needed to provide notice once for any campaign or cause. *See id*. at 613, 622. They did not have to provide any information about the nature of their solicitation. The Court held that the law was unconstitutional vague because it did "not explain either what the law covers or what it requires," notwithstanding the enforcing agency's narrowing construction. *Id.* at 621-23. Similarly, the Court has invalidated registration requirements for members of "subversive organizations" where the law was vague as to what organizations were included. *Dombrowski*, 380 U.S.at 492-94.

The Act suffers from these same problems, problems that are magnified by the harsh penalties for non-compliance. Its vagueness both exacerbates its First Amendment overbreadth and renders it facially invalid under the Fourteenth Amendment.

IV. The Other *Winter* Factors Support The Injunction

Aside from the merits, Appellants' sole claim is that the balance of hardships weighs against an injunction. But the District Court carefully examined the evidence and found that the "substantial chilling of Plaintiffs' First Amendment rights" outweighed the "weak showing of the [Act's] utility."

ER0018-19. This was well within its discretion. *See Melendres v. Arpaio*, 695 F.3d 990, 1002 (9th Cir. 2012) ("it is always in the public interest to prevent the violation of a party's constitutional rights"); *Thalheimer*, 645 F.3d at 1129.

CONCLUSION

This Court will affirm the grant of a preliminary injunction protecting constitutional rights even if Plaintiffs have merely shown that the "constitutional question is close." *Id.* at 1128 (citation omitted). Because the Act violates both the First and the Fourteenth Amendment, this Court should affirm.

DATED: May 8, 2013

Respectfully submitted,

By: */s/ Michael T. Risher*

Michael T. Risher
Linda Lye
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111

Hanni Fakhoury
Lee Tien
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Counsel for Plaintiffs-Appellees JOHN DOE, et al.

Case Nos. 13-15263, 13-15267

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

JOHN DOE, *et al*.,
Plaintiffs - Appellees,
v.
DAPHNE PHUNG, *et al*.,
Intervenors - Appellants,
KAMALA D. HARRIS, Attorney General of the State of California,
Defendant- Appellant.

STATEMENT OF RELATED CASES

To the best of our knowledge, there are no related cases.

DATED: May 8, 2013

Respectfully submitted,

By: */s/ Michael T. Risher*
Michael T. Risher

Michael Risher
Linda Lye
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111

Hanni Fakhoury
Lee Tien
ELECTRONIC FRONTIER
815 Eddy Street
San Francisco, CA 94109

Counsel for Plaintiffs-Appellees JOHN DOE, et al.

**CERTIFICATE OF COMPLIANCE
WITH TYPE-VOLUME LIMITATION,
TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS
PURSUANT TO FED. R. APP. P. 32(a)(7)(C)**

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. Appellees' Opening Brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 13,989 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

DATED: May 8, 2013

Respectfully submitted,

By: */s/ Michael T. Risher*

Michael T. Risher
Linda Lye
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111

Hanni Fakhoury
Lee Tien
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Counsel for Plaintiffs-Appellees
JOHN DOE, et al.

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on May 8, 2013.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

DATED: May 8, 2013

Respectfully submitted,

By: */s/ Michael T. Risher*

Michael T. Risher
Linda Lye
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA, INC.
39 Drumm Street
San Francisco, CA 94111

Hanni Fakhoury
Lee Tien
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Counsel for Plaintiffs-Appellees JOHN DOE, et al.