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.

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

OPENING BRIEF OF DEFENDANT-APPELLANT

KAMALA D. HARRIS
Attorney General of California
DOUGLAS J. WOODS
Senior Assistant Attorney General
PETER K. SOUTHWORTH
Supervising Deputy Attorney General

ROBERT D. WILSON
Deputy Attorney General
State Bar No. 136736
1300 I Street, Suite 125
P.O. Box 944255
Sacramento, CA 94244-2550
Telephone: (916) 327-7870
Fax: (916) 324-8835
Email: Robert.Wilson@doj.ca.gov
Attorneys for Defendant and Appellant Kamala D. Harris, Attorney General of California

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES
(continued)

Page

STATUTES

TABLE OF AUTHORITIES
(continued)

Page

PRELIMINARY STATEMENT

The Attorney General of California joins in the intervenors' opening brief, in which they demonstrate that the First Amendment is not implicated by Proposition 35, the Californians Against Sexual Exploitation Act (CASE Act or Act). Any purported chilling effect on a sex offender registrant's speech is hypothetical, remote, and incidental to the CASE Act's intent and effect of deterring and helping investigate sex crimes involving the Internet. We write separately to explain how the district court erred in ruling that the perceived danger of disclosure of a registrant's Internet identifier information, combined with the penalties a registrant faces for failure to comply with the Act's reporting requirements, in its view creates too great a chilling effect to pass First Amendment muster.

JURISDICTIONAL STATEMENT

The district court has subject matter jurisdiction over plaintiffs' claims pursuant to 28 U.S.C. §§ 1331, 1343. This is an appeal from an order granting plaintiffs' motion for a preliminary injunction, and this Court has jurisdiction under 28 U.S.C. § 1292(a)(1). The district court entered the preliminary injunction on January 11, 2013. Pursuant to Rule 4 of the Federal Rules of Appellate Procedure, the California Attorney General and

intervenors timely filed their notices of appeal on February 11, 2013. Excerpts of Record (ER) 0114-0120.

QUESTIONS PRESENTED

1. Whether the district court erred by examining the purported chilling effect of the CASE Act in isolation from other provisions of California's Sex Offender Registration Act, which restrict law enforcement's use of a registrant's information to legitimate law enforcement uses and instances in which public safety needs authorize limited public disclosure?

2. Whether the district court erred in ruling that the penalties for failing to register specific information under the Sex Offender Registration Act, as potentially applied to reporting of Internet identifiers, creates too much uncertainty (and hence a chilling effect) when (a) the act of registering information necessarily involves interaction with law enforcement about the registration process and requirements, (b) California law requires for conviction that a registrant must have failed to provide information he or she knows is required, and (c) California had been collecting Internet information from registered sex offenders for more than a year prior to the passage of the CASE Act without any complaints about those requirements?

STATEMENT OF THE CASE

On November 6, 2012, California voters approved Proposition 35, the CASE Act, with approximately 81% of the vote. ER 0001. The following day, when the Act was to take effect, plaintiffs John Doe, Jack Roe, and the non-profit organization California Reform Sex Offender Laws filed this action as a facial overbreadth challenge on behalf of present and future California sex offender registrants. *See* Cal. Const. art. II, § 10(a); ER 0595-0614. They contend that California Penal Code sections 290.014(b) and 290.015(a)(4)-(6), as enacted by Proposition 35, violate plaintiffs' First Amendment rights to engage in anonymous online speech. The district court granted plaintiffs' motion for a temporary restraining order on November 7, 2012. ER 0358-0361.

Chris Kelly and Daphne Phung, the proponents of Proposition 35, moved to intervene on November 12, 2012. The district court granted the motion on January 10, 2013.

The district court granted plaintiffs' motion for a preliminary injunction on January 11, 2013. ER 0001-0021. The district court determined that the CASE Act implicated registered sex offenders' First Amendment right to speak anonymously online. ER 0012-0014. Although the trial court construed the challenged provisions narrowly to avoid many

of plaintiffs' overbreadth challenges, and further concluded that the Act would further the government's legitimate interests, it nevertheless concluded that the measure applied to too many sex offenders and too much speech to survive intermediate scrutiny. ER 0007-0010. The district court also ruled that insufficient protections in the Act against disclosure of a registrant's Internet identifier information and the penalty a registrant may face if he or she fails to comply with the CASE Act's reporting requirements create too great a chilling effect to pass constitutional muster. ER 0017.

The California Attorney General and intervenors timely appealed. ER 0114-0120.

STATEMENT OF FACTS

The Sex Offender Registration Act, California Penal Code sections 290-294, mandates that certain persons convicted of specified sex offenses are required to register with specified law enforcement agencies. The law "assure[s] that persons convicted of the crimes enumerated therein shall be readily available for police surveillance at all times because the Legislature deemed them likely to commit similar offenses in the future." *In re Alva*, 33 Cal. 4th 254, 264 (2004). As applicable here, the law "simply requires a convicted offender to provide, and to update at specified intervals, information logically calculated to assist law enforcement authorities to

monitor his or her whereabouts, while it protects the offender's privacy by carefully restricting the public dissemination of this information." *Id*. at 289. "Given the 'frightening and high' danger of long-term recidivism by this class of offenders, the requirement has a legitimate regulatory aim." *Id*. (quoting *Smith v. Doe*, 538 U.S. 84, 103 (2003)).

Prior to release or parole from a jail, prison, or other place of confinement, any person subject to sex offender registration is informed of their duty to register.[1] ER 0323 (Schweig Decl., ¶ 6); Cal. Penal Code § 290.017(a). The person must read and sign a form required by the California Department of Justice (DOJ), stating that the duty been explained to the person. *Id.* The official in charge of the place of confinement or hospital obtains the address where the person expects to reside upon release and reports it to DOJ. *Id*. Copies of the completed form are given to the person and sent to DOJ and the appropriate law enforcement agency or agencies having jurisdiction over the place the person expects to reside upon discharge, parole, or release. *Id.* § 290.017(b). The released person then has five working days to register (or re-register under certain circumstances if

[1] A more detailed description of the process is found in Defendant-Appellant's Opposition to Plaintiffs' Motion for a Preliminary Injunction. *See* ER 0344-0350.

previously registered). *Id.* § 290.015(a). The offender must register with either the police department or sheriff's office, based on their residence. *Id.* § 290(b). Thereafter, the registrant must annually register and update the required information within 5 working days of their birthday or, if they are transient, every 30 days. *Id.* § 290.15(a), (c).

Immediately prior to the passage of the CASE Act, the Sex Offender Registration Act required that the registration consist of: (1) a written statement giving information as shall be required by DOJ and giving the name and address of the person's employer, and the address of the person's places of employment; (2) fingerprints and a current photograph; (3) license plate number of any vehicle owned by, regularly driven by, or registered in the name of the person; (4) notice to the person that they may have a duty to register in any other state if they relocate; and (5) copies of adequate proof of residence. Former Cal. Penal Code §§ 290.012(a), 290.015(a). If the person has no residence and no reasonable expectation of obtaining one in the foreseeable future, the person can state that fact in writing. Cal. Penal Code § 290.015(a)(5).

Pursuant to DOJ's authority to require additional information on the registration form, DOJ started collecting Internet information from registrants in June, 2011 (more than a year prior to the passage of the CASE

Act) concerning their email addresses and screen names/social networks. ER 0324-0325 (Schweig Dec., ¶ 13). Specifically, the DOJ registration form used by local law enforcement had fields to report "E-MAIL ADDRESS" and "SCREEN NAME(S)/SOCIAL NETWORK(S)." ER 0329 (Schweig Decl., Exh. A, p. 1 of 4.) Plaintiff Jack Roe acknowledges that he was required to provide this information to the sheriff's department when he registered prior the passage of the CASE Act, in September, 2012. ER 0555 (Roe Decl., ¶ 21).[2]

The CASE Act amended the above-described Penal Code sections 290.012 and 290.015 to expressly require that Internet identifying information be collected during the registration process. Specifically, it added three items to the list of identifying information that must be collected from a registrant during the initial and periodic update registrations: (1) a list of any and all Internet identifiers established or used by the person, (2) a list of any and all Internet service providers used by the person, and (3) a signed statement acknowledging that the registrant is required to register and

[2] At the time this action was filed and a temporary restraining order entered, DOJ was working to fully integrate the Internet information collected by local law enforcement into law enforcement telecommunications and software systems. ER 0324-0325 (Schweig Dec, ¶¶ 13-14).

update that information, as required by the Sex Offender Registration Act. Cal. Penal Code §§ 290.012(a) (amended eff. Nov. 7, 2012), 290.015(a)(4)-(6) (added eff. Nov. 7, 2012). In addition, the Act requires a registrant to notify registering agencies of any changes to their Internet identifiers within 24 hours. *Id.* § 290.014(b) (eff. Nov. 7, 2012). This was added to the existing requirement that a registrant promptly inform his or her registering agency of any name change. *Id.* § 290.014(a).

With the exception of certain limited disclosure discussed below, registrant information collected under the Sex Offender Registration Act is not open to inspection by the public or any person, other than a regularly employed peace officer or other law enforcement officer. Cal. Penal Code § 290.021; *see* Cal. Gov't Code § 6254(f). DOJ maintains access to that information through secure law enforcement telecommunications systems and requires standard acknowledgment of a law enforcement user's "need to know, right to know" before access is permitted. ER 03234-0325 (Schweig Dec., ¶¶ 11-13.) DOJ or the local law enforcement agency can investigate and take appropriate action to remedy any unauthorized access. *Id.* In her 20 years with DOJ, the current Program Manager for the Violent Crime Information Center is not aware of any report or investigation of any improper request to query the sex offender information database. *Id.*

The Sex Offender Registration Act permits limited disclosure of information on a specific registrant, potentially including Internet identifying information, to certain members of a community for public safety reasons. Cal. Penal Code § 290.45. Under that statutory provision, any law enforcement entity "may provide information to the public about a person required to register as a sex offender pursuant to Section 290, by whatever means the entity deems appropriate, when necessary to ensure the public safety based upon information available to the entity concerning that specific person." *Id.* § 290.45(a)(1). The disclosure must be accompanied by a statement that the purpose of the release of information is to allow members of the public to protect themselves and their children from sex offenders. *Id.* § 290.45(a)(2). The paradigm of this public notification is providing neighbors information about a high risk sex offender through a law enforcement "knock and talk" or leaflet. Information not already disclosed on the statewide public Megan's Law website cannot be released on the Internet unless there is a warrant outstanding for that person. *Id.* § 290.45 (a)(3). Registrant Internet information is not on the Megan's Law public website, which is governed by Penal Code section 290.46, and that website is not implicated in this action.

A law enforcement entity may authorize persons and entities who receive the information under Penal Code section 290.45 to disclose it to additional persons only if the entity determines that further disclosure will enhance the public safety, and identifies the appropriate scope of further disclosure. Cal. Penal Code § 290.45(c)(1). A law enforcement entity may not authorize such further disclosure by its placement on an Internet website. *Id*. A person who receives such information may disclose that information only in the manner and to the extent authorized by the law enforcement entity. *Id.* § 290.45(c)(1). There are criminal penalties for improper use of the disclosed information. *Id.* § 290.45(e). Civil immunity for private parties is only extended to schools and childcare facilities and their employees and only covers authorized, good faith dissemination of the information. *Id*. § 290.45(d)(2).

The CASE Act sets forth the basic policy underlying the requirement that registrants provide Internet information, noting the purpose of strengthening sex offender registration requirements is "to allow law enforcement to track and prevent online sex offenses." ER 0009 (Prop. 35, § 3, ¶ 3). Having this Internet identifying information does not permit law enforcement access to, or monitoring of, private communications. ER 0335 (Morgester Dec., ¶ 9). Under both federal and California law (which is

sometimes more restrictive), judicial authorization is required to access private communications or even basic subscriber information associated with an email account. ER 0335 (Morgester Dec, ¶¶ 9-10.) Moreover, a number of social media sites already bar registered sex offenders, deriving their identity from publically-available records. ER 0336 (Morgester Decl., ¶ 13).

SUMMARY OF ARGUMENT

The district court reasoned that the lack of protections on the disclosure of a registrant's Internet identifier information and the penalty for failure to register that information create too great a chilling effect to pass First Amendment overbreadth muster. This conclusion rests on at least three errors.

First, a critical part of the district court's analysis was the overall restriction in the California Sex Offender Registration Act on dissemination of registrant information, including any Internet identifying information. Instead, the trial court examined the challenged provisions in isolation from the entire statutory scheme, including other provisions that place narrow limitations and significant conditions on public disclosure of any information. The district court also incorrectly presumed that law

enforcement would access the information and disseminate it to the public without sufficient cause.

Second, the district court incorrectly overstated the potential chilling effect of the CASE Act arising from the registrants' hypothetical uncertainty about the specific information subject to registration and a concomitant fear of prosecution for failure to register items. This reasoning overlooked California law, established both in the Sex Offender Registration Act and case law, that scienter is a prerequisite to prosecution for failure to register specific information. In addition, except in a very limited circumstance, a registrant must appear personally before the relevant law enforcement entity to register. The possibility that a registrant with questions about the required information would be prosecuted for willfully omitting that information is greatly diminished by the very nature of the mandated interaction with law enforcement personnel.

Third and finally, California had been collecting Internet information from registered sex offenders for more than a year at the time the lawsuit was filed, yet the record was devoid of any claim up to that time by any person in California that his or her expressive activity was even *potentially* chilled. It was an abuse of discretion for the district court to base its decision on theoretical effects from the Act, especially when experience has

shown the absence of such effects over more than one full annual registration cycle in which Internet identifying information was collected from registrants.

STANDARD OF REVIEW

Although a district court's decision to grant a preliminary injunction is reviewed for abuse of discretion, its interpretation of the underlying legal principles is subject to de novo review. *Southwest Voter Registration Educ. Project v. Shelley*, 344 F.3d 914, 918 (9th Cir. 2003). A preliminary injunction must be supported by findings of fact. *See Independent Living Ctr. of S. California, Inc. v. Shewry*, 543 F.3d 1050, 1055 (9th Cir. 2008); *Hawkins v. Comparet-Cassani*, 251 F.3d 1230, 1239 (9th Cir. 2001). A district court "necessarily abuses its discretion when it bases its decision on an erroneous legal standard or on clearly erroneous findings of fact." *Johnson v. Couturier*, 572 F.3d 1067, 1078-79 (9th Cir. 2009).

ARGUMENT

I. THE DISTRICT COURT ERRED AS A MATTER OF LAW IN EXAMINING THE PURPORTED IMPACT OF THE CASE ACT WITHOUT CONSIDERING IT IN THE CONTEXT OF THE ENTIRE CALIFORNIA SEX OFFENDER REGISTRATION ACT.

The district court observed that "[b]efore determining whether a challenged provision violates the First Amendment, a court must first construe the provision: 'It is impossible to determine whether a statute reaches too far without first knowing what the statute covers.' " ER 0007 (citing, *United States v. Williams*, 553 U.S. 285, 293 (2008)). "What the statute covers" cannot be accurately determined if the statute is examined in isolation from its surrounding statutory scheme. If the assessment about what the statute covers (and does not cover) is wrong or incomplete, a court cannot reach an accurate conclusion about whether the challenged provision violates the First Amendment. In this case, the district court examined the potential impact of the CASE Act in virtual isolation from existing Penal Code provisions which significantly narrow the possibility that a registrant's Internet Service Provider and Internet identifier information would ever be publically disclosed and, if it were, which severely confine the extent of that disclosure.

The district court acknowledged that sex offender registration information is only available to law enforcement personnel (Cal. Penal Code § 290.021), but focused on the provision of Penal Code section 290.45 permitting a law enforcement entity to disclose registrants' information to the public "when necessary to ensure the public safety based upon information available to the entity concerning that specific person." ER 0012; *see* Cal. Penal Code § 290.45(a)(1). The trial court ignored, however, the concomitant legal limitations on access and use of registrants' information both under section 290.021 and as applicable to "community notification" under section 290.45.

The district court concluded that these two provisions do not contain the safeguards that are now present in Utah statutes that were amended after they were initially found unconstitutional in *Doe v. Shurtleff*, Case No. 1:08-CV-64-TC, 2008 WL 4427594 (D. Utah Sept. 25, 2008). ER 0012-0013. The trial court was wrong on both statutes.

A. The district court incorrectly presumed law enforcement would improperly use Internet identifying information accessible under Penal Code section 290.021.

On the question of law enforcement access generally, the Utah statute at issue in the *Shurtleff* litigation was amended to specify that the purpose for collecting and distributing registrant internet information was to "assist

in investigating kidnapping and sex-related crimes, and in apprehending offenders." *Doe v. Shurtleff,* 628 F.3d 1217, 1221 (10th Cir. 2010). In evaluating the amended statute, the Tenth Circuit construed it in light of this purpose and proceeded based thereon to uphold the amended Utah law. *Id*. at 1225. The district court here did not similarly consider a narrowing interpretation of the CASE Act based on the California law's parallel statement of purpose "to allow law enforcement to track and prevent online sex offenses." Prop. 35, § 3, ¶ 3; ER 00009.

Instead, citing *Comite de Jornaleros de Redondo Beach v. City of Redondo Beach*, 657 F.3d 936, 946-47 (9th Cir. 2011), the trial court refused to presume that law enforcement would act in good faith and adhere to standards not expressly included on the statutes' face. ER 0013. In *Comite*, a city argued that an ordinance that on its face applied broadly would be only enforced in a narrower set of circumstances. 657 F.3d at 946-47. But that argument contradicted the city's assertions about enforcement of the ordinance in the district court. *Id.* at 947. Under those circumstances, the court properly declined simply to presume the city would act in good faith and adhere to standards that did not exist. *Id.* at 946-47. It is this authority upon which the district court here rested its rejection of the Attorney General's contention that law enforcement in California can not use

registrant information without some nexus to a criminal investigation. ER 0013.

But legal limits on law enforcement use of confidential information and a city's representation that an ordinance would not be fully enforced are two distinct matters. It is not a question here of law enforcement representing how that agency will enforce the law. Instead, to conduct investigation or surveillance, "specific and articulable facts causing the officer to suspect that some activity relating to crime has taken place or is occurring or about to occur" are *required* and the suspicion "that the person he or she intends to place under surveillance is involved in that activity" is also *required*. 42A Cal.Jur 3d Law Enforcement, § 155 at 226-27 (2012). Moreover, the suspicion must be objectively reasonable. *Id.* Investigation predicated on mere curiosity, rumor, or hunch is unlawful, even though the officer may be acting in complete good faith. *Id.* at 227.

Thus, the Attorney General's argument that law enforcement should not be presumed to access and use registrants' information without a nexus to criminal activity is very unlike the city's assertion in *Comite* that it simply would not enforce an ordinance that on its face applied to certain activity. The district court should have declined to presume that law enforcement would access and use Internet identifying information without the

appropriate nexus, and the *Comite* opinion provides no support for its decision to the contrary.

B. The district court ignored restrictions on disclosure for public safety grounds under Penal Code section 290.45.

The district court likewise incorrectly ignored the restrictions of Penal Code section 290.45 that the release of information about a specific a registrant be only to ensure public safety.

The relevant restrictions, detailed above in the Statement of Facts on pages 9-10, would preclude: (a) the disclosure of any Internet identifying information on the Internet (save in the circumstances where a warrant is outstanding for that person), (b) further dissemination of the information by the community members notified, and (c) misuse of the information by the persons receiving the information. Any permissible disclosure must include "a statement that the purpose of the release of information is to allow members of the public to protect themselves and their children from sex offenders." ER 0012; *see* Cal. Penal Code § 290.45(a)(2). The district court nonetheless predicted widespread disclosure, citing the reasoning of *White v. Baker*, 696 F. Supp. 2d 1289 (N.D. Ga. 2010), that

> [i]t is conceivable, if not predictable, that a person in law enforcement might determine that Internet Identifiers for offenders ought to be released so that the public can search for and monitor communications

> which an offender intends to be anonymous. That these anonymous communications might well be on a matter of public policy, political speech, or other protected speech squarely implicates the First Amendment. . . . The prospect that Internet Identifiers, as currently defined, may be released to the community has an obvious chilling effect." ER 0012-0013.

Under California law, such general release of information based on such a sweeping rationale is impermissible, absent particular circumstances under which such monitoring was legitimately related to public safety concerns regarding a particular individual.

Accordingly, the *White v. Baker* decision likewise provides no support for the district court's decision.

C. The district court examined the CASE Act without considering the distinctions between the registration and notification provisions of the Sex Offender Registration Act.

During oral argument, the Attorney General drew an important distinction between the purpose of the CASE Act and the purpose of the risk assessment tool California presently uses to assess registered sex offenders. ER 0097-0098. The CASE Act is a registration statute which helps law enforcement locate a registrant in cyberspace if such need should arise. In contrast, the purpose of the risk assessment tool is to provide a way to assess the risk of danger and re-offense a particular registrant poses so that

members of the public, through the notification process, may be better informed as to the degree of need to take steps to protect themselves and their children from harm. *See*, *e.g.*, *Smith v. Doe*, 538 U.S. 84, 90 (2003) (distinguishing between registration law and notification law).

The distinction is, moreover, directly related to the *scope* of the CASE Act. When viewed as what it is -- a registration statute -- the sweep of the CASE Act is broad (but no broader than already existing registration laws) in terms of *who must provide information*. All registrants must comply because no one safely knows who will re-offend or when such offense might come. The Penal Code provisions that govern *public notification*, on the other hand, are narrow, and it is highly unlikely any particular registrant's Internet information will ever find its way to the public. So, the impact of the CASE Act is extremely small in terms of what the public would ever see.[3]

And this is an additional reason the decisions in *Doe v. Shurtleff*, 628 F.3d 1217 (10th Cir. 2010), and *White v. Baker*, 696 F. Supp. 2d 1289 (N.D. Ga. 2010), do not support the district court's decision. Unless Utah and

[3] For this additional reason, the fact that the CASE Act, as a *registration* statute, does not contain on its face restrictions on the *public disclosure* of the information registered is a non-issue.

Georgia have statutory schemes identical to California's, and there is no suggestion in the opinions that they do, the concern expressed by the courts in *Shurtleff* and *White* about public disclosure protections in their respective registration statutes is of no legal consequence here. The district court invalidated the Case Act registration requirements on the invalid grounds that it did not itself contain express protections against improper notifications, and did so without fully assessing the protections already existing under California law. This was error.

D. The district court ignored the Legislature's consideration of the concerns of registrants versus the public's need for information and how that balance is implemented in the Act.

Penal Code section 290.03 sets forth three important components of how the entire Sex Offender Registration Act is structured and applied. First, the State of California has a compelling and necessary public interest in the public's access to limited information concerning certain persons convicted of offenses involving unlawful sexual behavior. Cal. Penal Code § 290.03(a)(2). Second, the information made publicly available cannot be used to harm any registrant. Cal. Penal Code § 290.03(a)(7). Third, having weighed the competing interests, the Legislature concluded that the danger

to the public from nondisclosure far outweighs any risk of possible misuse. *Id*.

The district court, and plaintiffs, acknowledged that the State of California indeed has a compelling interest in protecting the State's children from predators on the Internet. ER 0009-0010. Section 290.03 declares that in furtherance of that interest, the State has "a compelling and necessary interest that the public have information concerning persons convicted of offenses involving unlawful sexual behavior pursuant to Sections 290 and 290.4 to allow members of the public to adequately protect themselves and their children from these persons." Cal. Penal Code § 290.03(a)(2).

Various specific provisions of the Sex Offender Registration Act show how the Legislature balanced the protection of the public against the interests of the registrants. Information about low and moderately-low offenders is limited to written inquires to DOJ asking whether that person is subject to registration. *See* Cal. Penal Code § 290.4. Information available regarding serious and high-risk offenders varies, depending upon risk assessment scores. Cal. Penal Code § 290.46(e)(4). General community notification is permitted only in conjunction with "high-risk offenders who are about to be released from custody or who already reside in communities in this state." Cal. Penal Code § 290.03(a)(6).

The Legislature also provided that the information cannot be used to inflict retribution or additional punishment on any person convicted of a sex offense. Cal. Penal Code § 290.03(a)(7). This concern is reflected in the criminal and civil penalties for misuse, and other restrictions, found in Penal Code sections 290.4 and 290.46.

Lastly, the Legislature considered arguments that the information might be misused. Cal. Penal Code § 290.03(a)(7). It concluded, however, that:

> the dangers to the public of nondisclosure far outweigh the risk of possible misuse of the information" as evidenced by studies in Oregon and Washington which indicated that "community notification laws and public release of similar information in those states have resulted in little criminal misuse of the information and that the enhancement to public safety has been significant.

Id. Thus, the Legislature balanced concerns of registrants against the "paramount" need to protect vulnerable members of the public against heinous crimes. It achieved that balance by limiting the categories of offenders who may be subject to *general* community notification and restricting the information that may be disclosed to the public about them by category.

There is no reason to presume, as did the district court here, that law enforcement will ignore this balance and decide to engage in any widespread

dissemination of a registrant's Internet information, without regard to classification, under the guise of "ensur[ing] the public safety based on information available . . . concerning that specific person" pursuant to Penal Code section 290.45. To be sure, under the CASE Act law enforcement may provide limited information to a discrete group of potentially affected citizens, including Internet identifying information, if the police have particularized information that indicates such information should be shared. Unlike notification to the general public, however, the classification of a particular registrant will be irrelevant if the need to share Internet identifying information with neighbors arises should police become aware that a particular person has begun using an alias to attempt to solicit illegal sexual activities on the Internet. But to presume that law enforcement will go beyond those narrow circumstances and generally release Internet information to the public under Penal Code section 290.45 was error.

E. The provisions of Penal Code section 290.45 provide no basis for the district court's concern about widespread disclosure of a registrant's Internet information.

Section 290.45 is the provision that the district court believed would open the door to widespread dissemination of a registrant's Internet information. ER 0012. Subdivision (a)(1) allows a designated law enforcement entity to provide information about a person required to register

as a sex offender, "by whatever means the entity deems appropriate, when necessary to ensure the public safety based upon information available to the entity concerning that specific person." Cal. Penal Code § 290.45(a)(1). As described, though, the restrictions on permissible notification preclude: (a) the disclosure of any Internet identifying information on the Internet (unless a warrant is outstanding for that person), (b) further dissemination of the information by the community members notified, and (c) misuse of the information by the persons receiving the information. *See* 42 U.S.C. § 16915a (prohibiting disclosure of a registrant's Internet information on a state's public website).

The district court's concern about theoretical widespread dissemination finds no basis in section 290.45. Law enforcement's responsibility under section 290.45 to control the dissemination of information on a person-by-person basis and to enforce penalties for misuse belies the district court's concern that law enforcement would use that provision as authority to broadcast the information to an entire community. Experience bears this out. California had been collecting Internet information from registrants for more than a year without any reported instances of community disclosure of a registrant's Internet information. ER 0324 (Schweig Decl., ¶ 13); ER 0326 (Schweig Decl., ¶ 16). Because registration takes place annually on the

registrant's birthday, the collection of information took place during at least one full registration cycle. Plaintiffs presented no evidence that any registrant Internet information was disclosed to the public by any law enforcement agency or that anybody (including plaintiff Jack Roe, prior to passage of the CASE Act) had expressed concern about providing that information.

Section 290.45 is a limited notification provision, which may only be used when public safety is at risk. There is no evidence that law enforcement has abused the discretion given it by the Legislature. This section provides no basis for the district court's conclusions about law enforcement misuse.

II. THE DISTRICT COURT ERRED IN RULING THAT THE PENALTY A REGISTRANT MAY FACE FOR FAILING TO COMPLY WITH THE CASE ACT'S REPORTING REQUIREMENTS CREATES TOO GREAT A CHILLING EFFECT TO PASS CONSTITUTIONAL MUSTER.

The district court was concerned that the uncertainty of whether specific Internet information should be registered would chill speech because of the potential of prosecution for failure to register such information. ER 0017. This concern is legally and factually unfounded.

To begin with, the district court itself first concluded that the CASE Act's definitions of information to be registered could be construed in such a

way as to make the reporting requirements sufficiently clear. ER 0007-0009. Moreover, to support a conviction of failure to register an item required by Sex Offender Registration Act, there must be evidence that the defendant *knew* that the particular requirement to disclose particular information applied to him. *See People v. Aragon*, 207 Cal.App.4th 504, 510 (2012); *People v. Edgar* 104 Cal.App.4th 210, 212 (2002).

Finally, in every instance aside from permitted mail registration for a change to an Internet identifier, a registrant is required to fill out the registration form *in person*. Cal. Penal Code § 290.15(a)(1) (registration requires registering officer to take fingerprints and current photograph). The likelihood that a registrant who intends to comply with the law in all respects, and who works directly with law enforcement personnel to register, could be prosecuted for innocently neglecting to register a specific item is low. Just like the district court's concern about public disclosure, in the more than one year California had been collecting Internet information, there is no evidence of prosecution for failing to register on the grounds the district court raised.

The theoretical possibilities upon which the district court based its decision, which have been refuted by actual experience, do not justify invalidating the entirety of the CASE Act's registration requirements.

CONCLUSION

The probability that there could be widespread misuse of a registrant's Internet information by one or more members of the public, or a law enforcement entity, is almost nil. Not only is the information restricted from any disclosure except in the most narrow of circumstances (so narrow in fact that it never happened during the year the Department of Justice collected the information), but the criminal and civil penalties attendant to the misuse are designed to make even the thought of improper disclosure a fleeting one at most. The CASE Act reporting requirements provide law enforcement with a tool to help protect and save our State's most vulnerable citizens from one of the most terrible experiences that can befall a person. The California Legislature balanced the competing interests and created the laws which serve the public, registrants, and law enforcement alike.

The district court's injunction disrupted this balance without fully assessing the entire statutory landscape. It was error to do so. This Court should reverse that decision.

Dated: April 10, 2013

Respectfully Submitted,

KAMALA D. HARRIS
Attorney General of California
DOUGLAS J. WOODS
Senior Assistant Attorney General
PETER K. SOUTHWORTH
Supervising Deputy Attorney General

/s/ ROBERT D. WILSON

ROBERT D. WILSON
Deputy Attorney General
Attorneys for Defendant and Appellant
Kamala D. Harris, Attorney General of California

SA2013110060
11067367.doc

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: April 10, 2013

Respectfully Submitted,

KAMALA D. HARRIS
Attorney General of California
DOUGLAS J. WOODS
Senior Assistant Attorney General
PETER K. SOUTHWORTH
Supervising Deputy Attorney General

/s/ ROBERT D. WILSON

ROBERT D. WILSON
Deputy Attorney General
Attorneys for Defendant and Appellant
Kamala D. Harris, Attorney General of California

CERTIFICATE OF COMPLIANCE
PURSUANT TO FED.R.APP.P 32(a)(7)(C) AND CIRCUIT RULE 32-1
FOR 13-15263, 13-15267

I certify that: (check (x) appropriate option(s))

[X] 1. Pursuant to Fed.R.App.P. 32(a)(7)(C) and Ninth Circuit Rule 32-1, the attached **opening/answering/reply/cross-appeal** brief is

[X] Proportionately spaced, has a typeface of 14 points or more and contains 5, 730 words (opening, answering and the second and third briefs filed in cross-appeals must not exceed 14,000 words; reply briefs must not exceed 7,000 words

or is

[ ] Monospaced, has 10.5 or fewer characters per inch and contains ____ words or ___ lines of text (opening, answering, and the second and third briefs filed in cross-appeals must not exceed 14,000 words or 1,300 lines of text; reply briefs must not exceed 7,000 words or 650 lines of text).

[ ] 2. The attached brief is **not** subject to the type-volume limitations of Fed.R.App.P. 32(a(7)(B) because

[ ] This brief complies with Fed.R.App.P 32(a)(1)-(7) and is a principal brief of no more than 30 pages or a reply brief of no more than 15 pages.

or

[ ] This brief complies with a page or size-volume limitation established by separate court order dated _____ and is

[ ] Proportionately spaced, has a typeface of 14 points or more and contains _____ words,

or is

[ ] Monospaced, has 10.5 or fewer characters per inch and contains __ pages or __ words or __ lines of text.

[ ] 3. Briefs in **Capital Cases**.
This brief is being filed in a capital case pursuant to the type-volume limitations set forth at Circuit Rule 32-4 and is

[ ] Proportionately spaced, has a typeface of 14 points or more and contains _____ words (opening, answering and the second and third briefs filed in cross-appeals must not exceed 21,000 words; reply briefs must not exceed 9,800 words).

or is

[ ] Monospaced, has 10.5 or fewer characters per inch and contains __ words or __ lines of text (opening, answering, and the second and third briefs filed in cross-appeals must not exceed 75 pages or 1,950 lines of text; reply briefs must not exceed 35 pages or 910 lines of text).

☐ 4. **Amicus Briefs**.

☐ Pursuant to Fed.R.App.P 29(d) and 9th Cir.R. 32-1, the attached amicus brief is proportionally spaced, has a typeface of 14 points or more and contains 7,000 words or less,

or is

☐ Monospaced, has 10.5 or few characters per inch and contains not more than either 7,000 words or 650 lines of text,

or is

☐ Not subject to the type-volume limitations because it is an amicus brief of no more than 15 pages and complies with Fed.R.App.P. 32 (a)(1)(5).

April 10, 2013
Dated

/s/ ROBERT D. WILSON
Robert D. Wilson
Deputy Attorney General