No. 15-2346/2486

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

JOHN DOES, #1-5; MARY DOE

Plaintiffs-Appellants/Cross-Appellees,

-vs-

RICHARD SNYDER, Governor of the State of Michigan;
COL. KRISTE ETUE, Director of the Michigan State Police, in their official capacities,

Defendants-Appellees/Cross-Appellants.

On appeal from the United States District Court
for the Eastern District of Michigan

Amicus Curiae Brief of the Center for Democracy & Technology, First Amendment Lawyers Association, and David G. Post in Support of Plaintiffs-Appellants and Reversal

---

Jennifer M. Kinsley
Associate Professor of Law
Northern Kentucky University
Chase College of Law, Nunn Hall 507
Highland Heights, Kentucky 41099
(859) 572-7998
kinsleyj1@nku.edu
Counsel of Record
Counsel for Amicus Curiae
First Amendment Lawyers Association

Emma J. Llansó
Center for Democracy & Technology
1634 I Street, N.W., Ste. 1100
Washington, D.C. 20006
(202) 637-9800
ellanso@cdt.org
Counsel for Center for Democracy & Technology

David G. Post
Open Technology Institute
740 15th Street N.W., Ste. 900,
Washington D.C., 20005
(202) 256-7375
Post@opentechinstitute.org

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate, *amici curiae* the Center for Democracy & Technology and the First Amendment Lawyers Association hereby submit the following corporate disclosure statements:

The Center for Democracy & Technology ("CDT") is a non-profit, non-stock corporation organized under the laws of the District of Columbia. CDT has no parent corporation, and no company owns 10 percent or more of its stock.

The First Amendment Lawyers Association ("FALA") is a nonprofit organization recognized as tax exempt under Internal Revenue Code § 501(c)(3). FALA has no parent corporation and no publicly held corporation owns 10 percent or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTERESTS OF AMICI

The Center for Democracy & Technology ("CDT") is a non-profit public interest organization that advocates for individual rights in Internet policy. CDT represents the public's interest in an open, innovative, and decentralized Internet that promotes constitutional and democratic values of free expression, privacy, and individual liberty. CDT has participated in a number of cases addressing First Amendment rights and the Internet, including as litigants in *CDT v. Pappert*, 337 F. Supp. 2d 606 (E.D. Pa. 2004) (striking down as unconstitutional a statute that imposed criminal liability on Internet service providers who failed to comply with requests issued by the Pennsylvania Attorney General to block access to websites containing child pornography), and as *amicus curiae* in First Amendment challenges including *Backpage.com, L.L.C., v. Dart*, No. 15-3047, slip op. at 4 (7th Cir. Nov. 30, 2015) (holding campaign by sheriff's office to pressure pressuring financial intermediaries to cease payment processing for online classified advertising website to be an unconstitutional prior restraint).

The First Amendment Lawyers Association ("FALA") is an Illinois-based, not-for-profit organization comprised of approximately 200 attorneys who routinely represent businesses and individuals that engage in constitutionally protected expression. FALA's members practice throughout the United States and Canada in defense of the First Amendment and, by doing so, advocate against

governmental forms of censorship. Member attorneys frequently litigate the facial validity of speech-restrictive legislation, often by way of anticipatory challenges that arise when a law is newly enacted and has not yet been enforced. In addition, FALA has a tradition of submitting *amicus* briefs to the Court on issues pertaining to the First Amendment. *See, e.g.*, *City of Littleton v. Z.J. Gifts D-4, L.L.C.*, 2004 WL 199239 (Jan. 26, 2004); *United States v. 12,200-ft Reels of Super 8mm Film*, 409 U.S. 909 (1972) (order granting FALA's motion to submit *amicus* brief).

Amicus David G. Post is well positioned to assist the Court in these matters. Until his recent retirement, he was the I. Herman Stern Professor of Law at the Beasley School of Law at Temple University. He previously taught at Georgetown Law Center and the George Mason University School of Law, and is currently a Senior Fellow at the Open Technology Institute of the New America Foundation. Prof. Post is a nationally-recognized expert on constitutional law, Internet law, and the First Amendment, and has written numerous scholarly articles on the application of First Amendment principles and doctrine to online activities. He has served as an expert witness in a number of cases involving the required disclosure of "Internet identifiers" by registered sex offenders, including *John Doe and Jane Doe 1 through 36 et al. v. State of Nebraska et al.* (Docket No. 8:09-cv-456 U.S. District Court, D. Neb., 2012), *Doe v. Harris* (Docket No. C12-5713-TEH US

District Court, N.D. Ca., 2012), *Doe v. Commonwealth of Kentucky* (U.S. District Court, E.D. Ky. 2014), *State v. Windham* (Docket No. DC-13-118C, Montana 18th Judicial District Court, 2015), and *State v. Bonacorsi* (Docket No. 218-2014-CR-01357 N.H. Superior Court, 2015). He also serves as a commentator on legal issues for national and local media, and is a regular contributor to the influential legal blog The Volokh Conspiracy at Washingtonpost.com.

RULE 29 STATEMENTS

Pursuant to Rule 29(c)(5) of the Federal Rules of Appellate Procedure, no counsel for a party authored this brief in whole or in part and no person other than amici curiae or their counsel made a monetary contribution to its preparation or submission. In accordance with Rule 29(a), counsel for amici provided notice to counsel for Appellant and Appellee of *amici*'s intent to file a brief. Appellant consented to the filing; Appellee did not respond to *amici*'s request for consent. A motion for leave to file accompanies the brief.

STATEMENT OF THE CASE

Michigan law provides that all convicted sex offenders registered in the state must disclose "any electronic mail or instant message address," and "any other designations used in internet communications or postings," M.C.L. § 28.725(1)(f), and requires that former sex offenders report to authorities within three business days of adding or changing such an identifier or setting up a new online account. M.C.L. § 28.722(g). Failure to comply with these or any of SORA's requirements constitutes failure to register as a sex offender, punishable by up to four years' imprisonment for a first offense. M.C.L. §§ 28.728a, 28.729(a). Registrants in the "Tier III" category, subject to the most stringent registration requirements, must under recent amendments to SORA report their Internet identifiers for life. M.C.L. § 28.727(1)(i).

SORA's "Internet identifiers" requirement applies to all individuals with an obligation to register under SORA. M.C.L. § 28.723. Application of the identifier requirement does not differentiate based on whether a computer or the Internet was used in the underlying offense, or any other assessment of risk that the individual will use the Internet in the commission of a future crime.

The District Court for the Eastern District of Michigan concluded that the Internet registration provision as drafted "implicated the First Amendment," and

offered certain narrowing constructions. 3/31/15 Opinion, R. 103, Pg.ID#5894. First, the district court narrowly construed SORA's registration requirement in order to "alleviate ambiguity" and limit the burden of reporting, holding that the reporting requirements applied only to identifiers used "*primarily* for the purposes of Internet communications or postings." 3/31/15 Opinion, R. 103, Pg.ID#5905. Next, the court held that SORA does not infringe registrants' right to speak anonymously, because the identifier requirement does not unmask their Internet communications to the public, and because the court deemed it unlikely that officials with internal access to the database of registrants' identifiers would follow any particular registrant's activities online in real time. 3/31/15 Opinion, R. 103, Pg.ID# 5923-24 (citations omitted). Finally, the district court held that SORA should be evaluated according to an intermediate standard of scrutiny because it does not discriminate against identifiable content or viewpoints, and does not prohibit the creation of certain identifiers or proscribe the use of any particular application or service. 3/31/15 Opinion, R. 103, Pg.ID#5920-21. The district court concluded that the identifier requirement survives intermediate scrutiny.

ARGUMENT

I. The ability to freely create and use Internet identifiers is central to online speech and access to information.

The ability to use the Internet has become essential to daily life. Recent studies by Pew found that 87% of American adults, including fully 97% of adults between the ages of 18 and 29, use the Internet.[1] Pew found that 71% of all American adults say they use the Internet on a typical day. An earlier study reported that 92% of online adults have email, with 61% using email on an average day.[2] Social media use is rising, with 74% of online adults use social networking sites, and 52% of online adults using two or more social media sites.[3] Pew has found that Internet use, including use of email and social media, is now strongly correlated with age, education, and household income.[4]

---

[1] Pew Research Center, The Web at 25 in the U.S., 5, 19 (2014), *available at* http://www.pewinternet.org/files/2014/02/PIP_25th-anniversary-of-the-Web_0227141.pdf. The 2014 Pew study found that "53% of internet users say the internet would be, at minimum, "very hard" to give up, compared with 38% in 2006. . . . Among those [users], most (61% of this group) said being online was essential for job-related or other reasons. Translated to the whole population, about four in ten adults (39%) feel they absolutely need to have internet access." *Id.* at 6.

[2] Pew Internet & American Life Project, Search and Email Still Top the List of Most Popular Online Activities, 2 (2011), *available at* http://www.pewinternet.org/files/old-media//Files/Reports/2011/PIP_Search-and-Email.pdf.

[3] Pew Internet & American Life Project, Social Media Update 2014, 1 (2015), *available at* http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/.

[4] Pew Internet & American Life Project, Digital Differences (2012), *available at* http://www.pewinternet.org/2012/04/13/digital-differences.

The Supreme Court noted as early as 1997 that "the content on the Internet is as diverse as human thought." *Reno v. American Civil Liberties Union*, 521 U.S. 844, 852 (1997) (internal citations omitted). Today, that diversity is compounded as Internet use becomes ever more integrated into people's personal, educational, and professional lives. People use the Internet to read the news, debate political matters, access government services, seek health information, watch films and videos, play video games, buy and sell books and art, take online courses and complete their degrees, find new friends and reconnect with old ones, and share their ideas and opinions with the world.

To do so, they use a diverse range of websites, online services, and applications that offer various combinations of the ability to access information, post user-generated content, and interact with others. Social media sites such as Twitter and Instagram allow users to share news and personal updates and respond to each others' posts, and message boards such as MetaFilter and Reddit host wide-ranging discussions devoted to specific topics and interests. E-commerce sites such as Craigslist, Amazon, and Etsy, and review sites such as Yelp and TripAdvisor allow users to provide their evaluations of products, businesses, and purchasing experiences. Blogs and newspapers include comment sections that enable users to discuss what they have read with the author and other readers. People purchase hardware, download software, pay for Internet services, and communicate with

technical support teams online and in real time. They use messaging apps such as WhatsApp and Telegram and voice-over-Internet-protocol (VOIP) services such as Skype and Viber to communicate with others via text or voice, from computers, tablets, or mobile phones.

As interactivity and personalization become key features for everything from Facebook's news feed to credit monitoring services such as Lifelock and educational technology such as Study Island, people will be required to create more accounts – that is, to establish an "Internet identifier" of the sort that may be covered by SORA's reporting requirement.

II. The Internet identifiers registration requirement creates substantial chilling effects on registrants' First Amendment rights.

Registrants' engagement with these myriad opportunities for speech, association, and access to information is chilled by SORA's requirement that individuals register their "Internet identifiers" with the state. SORA's Internet identifier registration requirement is vague, leaving registrants uncertain of their reporting obligations and creating a risk of arbitrary enforcement that will discourage registrants from creating online accounts. The identifier requirement is substantially overbroad: compliance will necessarily require registrants to provide the government with a list of the websites and other online applications or services for which they maintain accounts, sweeping in protected speech unrelated to the

legitimate purpose of the statute. Further, registrants will be required to identify their usernames and accounts to government officials as a condition of speaking, burdening their right to engage in anonymous speech online. The record below shows that the chilling effect of the Internet identifiers registration requirement is more than speculative.

A. The registration requirement is unconstitutionally vague because it provides no meaningful definition of covered "Internet identifiers," creating a risk of arbitrary enforcement by the state and encouraging self-censorship among registrants.

SORA's Internet identifiers registration requirement is void for vagueness because it fails to provide fair notice about what a reasonable person must know he is obligated to report and it fails to provide law enforcement with clearly articulated standards to avoid arbitrary and discriminatory enforcement. *Gentile v. State Bar of Nevada*, 501 U.S. 1030, 1051 (1991). "Given the vague contours of the coverage of the statute, it unquestionably silences some speakers whose messages would be entitled to constitutional protection." *Reno*, 521 U.S. at 874.

SORA is unclear as to what information it requires registrants to provide. The district court's ruling creates further ambiguities, making the reporting requirement impossible to apply with any consistency to the ways that online accounts are used today. Under SORA, a Michigan registrant must contact the registering authority every time "[t]he individual establishes any electronic mail or

instant message address, or any other designations used in internet communications or postings." M.C.L. § 28.725(5)(f). The district court interpreted the phrase "any other designations used in internet communications or postings" (which it conceded "includes some degree of ambiguity") "to refer only to designations used *primarily* for the purposes of Internet communications or postings." 3/31/15 Opinion, R. 103, Pg.ID#5904, 5905 (emphasis in original). The court interpreted this obligation to "exclude[] designations used primarily to engage in e-commerce and online banking, or to read content appearing on online newspaper accounts," even though registrants may "chat" with Amazon representatives or post comments to other readers on news sites. 3/31/15 Opinion, R. 103, Pg.ID#5906. At the same time, the court reasoned that an alias for a massively multi-player online role-playing game (MMORPG) is created primarily for the purpose of communicating with other online gamers, making such an identifier "similar in nature" to email and instant message addresses and therefore falling within SORA's identifier requirement. 3/31/15 Opinion, R. 103, Pg.ID#5906.

Both on its face and under the district court's "narrowing" construction, SORA is deeply unclear as to what information registrants are required to report. As a threshold matter, it is not clear under SORA whether registrants are required to report identifiers that they use with communications applications that do not or may not transmit messages using the Internet. Today, thousands of applications

and programs are available that enable individuals to communicate from computers and mobile devices using the Internet, cellular networks, mesh networking, or a combination of these networks. For example, messaging apps such as FireChat enable users to send text messages from their mobile devices, much as they might use the Facebook app or iChat instant messaging program, but explicitly without accessing the Internet.[5] The distinctions between applications that enable mobile messaging through SMS, the Internet, or mesh networking may not be immediately apparent to registrants, and it is unclear whether these distinctions would be considered relevant for SORA registration purposes.

The court's narrowing construction – limiting the statute to cover designations "used *primarily* for the purposes of Internet communications or postings" – only compounds the requirement's ambiguity. The Internet is, at its core, a network of communications networks that enables the exchange of data between remotely located computers; essentially all Internet activity is to some degree an "Internet communication". Indeed, several of the state's law enforcement witnesses stated that they understood the phrase "any other designations" used in Internet communications or posting broadly. *See, e.g.*, Joint

[5] Sophie-Claire Hoeller, *This App Lets You Text Without Wi-Fi or a Data Plan Anywhere in the World – Even On a Plane*, Business Insider (Aug. 4, 2014), http://www.businessinsider.com/firechat-app-lets-you-text-without-wifi-or-data-2015-8 (discussing FireChat's use of "mesh networking" to create ad hoc connections among users within a certain geographic radius that do not depend on access to the Internet or a cellular network).

Statement of Fact ("JSOF") ¶ 629, R. 90, PageID #3880 ("When [plaintiffs' counsel] surveyed law enforcement agencies regarding whether an on-line bank account, newspaper account, Amazon account or X-box account needs to be reported, he received varying responses. Different respondents stated that all accounts, or all accounts with usernames, or all accounts with email addresses would need to be reported.").

The district court's proffered standard of designations *primarily* used for Internet communications is inherently arbitrary, as illustrated by the court's own application of the new standard to various kinds of accounts demonstrates. For instance, it can easily be argued that an identifier used to access an online newspaper account *is* used "primarily for the purposes of Internet communication": the author of the newspaper article is communicating with the reader, and the reader, in turn, is communicating with the author (and other readers) when she posts a responsive comment. Similarly, joining a website to play a game and engage with other players is not obviously more "communicative" than joining a website to read the news and engage with the editorial board and other readers. The court does not explain the origin of its rule.

Plaintiffs have provided testimony tending to show their deep uncertainty about reporting online usernames and accounts. *See* JSOF ¶¶653, 663, 682, R. 90, Pg.ID#3886, 3888, 3891. Indeed, and despite the court's narrowing construction,

the ambiguities in the statute are likely to lead registrants "either to overreport their activity or underuse the Internet to avoid the difficult questions in understanding what, precisely, they must report." *Doe v. Harris*, 772 F.3d 563, 579 (9th Cir. 2014). This uncertainty "undermines the likelihood that [SORA] has been carefully tailored to the [State's] goal of protecting minors' and other victims." *Id.* (quoting *Reno*, 512 U.S. at 871). And notwithstanding the lower court's rejection of strict liability for improper reporting, 3/31/15 Opinion, R. 103, Pg.ID#5908, this Court "'cannot assume that, in its subsequent enforcement, ambiguities will be resolved in favor of adequate protection of First Amendment rights.'" *Id.* (quoting *NAACP v. Button*, 371 U.S. 415, 438 (1963)). SORA's Internet identifiers registration requirement is highly ambiguous, difficult to apply consistently, and is unconstitutionally vague.

B. The registration requirement is substantially overbroad because it regulates vast quantities of protected Internet speech in relation to its legitimate purpose.

SORA's Internet identifiers registration requirement "effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another." *Reno*, 521 U.S. at 874. The registration scheme is substantially overbroad, and imposes a chilling effect on large quantities of protected speech online.

SORA compels disclosure of far more speech than necessary for pursuing the legitimate public-safety goals of the state. SORA compels disclosure of all of a registrant's usernames and the website or service on which they are used "primarily" for communication and associates this expressive activity with her name and other personally identifiable information in the SOR database. *See* JSOF ¶638-95, 700, R. 90, Pg.ID#3882-94 (noting that 13,232 registrants have contributed one or more Internet identifiers to the SORA database). It imposes these burdens on all registrants, in some cases for the rest of their lives, without any demonstration that the intended deterrent effect is necessary for registrants as a class, much less individualized determination of whether a given registrant presents a risk of re-offending, and of doing so by using the Internet.

As part of the burden of reporting a large number of previously created and new usernames to a SOR authority, sections 28.727(1)(I) and 28.726(1)(f) compel registrants to disclose all of the account-based websites and applications they use primarily for communication purposes. While neither the statute on its face nor the court below expressly requires disclosure of the sites and services a registrant uses, SORA's focus on the "addresses" associated with email and instant message *programs* describes a requirement to report a username along with the service or application where it is used. Law enforcement and the court below have similarly presumed and required this result. *See, e.g.*, JSOF ¶ 629, R. 90, PageID #3880

("Ms. Johnson testified that the SOR Unit trains law enforcement agencies to register email addresses and screen names in which social communication exists. This includes things like Facebook, Myspace, Yahoo! email . . . ."). Indeed, a standalone username (such as "GrandRapidsJoe") would be meaningless absent the associated site or service (such as "Twitter.com" or "AtheistForums.org"). Law enforcement officials who must now determine whether a username is used "primarily" for the purposes of "communication" would find it difficult, if not impossible, to complete this assessment without knowledge of the service with which it is used. Thus, the identifier registration requirement compels registrants to disclose all of the account-based websites and applications they use "primarily" for purposes of Internet communication. This subjects information about registrants' expressive activities and associations – e.g., that they have an account on Grindr ("the world's largest gay social network") or have joined Ummah.com (an online message board for the Muslim community) – to compulsory disclosure to the government. This will likely discourage registrants from creating accounts for online fora that might reveal sensitive personal, health, religious, or political information, thus chilling their engagement in wholly protected speech.

Finally, the resulting chilling effect is not justified by a showing of necessity or degree of risk that registrants pose online. The court below acknowledged that "93% of [registrants] were not convicted of a computer or Internet-related crime,"

and struck down retroactive extension of the registration requirement because the record did not support a finding that registrants who have not re-offended in twenty-five years "pose an enhanced risk of committing sex offenses." 9/03/15 Opinion, R. 118, Pg.ID#6023, 6028 (holding that the state did not carry its burden in demonstrating that extending the reporting requirement from twenty-five years to life is not substantially broader than necessary). Likewise, by failing to show that registrants as a class pose an enhanced risk of committing sex offenses involving online communication, the state cannot justify the chilling effect caused by SORA's Internet registration requirement. "Persons whose expression is constitutionally protected may well refrain from exercising their rights for fear of criminal sanctions provided by a statute susceptible of application to protected expression." *Gooding v. Wilson*, 405 U.S. 518, 519 (1972). As a result, SORA is substantially overbroad in violation of the First Amendment. *Reno*, 521 U.S. 844.

C. The Internet identifier registration requirement restrains anonymous expression and significantly chills online speech.

First Amendment law recognizes a right to engage in unidentified speech because information about authorship is an important aspect of the speaker's message. "An author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of

the freedom of speech protected by the First Amendment." *McIntyre v. Ohio Elections Comm'n*, 513 U.S. 334 (1995). The right includes the right to withhold one's name from the public or agents of the government, while engaging in the exercise of First Amendment rights.

The district court recognized plaintiffs' First Amendment right to engage in anonymous expression. 3/31/15 Opinion, R. 103, Pg.ID# 5922-24. Yet it held that SORA does not infringe that right, because it does not "unmask their anonymity to the public," and because the court was not convinced that officials with internal access to the database of SORA identifiers were likely to follow any particular registrant's activities online in real time. 3/31/15 Opinion, R. 103, Pg.ID# 5926-27 (quoting *Laird v. Tatum*, 408 U.S. 1 (1972)).

The district court's conclusions are wrong for two reasons. First, no First Amendment doctrine holds that the burden of disclosing one's identity is recognized only when the disclosure becomes publicly available. In fact, the Supreme Court recognized that compulsory identification to state officials infringes the freedom to engage in anonymous association for expressive purposes. *See NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 450 (1958) (reversing court order compelling the NAACP to produce members list to movant in state injunctive proceedings). In subsequent cases, the Court similarly invalidated requirements that public school teachers and principals submit affidavits of past

membership to their board of trustees, *Shelton v. Tucker*, 364 U.S. 479, 484, n.2 (1960), and that organizations respond to membership inquiries to a legislative investigatory committee, *Gibson v. Florida Legislative Comm.*, 372 U.S. 539, 543 (1963); in neither of these cases did the Court first determine that the sensitive disclosures would be subject to some manner of public exposure.

Second, while SORA does not require registrants' identifiers to be automatically published alongside other identifying information that appears on Michigan's OffenderWatch website, it provides no legal or technical protections that prevent identifiers from being made publicly available. Unlike the statute in *Shurtleff*, which the district court cites as analogous, SORA does not prescribe narrow circumstances under which identifier information may be disclosed to the public; it in no way limits how or why the information may be used or disseminated. *Cf. Doe v. Shurtleff*, 628 F.3d 1217, 1222 (10th Cir. 2010) (upholding identifier registration statute where the law specified that information would remain non-public, and disclosure was permissible only with court order or subpoena).

All of the identifiers provided by registrants are available in the SOR database without any statutory limits on access, use, dissemination, or publication. Approximately 600 law enforcement agencies and 8,000 users of the SORA database have direct access to registrants' identifier information, and can use

Michigan's OffenderWatch software to search for usernames and accounts. SORA does not require that officers seek special permission, such as from a supervising authority or a court. JSOF ¶695, R. 90, Pg.ID#3894. This appears to be the case even if officers were to monitor individuals' postings on a daily basis or conduct social media "sweeps" for registrants. Nor does SORA expressly require that officers notify registrants when their usernames and accounts are being monitored.

Finally, the highly sensitive information contained in the database gives rise to serious risks of data breach,[6] which can have profound repercussions for a person's life and his willingness to participate in social, political and economic activities online. Particularly for registered sex offenders, the very real threat of data breach can serve as a powerful disincentive to joining online services for the purposes of communication.[7]

---

[6] In addition to high-profile breaches of data stored by private entities such as Target and Apple's iCloud, federal offices and agencies such as the Office of Personnel Management, the State Department, and the White House have suffered data breaches affecting millions of people. *See* Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, Wash. Post (July 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/; Nicole Perlroth, *State Department Targeted by Hackers in 4th Agency Computer Breach*, N.Y. Times (Nov. 16, 2014), http://www.nytimes.com/2014/11/17/us/politics/state-department-targeted-by-hackers-in-4th-agency-computer-breach.html?_r=0; Ellen Nakashima, *Hackers Breach Some White House Computers*, Wash. Post (Oct. 28, 2014), https://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html.

[7] "Cyber-mobs" have used public-shaming campaigns to drive targeted users away from social media platforms, often with threats of future violence or release of sensitive information such as the victim's telephone number and home address. *See, e.g.*, Danielle Keats Citron, Hate Crimes in Cyberspace (Harv. Univ. Press 2014). Registered sex offenders currently experience severe and well-documented discrimination, harassment, and assault in their "offline" lives. *See, e.g.*, Jill Levenson, et al., *Megan's Law and Its Impact on Community Re-Entry for Sex Offenders*, 25

Thus, the identifier reporting requirement creates a substantial risk to anonymous expression by creating a database of identifiers without sufficient safeguards around access or use. *Doe v. Harris*, 772 F.3d at 579-80 (holding failure to provide protections against unauthorized access and publication threatens anonymous expression). Though registrants are not required to disclose their identities directly to the public, SORA nevertheless chills anonymous speech "because it too freely allows law enforcement to disclose sex offenders' Internet identifying information to the public." *Id.* This risk of data breach likewise creates a chilling effect, particularly where disclosure of similar identifying information has subjected registrants to "economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility." *NAACP v. Alabama*, 357 U.S. at 462. Because of its implications for anonymous expression, the Internet identifier registration requirement "must be regarded as entailing the likelihood of a substantial restraint" upon the exercise of registrants' First Amendment rights. *NAACP v. Alabama*, 357 U.S. at 462.

D. The reporting requirement and its implications for registrants chill substantial amounts of registrants' online speech.

Behav. Sci. L. 590, 592-93 (2007). The record indicates the harassment plaintiffs have suffered as a result of the publication of their status and identity on SORA's OffenderWatch website. JSOF ¶¶939, 942-52, 993-98, 1003, R. 90, Pg.ID#3949-52, 3964-65, 3966.

Compulsory registration of the websites, applications, and online services that registrants use primarily for communication imposes a considerable burden on registrants' online association, access to information, and access to platforms for speech and is "almost certain to have a deterrent effect" on those activities. *Lamont v. Postmaster General*, 381 U.S. 301, 307 (1965). Understandably, many registrants avoid the burdens of reporting their Internet identifiers and the risks of arbitrary punishment or potential data breach by simply refraining from participating in online life. *See* JSOF ¶¶ 638-95, R. 90, PageID #3882-3894. The plaintiffs testified that their reasons for abstaining from Internet activity included the burdens of reporting, the stark consequences for failing to do so properly, and the fear of unseen supervision or unauthorized public exposure. *See, e.g.*, JSOF ¶ 657, R. 90, PageID #3886, 3889 .

Their fear, moreover, is widespread among registrants. The record shows that of the 28,000 registrants in the SORA database, only 13,232 have disclosed any kind of Internet identifier to the registering authority. JSOF ¶¶ 639, R. 90, PageID #3882. In other words, as many as half of Michigan registrants may not be using the Internet. *See* 9/03/15 Opinion, 11 n.4, R. 118, Pg.ID#6025; *cf.* section I, *supra* (92% of adult Americans use email). Their low rate of Internet participation is problematic for a group of people whose economic, social, and family lives are already severely curtailed by restrictions on their place of work, place of domicile,

and freedom of association and movement. Finally, with online identifiers becoming increasingly essential for participating in digital life, the chill on their use is likely to have profound effects on registrants' ability to engage in First Amendment-protected activities, such as accessing information and engaging in expressive association and speech. Disparities in knowledge and skills related to online research, communication, and networking will in turn impact the ability to access opportunities in personal, educational, and professional life.

III. SORA's Internet identifiers registration requirement should be evaluated under strict scrutiny.

A. SORA punishes the failure to report one's intention to speak at some future point, creating a presumptively unconstitutional prior restraint.

"Threatening penalties for future speech goes by the name of 'prior restraint,' and a prior restraint is the quintessential first-amendment violation." *Backpage.com, L.L.C.*, *v. Dart*, No. 15-3047, slip op. at 12 (7th Cir. Nov. 30, 2015) (quoting *Fairley v. Andrews*, 578 F.3d 518, 525 (7th Cir. 2009)). As noted in this Circuit, "[a]ny prior restraint bears 'a heavy presumption against its constitutional validity.'" *In re King World Prods., Inc.*, 898 F.2d 56, 60 (6th Cir. 1990) (quoting *New York Times Co. v. United States,* 403 U.S. 713, 714 (1971) (per curiam)).

Prior restraints chill future speech when they condition "the exercise of a First Amendment right . . . on the prior approval of public officials." *Deja Vu of Nashville, Inc. v. Nashville*, 274 F.3d 377, 400 (6th Cir. 2001); *Near v. Minnesota ex rel. Olson*, 283 U.S. 697, 706 (1931). Such licensing or notification schemes are permissible only where they provide "adequate standards to guide the exercise of official discretion and make possible meaningful judicial review," *Utah Animal Rights Coalition v. State Lake City Corp.*, 371 F.3d 1248 (10th Cir. 2004), and guarantee sufficient procedural safeguards to ensure that those substantive protections are observed, *Bantam Books*, 372 U.S. at 71.

SORA's identifier registration requirement imposes a prior restraint by preventing the unregistered use of usernames and online communications fora. In its landmark prior restraint ruling, *Near v. Minnesota*, the Supreme Court reversed an injunction against future publications "under the name and title of . . . The Saturday Press or any other name or title," because the clear object of the statute at issue was "not punishment, in the ordinary sense, but suppression" of future issues of the publication. 283 U.S. at 706, 711. This same suppression of future speech under a particular name or title is an acknowledged aim of SORA's identifiers requirement. *See* 3/31/15 Opinion, R. 103, Pg.ID#5922 (citing Justice Department guidelines for the proposition that "knowledge that their Internet identifiers are known to the authorities may deter registered sex offenders from engaging in

criminal activity on the Internet"). While the goal of deterring criminal activity is a legitimate aim of the state, the effort to accomplish this by burdening all future opportunities for online speech is not. By restricting online publication under any "name and title" other than those that are registered as "identifiers" with the state, SORA operates as a prior restraint on all future postings.

SORA includes no substantive safeguards to mitigate against administrative abuses, including content- or viewpoint-based enforcement by the registering authority or enforcement agencies. *Shuttlesworth v. Birmingham,* 394 U.S. 147, 150-51 (1969) (law "subjecting the exercise of First Amendment freedoms to the prior restraint of a license, without narrow, objective, and definite standards" is unconstitutional); *City of Lakewood v. Plain Dealer*, 486 U.S. 750, 757 (1988) (when a licensing regime lacks standards limiting officials' discretion, it is difficult for courts to review First Amendment issues, giving officials unbridled discretion over individuals' exercise of rights). The lower court's construction limiting the identifier requirement to those identifiers used "primarily" for the purpose of communication calls on registering and prosecuting officials to make content-based determinations of registrants' prospective speech (discussed *infra* section III.C). The lack of substantive standards for determining if an identifier is subject to the reporting requirement renders it highly susceptible to content- or even viewpoint-based enforcement.

Moreover, SORA provides no procedural mechanism whereby registrants may assert their First Amendment rights. Indeed, liability arises not from an independent judicial determination that registrants have engaged in unprotected speech, but rather because they have failed to provide the government with notice of the usernames and accounts through which they intend to speak. *Freedman v. Maryland*, 380 U.S. 51, 58 (1965) ("[B]ecause only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression, only a procedure requiring a judicial determination suffices to impose a valid final restraint."). Registrants are thus afforded no mechanism for requesting an exemption prior to the statutory timeframe for reporting, and no opportunity following a failure to properly report an identifier to request "a full and fair determination of the constitutionally protected nature of the expression by an independent judicial forum." Martin H. Redish, *The Proper Role of the Prior Restraint Doctrine in First Amendment Theory*, 70 Va. L. Rev. 53, 57 (1984).[8] Under SORA, a speaker who shares constitutionally protected information or opinion but who is not on the government's list of approved speakers will face punishment, regardless of the protected nature of his speech.

[8] *See* Michael I. Meyerson, *The Neglected History of the Prior Restraint Doctrine: Rediscovering the Link Between the First Amendment and the Separation of Powers*, 34 Ind. L. Rev. 295, 339 (2001) (arguing "[t]he 'prior' in the prior restraint doctrine refers not only to regulatory activity which is undertaken before the specific expression is communicated, but also when the executive or judicial branch acts out of its 'constitutional order' vis-á-vis the other branches of government.").

SORA imposes a burden on presumptively protected speech out of proportion to the state of Michigan's legitimate interests, rendering the identifier requirement an unconstitutional prior restraint on speech. *Watchtower Bible & Tract Society v. Village of Stratton*, 536 U.S. 150, 164-66 (2002) (prior restraint where misdemeanor punished individuals engaging in door-to-door canvassing for any "cause" without first registering for a permit from the office of the mayor and producing identity information on demand to police or the public). Just as the licensing scheme in *Watchtower Bible* imposed substantial burdens on protected expression, the identifier requirement necessarily results in the surrender of anonymity; disproportionately burdens religious, political, and other controversial speech; and effectively bans a significant amount of spontaneous speech without any evidence that it is narrowly tailored to the government's interest in community policing. *Id.* at 150. By discouraging citizens from speaking freely, SORA creates an unconstitutional prior restraint. *American-Arab Anti-Discrimination Comm. v. Dearborn*, 418 F.3d 600, 605 (6th Cir. 2005) ("The simple knowledge that one must inform the government of his desire to speak and must fill out appropriate forms and comply with applicable regulations discourages citizens from speaking freely."). The identifier requirement is therefore subject to the most stringent form of scrutiny available under the First Amendment.

B. The Internet identifiers registration regime requires government officials to make content-based evaluations of registrants' speech.

"Any permit scheme controlling the time, place, and manner of speech must not be based on the content of the message." *Forsyth Cty. v. Nationalist Movement*, 505 U.S. 123, 130 (1992) (citing *Freedman*, 380 U.S. 51). "Content-based laws – those that target speech based on its communicative impact – are presumptively unconstitutional and may be justified only if the government proves that they are narrowly tailored to serve compelling state interests." *Reed v. Town of Gilbert*, 576 U.S. _, No. 13–502, slip op. at 6 (June 18, 2015).

SORA's Internet identifiers registration regime requires government officials to make content-based evaluations of registrants' speech and is highly susceptible to content-based applications. For this reason, the identifier requirement is also subject to strict scrutiny as a content-based regulation. Applying SORA according to the district court's interpretation requires the registering authority to make a determination of the subject matter or content of the registrant's intended speech. Such official determinations of the subject matter or content of speech are subject to strict scrutiny under the First Amendment. *Reed*, No. 13–502, slip op. at 10 (sign law's differentiation between temporary directional signs and other types of political or ideological signs is a content-based distinction subject to strict scrutiny).

As discussed in Section II, *supra*, the district court explained that its narrowing construction of the identifiers reporting requirement applies to online role-playing game aliases and other accounts used "primarily" for communication, but excludes usernames used "primarily" for communicating with bank representatives online or posting comments on news sites. 3/31/15 Opinion, R. 103, Pg.ID#5906. By instructing government officials to draw distinctions between a registrant's accounts for communicating with her banker or commenting on the newspaper online and her accounts used for communicating with her neighbor on social media or commenting on the gameplay in an online video game, the district court instructs officials to make distinctions among registrants' identifiers based on the content or subject matter of registrants' speech. *Reed*, No. 13–502, slip op. at 13. Distinctions between commercial, informational, social, and recreational are "obvious[ly]" content based. *Id.*

Moreover, because SORA offers no substantive standards for determining if an identifier is subject to the reporting requirement, the identifier requirement is highly susceptible to content-based or viewpoint-based enforcement. *Forsyth County*, 505 U.S. at 130 ("A government regulation that allows arbitrary application . . . has the potential for becoming a means of suppressing a particular point of view."); *ACLU v. City of Las Vegas*, 333 F.3d 1092, 1107-08 (9th Cir. 2003) (vending permit regulation that fails to set forth any standards to guide

administrative decision making provides no basis to determine whether content-based discrimination was likely to arise). Indeed, as discussed above, SORA confers unbridled discretion on government officials charged with making determinations regarding which identifiers are "primarily communicative" – and, correspondingly, which registrants are subject to prosecution for failing to register as a sex offender. This creates a grave risk of arbitrary or content-discriminatory punishment. *See Deja Vu of Cincinnati, L.L.C. v. Union Township Bd. of Trustees*, 411 F.3d 777 (6th Cir. 2005).

Because SORA "delegate[s] overly broad licensing discretion to a government official" and directs official discretion to be exercised "based on the content of the message," *Forsyth County*, 505 U.S. at 130 (citing *Freedman*, 380 U.S. at 56), Michigan must establish that SORA's identifier requirement "furthers a compelling governmental interest and is narrowly tailored to that end," *Reed*, No. 13–502, slip op. at 14.

IV. SORA's Internet registry requirement is not sufficiently tailored to satisfy even an intermediate standard of scrutiny.

SORA's identifier requirement is a content-based prior restraint on speech subject to strict scrutiny. Yet even under the standard reserved for content-neutral time, place, and manner regulations – applied by the court below – the identifier

requirement fails to satisfy intermediate scrutiny.[9]

To withstand intermediate scrutiny, SORA's identifier requirement must have been enacted within Michigan's constitutional power; must further a substantial governmental interest; the interest must be unrelated to the suppression of speech; and the identifier requirement may pose only an "incidental burden on First Amendment freedoms that is no greater than is essential to further the government interest. *Deja Vu of Nashville*, 274 F.3d at 400 (quoting *East Brooks Books, Inc. v. City of Memphis*, 48 F.3d 220, 226 (6th Cir. 1995)).

As the district court noted, "investigating and deterring online sex offenses" is a legitimate state interest. *See* 9/03/15 Opinion, 10, R. 118, Pg.ID#6024. But the fact that an identity reporting requirement might "enhance public safety does not, by itself, mean that [the law] is narrowly tailored." *Id.* Michigan's interest in regulating registrants' Internet use is not "unrelated to the suppression of expression," *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 37 (1984); indeed, the

[9] In the context of prior restraints, courts have traditionally reserved intermediate scrutiny for licensing schemes that regulate the time, place, and manner of activities including parades and concerts in traditional public forums, and for generally applicable zoning ordinances regulating the secondary effects of adult theaters and other businesses. *Cf. Thomas v. Chicago Park District*, 534 U.S. 316 (2002) (time, place or manner licensing for use of a traditional public forum, "not even directed to communicative activity but rather to *all* activity conducted in a public park"); *City of Littleton, Colo. v. Z.J. Gifts D–4*, 541 U.S. 774, 781 (2004) (generally applicable zoning ordinance). The Internet, however, is a series of private forums and not a public forum created by the government; nor should communication on the web be considered a form of "expressive conduct" as opposed to pure speech. *See* Douglas B. McKechnie, *Facebook Is Off-Limits? Criminalizing Bidirectional Communication Via The Internet Is Prior Restraint 2.0*, 46 Ind. L. Rev. 643, 664 (2013); *cf.* 3/31/15 Opinion, R. 103, Pg.ID#5920-21 (applying *Ward v. Rock Against Racism,* 491 U.S. 781, 791 (1989)).

district court construed the reporting requirement to apply specifically to identifiers used "primarily for Internet communication," 3/31/15 Opinion, R. 103, Pg.ID#5905. Laws that control crime by regulating communication and its impacts cannot be said to be "unrelated to the suppression of expression." At its core, SORA seeks to prevent crime by burdening speech.

Neither is SORA's "limitation on First Amendment freedoms no greater than necessary or essential to the protection of the particular government interest involved." *Seattle Times*, 467 U.S. at 37 (quoting *Procunier v. Martinez*, 416 U.S. 396, 413 (1974)). As discussed in Section II.B, SORA affects a significant amount of presumptively protected speech. It applies to an ambiguous and arbitrarily defined subset of Internet communications and prescribes strong penalties for failure to properly comply. SORA provides no forum, independent or otherwise, for a registrant to claim her First Amendment right to anonymous expression. Nor does it protect a registrant from the risk of unauthorized access, disclosure, or publication. It makes no distinction between individuals registered to different "tiers" under the sex offender statute, much any less individualized assessment of the necessity of restricted Internet use. Its chilling impact on registrants' Internet use and expression is profound – far greater than necessary to promote online safety in Michigan.

SORA thus fails to survive even an intermediate level of scrutiny under the First Amendment. *Doe v. Harris*, 772 F.3d at 579 (citing *United States v. Turner Broadcasting System*, 512 U.S. 622, 642 (1994)).

CONCLUSION

> It is offensive – not only to the values protected by the First Amendment, but to the very notion of a free society – that in the context of everyday public discourse a citizen must first inform the government of her desire to speak to her neighbors and then obtain a permit to do so.

Watchtower Bible, 536 U.S. at 165.

Given the vague contours of the statute, and the license requirement it imposes on a class of Internet users who, despite their registration status, retain the full protections of the First Amendment, SORA "unquestionably silences some speakers whose messages would be entitled to constitutional protection." *Reno*, 521 U.S. at 874. SORA is unconstitutionally vague and overbroad, and fails to satisfy either a strict or an intermediate standard of scrutiny because it fails to guide an officer's discretion about which "primarily" communicative identifiers must be disclosed and for which expressive activities a registrant may be punished for failure to register.

January 11, 2016

Respectfully submitted,

/s/ Jennifer M. Kinsley
Jennifer M. Kinsley
Counsel of Record
Associate Professor of Law
Northern Kentucky University
Chase College of Law, Nunn Hall 507
Highland Heights, Kentucky 41099
(859) 572-7998
kinsleyj1@nku.edu
Counsel for Amicus Curiae
First Amendment Lawyers
Association

ellanso@cdt.org
Counsel for Center for Democracy &
Technology

David G. Post
Open Technology Institute
740 15th Street N.W., Ste. 900
Washington D.C., 20005
(202) 256-7375
Post@opentechinstitute.org

Emma J. Llansó
Center for Democracy & Technology
1634 I Street, N.W., Ste. 1100
Washington, D.C. 20006
(202) 637-9800

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify that the attached *amicus brief* is proportionately spaced in 14-point Times New Roman typeface and contains 6,661 words (as calculated by Microsoft Word for Mac 2011), excluding the caption page, Disclosure Statement,[10] Table of Contents, Table of Authorities, and this Certificate of Compliance.

Respectfully submitted,

/s/ Jennifer M. Kinsley

[10] *Amici* understand this exemption to cover the Rule 26.1 statement. This certificate of compliance therefore excludes *amici*'s corporate disclosure statement.

CERTIFICATE OF SERVICE

I hereby certify that an exact copy of the foregoing document was provided to all counsel of record via the Court's electronic filing system (CM/ECF) this 11th day of January, 2016.

Respectfully submitted,

/s/ Jennifer M. Kinsley