MITCHELL | HAMLINE School of Law

Mitchell Hamline Law Review

Volume 49 | Issue 4 Article 4

2023

# Sex Offenders and Internet Speech: First Amendment Protections for America's Most Reviled Outcasts

Gabriel Aderhold

# SEX OFFENDERS AND INTERNET SPEECH: FIRST AMENDMENT PROTECTIONS FOR AMERICA'S MOST REVILED OUTCASTS

*Gabriel Aderhold*[1]



[1] Gabriel Aderhold is a J.D. candidate at Mitchell Hamline School of Law. The author wishes to thank James Cornelio for sharing his story and Alisha Hennen, Eric Janus, Sarah Lageson, Madeline Ranum, Michael Steenson, and the entire Mitchell Hamline Law Review staff for their contributions and support.

## I. INTRODUCTION

On Sunday, April 22, 2018, James Cornelio was arrested in his Connecticut home after a judge signed a warrant for his arrest.[2] Mr. Cornelio was charged with a class D felony, a crime punishable by up to five years in prison.[3] What was his crime? Mr. Cornelio did not include an email address—that he had used to communicate with a state police officer—on a proper verification form.[4] Mr. Cornelio then found himself tangled in the growingly complex and constitutionally questionable web of sex offender registry requirements: mandated disclosure of Internet identifiers.

Despite over ninety-one percent of Americans using the Internet today,[5] one would be hard-pressed to precisely define what an "Internet identifier" is. Does "Internet identifier" just mean an email address or a username, with or without a password? Does it mean the IP address or original source of where online activity is coming from? Even if one could precisely define what an "Internet identifier" is, the challenge to determine when it must be disclosed by sex offenders is far greater.

For a legal definition, surveying the fifty states will not answer these questions either, as jurisdictions differ in their definitions of "Internet identifier."[6] For example, Florida defines an "Internet identifier" as "any designation, moniker, screen name, username, or other name used for self-identification to send or receive social Internet communication."[7] Does this mean an individual, subject to reporting requirements, who creates a New York Times online account must disclose such an account or risk criminal penalty? What about someone who sets up a smart refrigerator, which connects directly to the manufacturer through the Internet for twenty-four-seven support? And what happens if one must create a new "Internet identifier" for work, school, or other (legal) personal purposes, such as a workplace online username which can only be accessed at the job site? What is the appropriate legal timeframe for sex offenders to inform law enforcement of their Internet identifiers? A month? A day? Thirty minutes?[8]

---

[2] Brief of Appellant at 8, Cornelio v. Connecticut, 32 F.4th 160 (2d Cir. 2022) (No. 20-4106).

[3] Cornelio v. Connecticut, 32 F.4th 160, 169 (2d Cir. 2022) (citing to CONN. GEN. STAT. §§ 54-253(e), 53a-35a(8), 53a-41 which provide that failure to properly report an online communication identifier can result in a class D felony "punishable by up to five years in prison and a $5,000 fine").

[4] *See id.* at 167–68.

[5] *Internet usage penetration in the United States from 2018 to 2027*, STATISTA (Aug. 31, 2022), https://www.statista.com/statistics/590800/internet-usage-reach-usa/ [https://perma.cc/VL6K-WPVX].

[6] *See generally* ALA. CODE § 15-20A-7 (2022); ALASKA STAT. § 12.63.010 (2022); COL. REV. STAT. § 16-22-108 (2021); FLA. STAT. § 943.0435 (2021); VA. CODE ANN. § 9.1-903 (2022).

[7] FLA. STAT. § 775.21(2)(j) (2021) (defining an "Internet identifier" in Florida). Florida's statute excludes date of birth, social security number, personal identification number (PIN), and password from the definition. *Id.*

[8] *See* VA. CODE ANN. § 9.1-903 (2022) (requiring sex offenders to notify proper law enforcement officials within thirty minutes of changing any Internet identifier or email address information, among other things).

How did we get here? Why does it matter so much to First Amendment rights? What is the proper remedy for balancing the need to protect the public from dangerous predators and safeguarding the constitutional rights of those we deem most contemptible? Section II of this Note offers the historical context of sex offender registry ("registry" or "registries") laws over time, offering insight into how Internet identifier requirements deviated from the traditional goals of registries. Section III follows, establishing the essential framework of the constitutional issues with an assessment of relevant First Amendment jurisprudence. Section III acts as a springboard for Section IV, which analyzes recent caselaw and ultimately shows how many Internet identifier laws today are unconstitutional. Section V paves a pathway for action, providing solutions to remedy current unconstitutional laws. This Note offers three potential solutions, with the final one seeking the perfect balance between the *want* for greater public safety and the *need* for safeguarding essential civil liberties. Finally, this Note concludes with Section VI, a final appeal to stand up for those we might otherwise cast aside.

## II. THE MODERN EVOLUTION OF SEX OFFENDER REGISTRIES

Today, it is hard to imagine living in a country without easy access to sex offender registries. In 2013, for example, a majority of Americans, including sixty-six percent of parents, stated they had checked a registry online.[9] Despite the long history of privately maintained registries, having them available to the general public is a fairly novel concept.[10] This section focuses on three timeframes: first, the origin of registries before the advent of widespread Internet use; second, the point where many state registries went "online" following the passage of federal sex offender legislation in 1994; and third, the vast expansion of registry Internet regulations since 2006. By reviewing these three distinct timeframes, context is offered into how registry policies, originally rooted in constitutionally permissible efforts to protect the public, became grossly perverted and were put on a collision course with First Amendment protections surrounding Internet speech.

### *A. Rotary: Registry Origins (1947–1994)*

Before jumping into registries going "online," it is important to understand some history. In 1947, California enacted the first state registry

[9] Kate Palmer, *Half of Americans have checked the Sex Offender Registry*, YOUGOV (Aug. 14, 2013), https://today.yougov.com/topics/society/articles-reports/2013/08/14/half-americans-have-checked-sex-offenders-register [https://perma.cc/8TEW-EBQQ].

[10] *See Legislative History of Federal Sex Offender Registration and Notification*, Department of Justice (Oct. 15, 2022), https://smart.ojp.gov/sorna/current-law/legislative-history [https://perma.cc/T4JN-5UKF]; *see Sex Offender Enactments Database*, NCSL (Jan. 1, 2018), https://www.ncsl.org/research/civil-and-criminal-justice/sex-offender-enactments-database.aspx [https://perma.cc/WBC8-GTDB] (contains a database of state sex offender laws, with a significant uptick following the passage of the Adam Walsh Child Protection and Safety Act of 2006, which is further discussed below).

law in the United States.[11] This novel law required those convicted of specific sex crimes to register with local law enforcement.[12] Arizona followed with the passage of a similar law in 1951,[13] in addition to four other states by the end of the late 1960s.[14] None of the registries were available to the public.[15] In 1991, Washington became the lone state to implement mandatory community notifications for individuals released following conviction of certain sex crimes.[16] At that point in time, a majority of states did not have registries,[17] and there were no federal requirements whatsoever.[18]

Leading up to the explosion of state registries in 1994, there was a fundamental change in the American psyche. Between 1980 and 1990, the United States saw a roughly thirty-three percent increase in violent crime,[19] and Americans reported high levels of concern about crime in the early 1980s.[20] A handful of high-profile childhood abductions, sexual assaults, and brutal murders led to a widespread panic around "stranger danger."[21] Then, in what was likely the last straw for anxious families and politicians, eleven-

---

[11] *California Sex Offender Registry*, California Department of Justice (Oct. 15, 2022), https://oag.ca.gov/sex-offender-reg [https://perma.cc/6CS3-VPWK].

[12] *Id.*

[13] *See* Ariz. Sess. Laws Ch. 105 § 1 (1951).

[14] Elizabeth Pearson, *Overview of current State laws*, PROC. NAT'L CONF. ON SEX OFFENDER REGISTRIES 45 (1998), https://bjs.ojp.gov/content/pub/pdf/Ncsor.pdf [https://perma.cc/Q5TU-L9QD].

[15] Jennifer Cecil, *Criminal: Sex Offenders: No More Escaping Registration*, 36 MCGEORGE L. REV. 822, 824 (2005). Naturally, these laws also didn't include any Internet restrictions because websites were not generally available to the public until after 1991. Thus, registries were not yet "online." Josie Fischels, *A Look Back at The Very First Website Ever Launched, 30 Years Later*, NPR (Aug. 6, 2021), https://www.npr.org/2021/08/06/1025554426/a-look-back-at-the-very-first-website-ever-launched-30-years-later [https://perma.cc/7D9X-ULY8].

[16] Community Protection Act 1990 Wash. Sess. Laws 12, 13–36. "[T]he [correctional/public safety] department is authorized . . . to release relevant information that is necessary to protect the public . . . ." *Id.* at 17, 18, 20, 26.

[17] *See* Pearson, *supra* note 14. Thirty-eight states did not have registry laws until after 1994. *Id.*

[18] *Legislative History of Federal Sex Offender Registration and Notification*, *supra* note 10.

[19] NATHAN JAMES, CONG. RSCH. SERV., R45236, RECENT VIOLENT CRIME TRENDS IN THE UNITED STATES 2 (2018), https://sgp.fas.org/crs/misc/R45236.pdf [https://perma.cc/T3CY-D45S].

[20] *In Depth Topics: Crime*, GALLUP (Oct. 16, 2022), https://news.gallup.com/poll/1603/crime.aspx [https://perma.cc/CC5S-FP4C]. In 1981, 83% of Americans responded that there was "more" or "the same" amount of crime than there was a year ago, the highest recorded number to date. *Id.* In 1982, 48% of Americans responded that there was an area within 1 mile of their home they "would be afraid to walk alone at night." Also, the highest recorded number to date. *Id.*

[21] Rich Juzwiak, *Half-True Crime: Why the Stranger-Danger Panic of the '80s Took Hold and Refuses to Let Go*, JEZEBEL (Oct. 28, 2020), https://jezebel.com/half-true-crime-why-the-stranger-danger-panic-of-the-8-1845430801 [https://perma.cc/X4UJ-KHLE]. Adam Walsh, Yusuf Bell, and Johnny Gosch were all kids under the age of thirteen that were sexually assaulted, murdered, or vanished in the presumed safety of their own neighborhood. *Id.* "The can't-unsee-able murder of Adam Walsh was made further indelible by a TV movie that aired in 1983 to a reported audience of 38 million people . . . [i]n 1986, the classroom-distributed periodical for kids *Weekly Reader* found in a poll that Stranger Danger and the threat of nuclear war were among the biggest concerns of kids . . . ." *Id.*

year-old Jacob Wetterling was abducted when biking with friends in late 1989.[22] The following year, the Jacob Wetterling Foundation was created,[23] and in 1991, United States Senator Dave Durenberger from Minnesota proposed legislation to create a national registry of sex offenders.[24] Congress acted in 1993 with the passage of the first federal registry law: the Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act ("Wetterling Act").[25] The Wetterling Act was subsequently included in the omnibus Federal Violent Crime Control and Law Enforcement Act of 1994, which President Bill Clinton signed into law that same year.[26]

The Wetterling Act established registry guidelines for all states and applied to any person who committed a criminal sexual act against a minor or a sexually violent offense against an adult.[27] Under this Act, any person required to register must provide their current address, provide notice of any address changes, and submit to being photographed/fingerprinted by law enforcement.[28] The last two sections of the Wetterling Act were arguably the most important. First, the Act provided for registrant privacy, stating that "the information collected under a State registration program shall be treated as private data . . . ." and the disclosure of "relevant information" to non-government actors was only permissible when it was "necessary to protect the public . . . ."[29] The Act did not mandate public disclosure.[30] Second, the Act pushed states to move quickly as it gave them "not more than 3 years" to implement the guidelines or face a ten-percent reduction in specified federal funding.[31] The state scramble to fall into compliance began.

### *B. Dial-Up: Registries Go Online (1995–2005)*

In the blink of an eye, every single state had a registry law on the books.[32] Thirty-eight states had promulgated registries in compliance with the Wetterling Act in under two years, with Massachusetts being the last in

---

[22] *The Jacob Wetterling Investigation*, APM (Oct. 16, 2022), https://features.apmreports.org/in-the-dark/jacob-wetterling-investigation-timeline/ [https://perma.cc/9XTE-X5HE]. Although not confirmed until 2016, Wetterling's abduction was suspected to be related to sexual assault within days of his disappearance. *Id.*

[23] *Id.*

[24] DUCHESS HARRIS, THE HISTORY OF CRIMINAL LAW 11 (2020).

[25] Jacob Wetterling Crimes Against Children Registration Act, H.R. 324, 103rd Cong. (1993).

[26] *Violent Crime Control and Law Enforcement Act of 1994*, U.S. Dept. of Justice (Oct. 24, 1994), https://www.ncjrs.gov/txtfiles/billfs.txt [https://perma.cc/E4YM-J264].

[27] 42 U.S.C. § 14071, *amended* by 42 U.S.C. § 14071 (Supp. I 1996). The Act also included required registration for two crimes against children that did not require sexual elements: kidnapping and false imprisonment. *Id.* at § 14071(a)(3).

[28] *Id.*

[29] *Id.* § 14071(e)(2).

[30] *Id.* § 14071(g)(1)

[31] *Id.* § 14071(f). States were given an additional two-year grace period if they were "making a good effort[] to implement" the law. *Id.* Any state that did not comply within the requisite timeframe had its funding reallocated to other states. *Id.*

[32] Pearson, *supra* note 14.

mid-1996.[33] Then arose another major development: mandatory public disclosure laws. Following another particularly gruesome sexual assault and murder of a child, Megan Kanka, Congress amended the Wetterling Act in 1996 ("Megan's Law").[34] The facts of Megan's case were powerful; her mother stated that "they never would have let their daughter travel their neighborhood freely if they had been alerted to the presence of a convicted sexual offender living across the street from their residence."[35] Megan's Law amended the Wetterling Act to remove the default assumption that registrant data was private, unless an exception applied; it allowed registrant data to be "disclosed for any purposes permitted under the laws of the [s]tate."[36] The purpose of the law was "to increase public awareness of sex offenders in a particular area."[37] Within two years of the passage of Megan's Law, forty-four states implemented statutes that offered public notification systems.[38]

At the same time legislative bodies implemented these new laws, Americans were exposed to the newest technological frontier: the Internet. In 1995, fourteen percent of Americans reported Internet usage, with that number more than doubling to thirty-six percent by the end of 1997.[39] The rapid introduction of widespread Internet access, registry laws, and continued concern about "stranger danger" began to intertwine. First, in 1996, the AMBER Alert system was introduced to alert the public of child abduction through broadcast media.[40] Then, in the same year, after passing Megan's Law, President Bill Clinton signed another amendment to the Wetterling Act into law, known as the "Pam Lychner Sexual Offender

---

[33] *Id.*

[34] *See Legislative History of Federal Sex Offender Registration and Notification*, *supra* note 10.

[35] Pennsylvania State Police, *History of the Law and Federal Facts* (Oct. 16, 2022), https://www.pameganslaw.state.pa.us/InformationalPages/History [https://perma.cc/9LWQ-5QMN]. Megan's sexual assaulter and murderer had two previous sexual convictions against children. *Id.*

[36] Megan's Law, Pub. L. 104-145, § 2, 110 Stat. 1345 (1996).

[37] Pearson, *supra* note 14. Patty Wetterling described Megan's Law as the "equivalent of warning children about a dog in their neighborhood that's known to bite." Jennifer Bleyer, *Patty Wetterling Questions Sex Offender Laws*, Citizens for Criminal Justice Reform – New Hampshire (Aug. 1, 2014), https://www.ccjrnh.org/sex_offender_laws_treatment/patty_wetterling_questions_sex_offender_laws [https://perma.cc/8UUW-LLC3].

[38] Pearson, *supra* note 14. Only five states did not have public notification provisions by mid-1998. *Id.*

[39] *Internet Use Over Time*, PEW RESEARCH CENTER (June 10, 2015), https://www.pewresearch.org/internet/chart/internet-use-over-time/ [https://perma.cc/KFX3-KNXN]. The steepest increase in Internet usage occurred between June 1995 and 1997. Kathryn Zickuhr & Aaron Smith, *Digital Differences*, PEW RESEARCH CENTER (Apr. 13, 2012), https://www.pewresearch.org/internet/2012/04/13/digital-differences/ [https://perma.cc/6H7M-JZ6R].

[40] *AMBER Alert Frequently Asked Questions*, Department of Justice (Jan. 2010), https://www.ojp.gov/sites/g/files/xyckuh241/files/media/document/amberfaq.pdf [https://perma.cc/L359-JF45]. Wireless AMBER Alerts were made available at a later time. *Id.*

Tracking and Identification Act of 1996" ("Pam Lychner Act").[41] While Megan's Law focused on the dissemination of information to the public, the Pam Lychner Act focused on the storage and transmission of data online.[42] It included the creation of the National Sex Offender Registry ("NSOR"), a "national database at the Federal Bureau of Investigation to track the whereabouts and movement [of sex offenders] . . . " regardless of the state having a fully implemented registry program.[43] The NSOR was only accessible by law enforcement,[44] and sought to fill in the gaps between differing state registry laws.[45]

Following more registry regulations signed into law through a federal appropriations bill in 1997,[46] Congress requested that the Attorney General conduct a study of "existing [s]tate programs for informing the public about the presence of sexual predators released from prison . . . including the use of CD-ROMs, Internet databases, and Sexual Offender Identification Hotlines . . . ."[47] At the same time, Elizabeth Pearson, a congressional liaison, noted that "technology has entered the discussion of registration and notification law," including a handful of states offering "sex offender information Web sites."[48] Although there were no federal Internet regulation requirements for sex offenders at the time,[49] inappropriate

[41] *Legislative History of Federal Sex Offender Registration and Notification*, *supra* note 10.

[42] *See* Pam Lyncher Sexual Offender Tracking and Identification Act of 1996, Pub. L. No. 104-236, 110 Stat. 3093–3098 (1996). Pam Lyncher was a survivor of sexual assault who later became an advocate for other victims. The federal legislation was named in her memory after she perished in a plane crash. Greg Abbott, *Justice for Victims, Justice for All*, WOODLANDS ONLINE (Apr. 1, 2008), https://www.woodlandsonline.com/npps/story.cfm?nppage=24252 [https://perma.cc/V5QQ-KSWL].

[43] *Id.* at 3093–3096.

[44] Cornelio v. Connecticut, 32 F.4th 160 (2d Cir. 2022).

[45] *Legislative History of Federal Sex Offender Registration and Notification*, *supra* note 10.

[46] *See Cornelio*, 32 F.4th 160. The appropriations bill included, among other things, a requirement for registered offenders who change their state of residence to register under the new state's laws, a requirement for the Bureau of Prisons to notify state agencies of released or paroled federal offenders and added state offenses to federal standards that are comparable to those listed in the Wetterling Act. *See* Departments of Commerce, Justice, And State, The Judiciary, And Related Agencies Appropriations Act, 1998, Pub. L. 105-119, § 115, 111 Stat. 2440, 2462–2468 (1998). It also included $25 million dollars in funding for the NSOR. *Id.* at 2451.

[47] Protection of Children From Sexual Predators Act of 1998, Pub. L. 105-314, § 902, 112 Stat. 2974, 2991 (1998). This Act also created the Sex Offender Management Assistance Program which required the federal government to "award a grant to each eligible [s]tate to offset costs directly associated with complying with this section (state registration requirements)." *Id.* at 2985.

[48] Pearson, *supra* note 14, at 48.

[49] *See generally* Protection of Children From Sexual Predators Act of 1998, Pub. L. 105-314, § 902, 112 Stat. 2974 (1998); Pam Lyncher Sexual Offender Tracking and Identification Act of 1996, Pub. L. No. 104-236, 110 Stat. 3093–3098 (1996); Megan's Law, Pub. L. 104-145, § 2, 110 Stat. 1345 (1996).

Internet use by sex offenders was a policy concern for members of Congress.[50]

At the turn of the twenty-first century, a milestone was reached: over fifty percent of Americans identified as Internet users.[51] Just under a decade after Congress made history by passing the Wetterling Act, it enacted the first registry requirement that involved the Internet, the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act ("PROTECT Act").[52] The PROTECT Act required state registries to "include the maintenance of an Internet site containing [sex offender registry] information. . . ." and instructed the Department of Justice to "create a national Internet site that links all State Internet sites established pursuant to this section."[53] The PROTECT Act gave all states three years to comply with the requirement of having online, publicly available registries or risk falling out of compliance with the law.[54] Slowly but surely, registries were becoming fully "online."

As states across the country rapidly introduced and modified regulations to comply with federal requirements, more sex offenders began to challenge the constitutionality of registries.[55] In Alaska, a state registry law followed Megan's Law and provided for a publicly available Internet registry database.[56] Multiple sex offenders who were required to register under Alaska's law sued, claiming that the law violated the *Ex Post Facto* Clause of the Constitution.[57] The Supreme Court held that the registry law did not violate the *Ex Post Facto* Clause because the "imposition of restrictive measures on sex offenders adjudged to be dangerous is a legitimate nonpunitive governmental objective and has been historically so regarded."[58] Further, "where a legislative restriction is an incident of the State's power to

---

[50] Protection of Children From Sexual Predators Act of 1998, Pub. L. 105-314, § 801, 112 Stat. 2974, 2990 (1998). Here, the congressional record discussed a case in which a Minnesota prisoner had unsupervised access to the Internet and obtained significant amounts of child pornography. *Id.* § 802. This led to a recommended prohibition on unsupervised Internet use for prisoners due to "an explosion in the use of the Internet in the United States, further placing our Nation's children at risk of harm and exploitation at the hands of predators on the Internet . . . ." *Id.*

[51] *Internet Use Over Time*, *supra* note 39.

[52] *See* Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003, Pub. L. No. 108-21, 117 Stat. 650, 651–688 (2003).

[53] *Id.* at 688.

[54] *Id.* States were given an additional two years to implement the law so long as they showed a "good faith effort" to come into compliance with the law. *Id.*

[55] *See generally* Smith v. Doe, 538 U.S. 84 (2003) (Supreme Court case in which a sex offender challenged the Alaska registry on *ex post facto* concerns); Connecticut Dep't. of Public Safety v. Doe, 538 U.S. 1 (2003) (Supreme Court case in which a sex offender challenged the Connecticut registry on due process concerns).

[56] *See* Smith v. Doe, 538 U.S. 84, 84–86, 89 (2003).

[57] *Id.* at 91. The Alaska law required "any sex offender or child kidnaper . . . [to] register with the Department of Corrections . . . providing his name, address, and other specified information." *Id.* at 84. The information made available to the public included the sex offender's name, address, photograph, and physical description, among other things. *Id.* at 90–91.

[58] *Id.* at 93 (internal quotation marks omitted) (quoting Kansas v. Hendricks, 521 U.S. 346, 363 (1997)).

protect the health and safety of its citizens, [the restriction] will be considered as evidencing an intent to exercise that regulatory power . . . ."[59]

In another state, Connecticut, the state registry law required the Department of Public Safety to "post a sex offender registry containing registrants' names, addresses, photographs, and descriptions on a[] [public] Internet Website."[60] A registered sex offender sued on the grounds that the Connecticut law violated the Due Process Clause of the Fourteenth Amendment because it "deprive[d] him of a liberty interest—his reputation combined with the alteration of his status under state law—without notice or a meaningful opportunity to be heard."[61] The Supreme Court again declined to strike down the registry law.[62]

By the turn of the twenty-first century, the majority of states had implemented public notification registry requirements,[63] the Supreme Court had upheld two registry statutory schemes,[64] and the march to keep up with rapid developments in Internet use accelerated.[65] At that moment in time, two additional facts were clear. First, registry requirements, including public disclosure requirements on the Internet, were constitutionally permissible.[66] Second, despite registries going "online," the actual *registrants* of these registries did not have any regulations around *their own* Internet usage.[67] Sex offenders still retained their First Amendment rights to speak and engage freely on the Internet.

### *C. High-Speed: The Vast Expansion of Registry Internet Regulations (2006–present)*

By the end of 2004, what was once a rarity had become a common utility, as roughly two-thirds of Americans were using the Internet.[68] With an ever-growing majority of Americans online, the 1980s and 1990s panic around "stranger danger" evolved with the times.[69] Then, on July 27, 2006,

---

[59] *Id.* at 93–94 (internal quotations marks omitted) (quoting Flemming v. Nestor, 363 U.S. 603, 616 (1960)).
[60] Conn. Dep't of Pub. Safety v. Doe, 538 U.S. 1, 1 (2003).
[61] *Id.* at 6.
[62] *Id.* at 8. The Court found that the law did not violate procedural due process because "[procedural] due process does not require the [offender to be awarded an] opportunity to prove a fact that is not material to the State's statutory scheme." *Id.* at 4.
[63] *See* Pearson, *supra* note 14, at 45.
[64] *See Smith*, 538 U.S. 84; *see also Conn. Dep't of Pub. Safety*, 538 U.S. 1.
[65] *See Ten Years of Protecting Our Children: Cracking Down on Sexual Predators on the Internet*, FBI (Dec. 12, 2003), https://archives.fbi.gov/archives/news/stories/2003/december [https://perma.cc/2958-WJ5T].
[66] *See Smith*, 538 U.S. 84; *see also Conn. Dep't of Pub. Safety*, 538 U.S. 1.
[67] *See Legislative History of Federal Sex Offender Registration and Notification*, *supra* note 10. The first federal law regulating registrant Internet use did not come until 2008. *See* Keeping the Internet Devoid of Sexual Predators Act of 2008, Pub. L. No.110-400, 122 Stat. 4224 (2008).
[68] *See Internet Use Over Time*, *supra* note 39.
[69] *See* Brian Stelter, '*To Catch a Predator' Is Falling Prey to Advertisers' Sensibilities*, N.Y.

a watershed moment occurred for sex offender registries: President George W. Bush signed "the most comprehensive national standards . . . for monitoring sex offenders in America's communities."[70] This comprehensive national standard was the Adam Walsh Child Protection and Safety Act ("Adam Walsh Act"), and it contained the first expansive Internet regulations in a federal registry law.[71]

The Adam Walsh Act honed in on sex offenders and Internet usage in three ways. First, the Act expanded state registry requirements to include "[c]riminal sexual conduct involving a minor, *or the use of the Internet to facilitate or attempt such conduct*."[72] Second, it mandated that more information about registrants be provided on the Internet.[73] Third, it directed the Attorney General to develop a new website to link all state registry databases together[74] and to study the effectiveness of "limiting access by sex offenders to the Internet or to specific Internet sites."[75] Like the Wetterling Act signed into law over a decade before, states that did not come into compliance with these three requirements would lose ten percent

---

TIMES (Aug. 27, 2007), https://www.nytimes.com/2007/08/27/business/media/27predator.html [https://perma.cc/34P9-L28G] (highlighting the success and failures of NBC's investigative segment "To Catch a Predator," which first aired in 2004 and focused on Chris Hansen confronting "men trolling online chat rooms hoping to meet teenagers for sex"). Hansen also stated that "[t]here was a time not long ago when stories about Internet crimes were a tough sell for TV newsmagazines." *Id. See also About iKeepSafe*, IKEEPSAFE, https://ikeepsafe.org/about/ [https://perma.cc/JQ8C-95ZS] (information about the organization, founded in 2005, dedicated to "a national effort promoting the safe and healthy use of technology.") *Id.* The same organization also released a document, titled *Statistics: Kids Online Are in Danger*, highlighting the dangers of sexual predators online. *See Statistics: Kids Online Are in Danger*, IKEEPSAFE, https://www.optimist.org/InternetSafety/iKeepSafe-Statistics.pdf [https://perma.cc/5BPG-Q6S7].

[70] Emanuella Grinberg, *5 Years Later, States Struggle to Comply with Federal Sex Offender Law*, CNN (July 28, 2011), http://www.cnn.com/2011/CRIME/07/28/sex.offender.adam.walsh.act/index.html [https://perma.cc/VA6V-AUM7]. Before signing the new regulations, President Bush stated: "[T]he bill I sign today will strengthen Federal laws to protect our children from sexual and other violent crimes . . . [and] make it harder for sex predators to reach our children on the internet. Some sex predators use this technology to make contact with potential victims, so the bill authorizes additional new regional Internet Crimes Against Children Task Forces." *Remarks on Signing the Adam Walsh Child Protection and Safety Act of 2006*, THE AMERICAN PRESIDENCY PROJECT (July 27, 2006), https://www.presidency.ucsb.edu/documents/remarks-signing-the-adam-walsh-child-protection-and-safety-act-2006 [https://perma.cc/35UH-EJ9N].

[71] *See* Adam Walsh Child Protection and Safety Act of 2006, Pub. L. No. 109-248, 120 Stat. 587 (2006) (codified as amended at 34 U.S.C. §§ 20901–20991) (stating in the preamble the goal of "promot[ing] Internet safety" as well as containing the word "Internet" 45 times).

[72] *See* 34 U.S.C. § 20911(7)(H) (2022) (emphasis added). This was the first time the use of Internet to "facilitate" a sex crime was added as a state registry requirement to a federal law. *See Legislative History of Federal Sex Offender Registration and Notification*, *supra* note 10.

[73] 34 U.S.C. § 20920 (2022).

[74] *Id.* § 20922.

[75] Adam Walsh Child Protection and Safety Act of 2006, Pub. L. No. 109-248, § 638, 120 Stat. 587 (2006).

of specific crime funding.[76] Despite the revolutionary change the Adam Walsh Act brought to state registry laws across the nation, it stood at the precipice of *directly* regulating registrant Internet usage. Direct regulation, in typical rapid registry evolution fashion, would come just two years later.[77]

Even though significant pieces of the Adam Walsh Act have faced legal and political scrutiny over the past fifteen years,[78] it is a lesser-known 2008 amendment to the law that is of potentially greater consequence.[79] The Keeping the Internet Devoid of Sexual Predators Act of 2008 ("KIDS Act") compelled state registry laws to enter a completely new terrain by mandating sex offenders provide *their own* Internet-related information to state registries.[80] Specifically, the law directed the Attorney General to "require that each sex offender provide to the sex offender registry those Internet identifiers the sex offender uses or will use of any type that the Attorney General determines to be appropriate."[81] It defined "Internet identifiers" as

[76] 34 U.S.C. § 20927(a). The Act also included other new mandates for state registry requirements that were not related to the Internet. This included: new "registration and notification standards," an expansion of "the number of sex offenses that must be captured by registration jurisdictions," the creation of the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART Office), and more. *Legislative History of Federal Sex Offender Registration and Notification*, *supra* note 10. Unlike the rapid state compliance following the previous federal registry regulations, only fourteen states had "substantially complied" with the requirements by mid-2011. Pearson, *supra* note 14, at 45; Grinberg, *supra* note 70. State registries substantially grew, even up to 500%, following the implementation of the Walsh Act. *Id.*

[77] *See* Keeping the Internet Devoid of Sexual Predators Act of 2008, Pub. L. No. 110-400, 122 Stat. 4224 (codified as amended in scattered sections of 42 U.S.C.).

[78] *See* United States v. Comstock, 560 U.S. 126, 149 (2010) (finding Congress had the constitutional authority to pass the Adam Walsh Act); *see also No Easy Answers: Sex Offender Laws in the US*, 19 HUM. RTS. WATCH, no. 4(G) (Sept. 2007), https://www.hrw.org/sites/default/files/reports/us0907webwcover.pdf [https://perma.cc/7PCJ-WZ6G]. Patty Wetterling, who helped spearhead the original Wetterling Act, expressed her concerns of the evolving registry requirements following the passage of the Adam Walsh Act. *Id.* at 4. "I have a tremendous amount of respect for what John and Reve Walsh have done in [spearheading the Adam Walsh Act] . . . I just think some of this really angry, punitive stuff is letting the bad guys win. They're building a world that isn't caring and believing in one another." Jennifer Bleyer, *Patty Wetterling Questions Sex Offender Laws*, CITIZENS FOR CRIM. JUST. REFORM – N. H. (Aug. 1, 2014), https://www.ccjrnh.org/sex_offender_laws_treatment/patty_wetterling_questions_sex_offender_laws [https://perma.cc/8UUW-LLC3].

[79] *See* Doe v. Harris, 772 F.3d 563, 583 (9th Cir. 2014) (finding that California's "Internet identifier" requirements were not "narrowly tailored to serve an important government interest"); Cornelio v. Connecticut, 32 F.4th 160, 177 (2d Cir. 2022) (main case at issue in this Note that also found "Internet identifier" requirement for sex offenders to potentially be unconstitutional); Jones v. Stanford, 489 F. Supp. 3d 140, 154 (E.D.N.Y. 2020) (permitting an injunction of New York's law requiring disclosure of "Internet identifiers" for some sex offenders on the grounds that it violated First Amendment rights).

[80] *See* Keeping the Internet Devoid of Sexual Predators Act of 2008, Pub. L. No. 110-400, 122 Stat. 4224 (codified as amended in scattered sections of 42 U.S.C.). The Act also included a mandate for the Attorney General to "establish and maintain" a system in which social media websites can compare sex offender registry databases. If a match was found, the social media website could request the Attorney General provide information related to the identity of the individual. *Id.* at 4225.

[81] *Id.* at 4224.

the "electronic mail addresses and other designations used for self-identification or routing in Internet communication or posting."[82] The KIDS Act mandated that "Internet identifiers" were barred from public disclosure.[83] Even though many states have yet to "substantially implement" all requirements set forth in the Adam Walsh Act,[84] most states have met the "Internet identifier" requirements pursuant to the KIDS Act.

In states that have implemented "Internet identifier" requirements, there are some similarities and differences in definitions and scope. For example, in Alabama, "Internet identifiers" are defined as including "any designations or monikers used for self-identification in Internet communications or postings other than those used exclusively in connection with a lawful commercial transaction."[85] In Florida, they are "any designation, moniker, screen name, username, or other name used for self-identification to send or receive social Internet communication."[86] In other states, rather than defining an "Internet identifier," the law simply requires a sex offender to provide "e-mail addresses, instant-messaging identities, or chat room identities" or "each electronic mail address, instant messaging address, and other Internet communication identifier used."[87] The laws differ on what type of offenders need to produce Internet identifiers, along with the timeliness and offender effort in disclosure,[88] but ultimately fall within the guidelines set out in the KIDS Act.[89]

Regardless of the nuances in each state's "Internet identifier" registry requirements, one universal fact exists: each law implicates constitutionally protected speech rights that were left untouched prior to the passage of the KIDS Act in 2008.[90] By implicating protected speech rights, there was a significant departure from the days of the Wetterling Act and

---

[82] *Id.* at 4225.

[83] 34 U.S.C. § 20916(c).

[84] *See generally Sex Offender Registration and Notification Act (SORNA) State and Territory Implementation Progress Check*, OFF. OF SEX OFFENDER SENTENCING, MONITORING, APPREHENDING, REGISTERING, AND TRACKING (Jan. 25, 2022), https://smart.ojp.gov/sites/g/files/xyckuh231/files/media/document/SORNA%20progress%20check%2001252022.pdf [https://perma.cc/RY2C-CS6E].

[85] ALA. CODE § 15-20A-7(a)(9) (2022).

[86] FLA. STAT. § 775.21(2)(j) (2021).

[87] *See* COLO. REV. STAT. § 16-22-108(2.5)(a) (2021); *see also* ALASKA STAT. § 12.63.010(b)(1)(I) (2022).

[88] ALA. CODE § 15-20A-7 (2022); ALASKA STAT. § 12.63.010 (2022); COLO. REV. STAT. § 16-22-108 (2021); FLA. STAT. § 775.21 (2021); VA. CODE ANN. § 9.1-903 (2022).

[89] *See* Keeping the Internet Devoid of Sexual Predators Act of 2008, Pub. L. No. 110-400, 122 Stat. 4224 (codified as amended in scattered sections of 42 U.S.C.). In tracking state compliance with SORNA and components of the KIDS Act, SMART tracks "information sharing" for state compliance, which includes "all identification and location information in registry." OFF. OF SEX OFFENDER SENTENCING, MONITORING, APPREHENDING, REGISTERING, AND TRACKING, *supra* note 84.

[90] Packingham v. North Carolina, 137 S. Ct. 1730, 1372 (2017) ("Here [is] one of the first cases the Court has taken to address the relationship between the First Amendment and the modern Internet . . . ."); Doe v. Harris, 772 F.3d 563, 568 (9th Cir. 2014) ("In 2012, California voters passed Proposition 35, known as the CASE Act, which added provisions to California's sex offender registration requirements related to Internet usage by persons subject to the Act.").

Megan's Law, where registry laws across the country were constitutionally sound and more easily implemented.[91] Even including the complications and disagreements brought about by the Adam Walsh Act, that law withstood the test of constitutional scrutiny at the nation's highest court.[92] The new "Internet identifier" registry requirements across the United States have, however, opened a new bandwidth for a direct collision course with protected speech under the First Amendment.

## III. FIRST AMENDMENT JURISPRUDENCE: THE FREE SPEECH CLAUSE

The First Amendment of the United States Constitution provides that "Congress shall make
no law . . . abridging the freedom of speech" ("Free Speech Clause").[93] Since the 1920s, the Free Speech Clause of the First Amendment has applied to the states.[94] Before an analysis of the "Internet identifier" First Amendment issues, it is necessary to understand what the Free Speech Clause framework looks like and how it is applied in the context of Internet identifier cases before the federal judiciary.

### *A. Judicial Interpretation of the Free Speech Clause*

Despite the brevity of the Free Speech Clause, its judicial interpretation has been far more complex.[95] Of the utmost importance, the Supreme Court recognizes the Free Speech Clause as extending to individual and collective speech "in pursuit of a wide variety of political, social, economic, educational, religious, and cultural ends."[96] When a federal or state

---

[91] *See* Smith v. Doe, 538 U.S. 84, 105–06 (2003) (Supreme Court upholding Alaska's registry in compliance with Megan's Law); Pearson, *supra* note 14, at 45–48 (showing registry laws being enacted across all 50 states within a few years of the passage of the Wetterling Act and Megan's Law).

[92] *See* United States v. Comstock, 560 U.S. 126, 148 (2010) (holding that requirements of the Adam Walsh Act were "narrow in scope").

[93] U.S. CONST. amend. I.

[94] *See* Gitlow v. New York, 268 U.S. 652, 666 (1925) (deciding that the Fourteenth Amendment to the Constitution applies to the governments of U.S. states); Stromberg v. California, 283 U.S. 359, 369–70 (1931) (finding that a state statute banning flag burning violated the First Amendment).

[95] Brent Ferguson, *The Distillery: The Constant Evolution of the First Amendment*, BRENNAN CTR. FOR JUST. (Sept. 4, 2015), https://www.brennancenter.org/our-work/analysis-opinion/distillery-constant-evolution-first-amendment [https://perma.cc/4A6L-2B4H] ("Interpretation of the First Amendment has changed radically in the past few decades."); *see* Stephen J. Wermiel, *The Ongoing Challenge to Define Free Speech*, 43 ABA HUM. RTS. MAG. 4, https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/the-ongoing-challenge-to-define-free-speech/the-ongoing-challenge-to-define-free-speech/ [https://perma.cc/V894-VFEY].

[96] Roberts v. U.S. Jaycees, 468 U.S. 609, 622 (1984). The Supreme Court has held that speech is generally protected pursuant to the Free Speech Clause unless it is deemed to be "unprotected." VICTORIA L. KILLION, CONG. RSCH. SERV., IF11072, THE FIRST

legislative body passes a law that possibly implicates individual or collective protected speech, judges must conduct a "test" to determine if the law is constitutional.[97] As part of this test, judges are tasked with determining what level of "scrutiny" to apply and whether the law "passes" that level of scrutiny.[98] Laws that do not pass the appropriate level of scrutiny violate the Free Speech Clause and are deemed unconstitutional.[99]

### *1. Protected Speech Framework*

The First Amendment, according to the Supreme Court, is "fashioned to assure unfettered interchange of ideas for the bringing about of political and social changes desired by the people"[100] and to "expressly target[] the operation of [] laws . . . rather than merely the motives of those who enacted them."[101] The Court has emphasized how "[p]recision of regulation must be the touchstone in an area so closely touching our most precious freedoms."[102] In their pursuit of legislative precision surrounding protected speech, the Court has established a precedent of distinguishing between "content-based" and "content-neutral" regulations of speech.[103] Content-based regulations "target speech based on its communicative content," while content-neutral regulations do not target the content of speech.[104]

When a law implicating speech is a content-based regulation, courts generally presume the law is unconstitutional unless the government proves the law is narrowly tailored to serve a compelling state interest.[105] This is called "strict scrutiny,"[106] and when it applies to a law under the Free Speech Clause, the law rarely survives judicial review.[107] On the other hand, when a

---

AMENDMENT: CATEGORIES OF SPEECH (2019). Although the Court has identified eight categories of unprotected speech, the issues discussed in this Note do not fit into any of those categories. *Id.*

[97] *See* KILLION, *supra* note 96.

[98] *See id.*

[99] *See generally id.*

[100] Dun & Bradstreet v. Greenmoss Builders, 472 U.S. 749, 759 (1985) (quoting Roth v. United States 354 U.S. 476, 484 (1957)).

[101] Reed v. Town of Gilbert, 576 U.S. 155, 167 (2015).

[102] NAACP v. Button, 371 U.S. 415, 438 (1963).

[103] *See* Nat'l Inst. of Fam. & Life Advocs. v. Becerra, 138 S. Ct. 2361, 2371 (2018).

[104] *See id.*; *see also* David L. Hudson Jr., *Content Neutral*, FIRST AMEND. ENCYC., https://www.mtsu.edu/first-amendment/article/937/content-neutral [https://perma.cc/Q7S7-P2RX] ("Content neutral refers to laws that apply to all expression without regard to the substance or message of the expression.").

[105] *See Becerra*, 138 S. Ct. at 2371.

[106] *See Reed*, 576 U.S. at 172.

[107] *See* Sable Commc'ns of Cal. v. F.C.C., 492 U.S. 115, 131 (1989) (The law at issue prohibited adults from sending and receiving obscene and indecent material; it triggered strict scrutiny and was unconstitutional.); Simon & Schuster v. Members of the N.Y. State Crime Victims Bd., 502 U.S. 105, 123 (1991) (The law at issue prohibited perpetrators of crimes from profiting off of their related written work; it triggered strict scrutiny and was

law implicating speech is a content-*neutral* regulation, a lesser level of scrutiny is applied.[108] This lesser level of scrutiny still requires the law to be narrowly tailored, but must only serve a *substantial*, *legitimate*, or *important* state interest.[109] In these circumstances, the court is looking for restrictions on speech that are "justified" but "need not be the least restrictive or least intrusive means of doing so . . . ."[110] How a state interest is deemed "substantial" or "important" is highly contextualized based on a court's interpretation of common sense.[111]

It may be easy to identify potentially protected speech when the speech is spoken or written, but what about circumstances when the actual "speech" has not happened yet? Courts have held that the Free Speech Clause may still be violated by "chilling effect[s] of governmental action that fall[] short of a direct prohibition against speech."[112] Thus, "[w]hen a law imposes 'special obligations' or 'special burdens' on those engaged in speech, 'some measure of heightened First Amendment scrutiny is demanded.'"[113] This includes disclosure requirements that single out "conduct with a significant expressive element."[114] In short, when courts consider what implicates "protected speech," it does not *literally* have to be verbal speech but can be behaviors and activities associated with "protected speech."[115]

There are three other essential components in the protected speech framework: the "overbreadth doctrine," vagueness/ambiguity in statutory construction, and anonymous speech. First, the "overbreadth doctrine prohibits the Government from banning unprotected speech if a substantial amount of protected speech is prohibited or chilled in the process."[116] For example, a statute that prohibits the exchange of child pornography may be constitutional because child pornography is unprotected speech, but a statute that prohibits the exchange of child pornography *and* more content that is protected is unconstitutional.[117] Second, statutes that contain "words

---

unconstitutional.); Boos v. Barry, 485 U.S. 312, 334 (1988) (The law at issue prohibited individuals from holding signs critical of foreign governments near that foreign government's embassy; it triggered strict scrutiny and was unconstitutional).

[108] *See Boos*, 485 U.S. at 321.

[109] *See* Ward v. Rock Against Racism, 491 U.S. 781, 796 (1989).

[110] *Rock Against Racisim*, 491 U.S. at 798–800.

[111] *See* Doe v. Harris, 772 F.3d 563, 577 (9th Cir. 2014) ("*Unquestionably*, the State's interest in preventing and responding to crime, particularly crimes as serious as sexual exploitation and human trafficking, is legitimate." (emphasis added)); Doe v. Shurtleff, 628 F.3d 1217, 1223 (10th Cir. 2010) ("*We have no doubt* that the State of Utah has a compelling interest in investigating kidnapping and sex-related crimes." (emphasis added)). It can be deduced in both instances that the judges did not question the government's interest, nor did they use any "test" to reach their conclusions.

[112] *See* Aebisher v. Ryan, 622 F.2d 651, 655 (2d Cir. 1980) (quoting Reps. Comm. for Freedom of Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1052 (D.C. Cir. 1978)).

[113] Cornelio v. Connecticut, 32 F.4th 160, 169 (2d Cir. 2022) (quoting Turner Broad. Sys., Inc. v. F.C.C., 512 U.S. 622, 641 (1994)).

[114] *See* Arcara v. Cloud Books, Inc., 478 U.S. 697, 706–07 (1986).

[115] *See* Texas v. Johnson, 491 U.S. 397, 404 (1989).

[116] Ashcroft v. Free Special Coal., 535 U.S. 234, 255 (2002).

[117] *See id.*

and phrases [that] are so vague and indefinite that any penalty prescribed for their violation constitutes a denial of due process of law" are constitutionally problematic.[118] Lastly, the ability of individuals to speak anonymously has been highlighted in major court cases.[119] Taken together, appellate courts, including the Supreme Court, have set a protected speech framework to best understand the scope of the Free Speech Clause.

### *2. "Internet Speech" as Protected Speech*

With the advent of widespread Internet use in the late 1990s,[120] the Supreme Court began its foray into applying the First Amendment speech test to "Internet speech."[121] The first major Supreme Court case illustrating this was *Reno v. ACLU* in 1997.[122] In *Reno*, the Court noted that

> the Internet can hardly be considered a "scarce" expressive commodity. It provides relatively unlimited, low-cost capacity for communication of all kinds. . . . Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer.[123]

The Court in *Reno* ultimately held that there was "no basis for qualifying the level of First Amendment scrutiny that should be applied to [the Internet],"[124] and opined that "narrow tailoring" was required to "save an

---

[118] *See Champlin Refining Corp.*, 286 U.S. at 243; Papachristou v. City of Jacksonville, 405 U.S. 156, 156 n.1 (1972) (finding restrictions on "wandering or strolling around from place to place without any lawful purpose or object" violated the Due Process Clause of the Fourteenth Amendment due to vagueness).

[119] Doe v. Harris, 772 F.3d 563, 574 (9th Cir. 2014) ("[A]n 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.") (quoting McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995)).

[120] *See 1960s – 1990s: Internet*, ELON UNIV., https://www.elon.edu/u/imagining/time-capsule/150-years/back-1960-1990/ [https://perma.cc/QH9M-D2GT] (noting that the creation of the World Wide Web made the Internet "much easier to use because all documents could be seen easily on-screen without downloading").

[121] *See* John Schwartz and Joan Biskupic, *Supreme Court Rejects Curbs on Online Speech*, WASH. POST (June 27, 1997), https://www.washingtonpost.com/wp-srv/national/longterm/supcourt/stories/internet.htm [https://perma.cc/Y3B7-HVHT] ("Jerry Berman of the Center for Democracy and Technology. . . called the decision 'the Bill of Rights for the 21st Century.'"). Senator Patrick J. Leahy of Vermont said that "[t]his is a victory for the First Amendment." *Id.*

[122] *See* Reno v. ACLU, 521 U.S. 844, 849 (1997) (holding unanimously that the Communications Decency Act of 1996, which made it illegal for anyone to knowingly transmit "obscene or indecent" messages to anyone under the age of eighteen, was unconstitutional by violating the First Amendment).

[123] *Id.* at 870.

[124] *Id.*

otherwise patently invalid unconstitutional provision."[125] The widespread use of the Internet may have been new, but many elements of the traditional protected speech test remained.

Twenty years after *Reno*, the Court further emphasized the importance of protecting Internet speech adjacent to that of "Internet identifier" requirements.[126] In *Packingham v. North Carolina*, the Court stated that "[w]hile in the past there may have been difficulty in identifying the most important places [] for the exchange of views, today the answer is clear. It is cyberspace—the 'vast democratic forums of the Internet' in general . . . and social media in particular."[127] The Court found a North Carolina law prohibiting sex offenders from using "social media" websites unconstitutional.[128] Despite finding that "[s]ocial media allows users to gain access to information and communicate with one another about it on any subject that might come to mind," the Court determined that "to foreclose access to social media altogether is to prevent the user from engaging in the legitimate exercise of First Amendment rights."[129] It further held, "[i]t is well established that, as a general rule, the Government 'may not suppress lawful speech as the means to suppress unlawful speech,'" and pronounced, "[t]hat is what North Carolina has done here. Its law must be held invalid."[130] *Packingham* made it clear that protected speech not only applies to Internet speech, but it is deserving of constitutional safeguarding, even for those society deems most contemptible.[131]

### *B. The Free Speech Clause Applied to Internet Identifier Laws*

Since the passage of the KIDS Act in 2008 and states subsequently implementing Internet identifier registry laws, there have been three essential appellate court applications of the Free Speech Clause:[132] *Doe v. Shurtleff*, decided in 2010; *Doe v. Harris*, decided in 2014; and most recently, *Cornelio v. Connecticut*, decided in 2022.[133] Understanding the facts and application of the protected speech framework in each case sets up the necessary foundation for analyzing the unconstitutionality of many Internet identifier laws today.

#### *1.* Doe v. Shurtleff *(2010 Tenth Circuit Case)*

[125] *See id.* at 882 (finding the statute unconstitutional, likening it to "burning the house to roast the pig").
[126] *See generally* Packingham v. North Carolina, 582 U.S. 98 (2017).
[127] *Id.* at 104 (quoting *Reno*, 521 U.S. at 868).
[128] *Id.*
[129] *Id.* at 107–09 (quoting Ashcroft v. Free Special Coal., 535 U.S. 234, 255 (2002)).
[130] *Id.*
[131] *See id.* at 107.
[132] *See* Doe v. Shurtleff, 628 F.3d 1217 (10th Cir. 2010); Doe v. Harris, 772 F.3d 563, 568 (9th Cir. 2014); Cornelio v. Connecticut, 32 F.4th 160 (2d Cir. 2022).
[133] *See id.*

The first time Internet identifier registry laws reached the federal court of appeals was in *Doe v. Shurtleff*.[134] The case was brought after Utah enacted an Internet identifier law in 2008.[135] The law required registrants to provide "Internet identifiers . . . [and] the name and Internet address of all websites on which the sex offender is registered using an online identifier, including all online identifiers and passwords used to access those websites . . . ."[136] The United States District Court for the District of Utah concluded that the law violated the First Amendment because even though it served a compelling state interest, the statute was not written in the least restrictive means possible.[137] The Utah legislature responded by amending the Internet identifier statute the following year to explicitly exclude passwords from the definition of Internet identifiers and prohibit the disclosure of Internet identifiers to the public in most circumstances.[138]

Following the amendments to the Utah Internet identifier law, the government argued before the United States District Court for the District of Utah that the amendment rectified any constitutional issues.[139] The district court conducted an analysis of the statute under "exacting scrutiny," a very similar framework to intermediate scrutiny,[140] and found that the Internet identifier law no longer burdened core political speech.[141] Because of this, the district court held that the "[r]egistry [s]tatute now complies with the requirements of the First Amendment," and thus, the newly amended law could stand.[142]

The Tenth Circuit affirmed the lower court.[143] The appellate court applied intermediate scrutiny because it found the law to be content-neutral.[144] The plaintiff argued that the possibility of disclosure of Internet identifiers to the public chilled his speech, but the appellate court disagreed on the grounds that the sharing of information under the statute was for "limited law-enforcement purposes."[145] The plaintiff further argued that disclosure of Internet identifiers to the government *in and of itself* chilled

---

[134] 628 F.3d at 1120.

[135] *See* Doe v. Shurtleff, No. 1:08-CV-64-TC, 2009 U.S. Dist. LEXIS 73955, at *1–2 (D. Utah Aug. 20, 2009).

[136] UTAH CODE ANN. § 77-27-21.5(14)(i) & (j) (2008).

[137] *See Shurtleff*, 2009 U.S. Dist. LEXIS 73955, at *3.

[138] *See id.*

[139] *See id.* at *6.

[140] *Id.* at *9 ("Under exacting scrutiny, 'the government may "regulate the content of constitutionally protected speech in order to promote a compelling interest if it chooses the least restrictive means to further the articulated interest."'") (quoting ACLU v. Johnson, 194 F.3d 1149, 1156 (10th Cir. 1999)).

[141] *See id.* at *10–11.

[142] *Id.* at *12.

[143] *See* Doe v. Shurtleff, 628 F.3d 1217, 1227 (10th Cir. 2010).

[144] *Id.* at 1223 ("The law says nothing about the ideas or opinions that [the plaintiffs] may or may not express, anonymously or otherwise. Neither is it aimed at 'supress[ing] the expression of unpopular views . . . .'") (quoting Am. Target Advert., Inc. v. Giani, 199 F.3d 1241, 1247 (10th Cir. 2000) (alteration in original)).

[145] *Id.* at 1224–25. The plaintiff argued that the disclosure of Internet identifiers potentially chilled his speech because it removed his ability to speak anonymously. *See id.* at 1222.

protected speech.[146] The court again disagreed, finding that the statute only allowed state actors "to look beyond the anonymity surrounding a username in the course of an investigation *after* a new crime has been committed."[147] Lastly, the plaintiff unsuccessfully argued that the statute was unconstitutionally overbroad because it was not "narrowly drawn to serve the stated purpose of investigating sex-related crimes."[148] Ultimately, Utah's Internet identifier registry requirements met intermediate scrutiny and were found permissible under the First Amendment.[149]

### *2.* Doe v. Harris *(2014 Ninth Circuit Case)*

On November 6, 2012, eighty-one percent of California voters passed Proposition 35, the most popular ballot measure in California state history.[150] Proposition 35 required, among other things, that sex offenders provide the government with "[a] list of any and all Internet identifiers established or used by the person" and that they "*shall send written notice* of the addition or change [of Internet identifiers] to the law enforcement agency or agencies with which he or she is currently registered *within 24 hours*."[151] Proposition 35 further defined Internet identifiers as "an electronic mail address, user name, screen name, or similar identifier used for the purpose of Internet forum discussions, Internet chat room discussions, instant messaging, social networking, or similar Internet communication."[152]

Following the passage of Proposition 35, a group of plaintiffs filed suit in *Doe v. Harris* on the grounds that the ballot measure violated their First Amendment speech rights.[153] In 2013, the Northern District Court of California noted that the First Amendment was implicated in this case because "speech by sex offenders who have completed their terms of probation or parole enjoy the full protection of the First Amendment."[154]

---

[146] *Id.* at 1225.

[147] *Id.* at 1225 (emphasis added). Under the law, the state could "use an offender's internet identifiers 'to assist in investigating kidnapping and sex-related crimes, and in apprehending offenders . . . ." *Id.* (quoting UTAH CODE ANN. § 77-27-21.5(2) (2005) (repealed 2012)).

[148] *Id.* at 1225–26 (citing Appellant's Reply Brief at 18). The statute included kidnapping offenses that did not include a sexual element. *See id.* The appellate court was unpersuaded because "individuals convicted of kidnapping offenses [did not] constitute 'third parties whose speech is more likely to be protected by the First Amendment than the plaintiff's speech.'" *Id.* at 1226 (quoting D.L.S. v. Utah, 374 F.3d 971, 976 (10th Cir. 2004)).

[149] *See id.* at 1225–26.

[150] *See* Ashley Zavala, *Ballot Propositions Historically Don't Do Well in California*, KCRA 3 (Nov. 2, 2022), https://www.kcra.com/article/ballot-propositions-dont-do-well-in-california/41849781 [https://perma.cc/K77T-4ZMQ].

[151] Doe v. Harris, 772 F.3d 563, 568 (9th Cir. 2014) (quoting CAL. PENAL CODE § 290.015(a)(4)(5)) (emphasis added).

[152] *Id.* at 569 (quoting CAL. PENAL CODE § 290.015(b)).

[153] No. C12-5713 TEH, 2013 U.S. Dist. LEXIS 5428 (N.D. Cal. Jan. 11, 2013). The plaintiffs included two convicted sex offenders and an organization called "California Reform Sex Offender Laws." *Id.* at *2. The Proposition was prevented from implementation by a federal judge the day after voters overwhelmingly voted for it. *Id.* at *2, 5–6.

[154] *Id.* at *8–9.

Then, the district court applied *intermediate scrutiny*, seeking to determine if the Internet identifier requirement for Proposition 35 was "narrowly tailored" and burdened less speech "than [] necessary."[155] After applying intermediate scrutiny, the district court construed the meaning of the language from Proposition 35.[156] Lastly, and most importantly, the district court determined that the ballot measure was not narrowly tailored because the government did not explain "why the collection of Internet-identifying information from registrants who present a low or moderately low risk of re-offending . . . ." was needed to accomplish public safety goals.[157] The district court enjoined the law from being implemented after determining that the "challenged provisions have some nexus with the government's legitimate purpose of combating online sex offenses . . . but [t]he Government may not regulate expression in such a manner that a substantial portion of the burden on speech does not serve to advance its goals."[158]

On appeal, in 2014, the Ninth Circuit affirmed the lower court decision.[159] The court began with an analysis of the difference between incarceration, parole, probation, and registry requirements.[160] In doing so, the court contrasted the "necessary withdrawal or limitation of many privileges and rights" that come with serving a sentence as a sex offender to the later registry requirements falling under First Amendment protections.[161] Finding Proposition 35 to be content-neutral, the court applied intermediate scrutiny.[162] Despite finding a "legitimate government interest," the court held that the language of Proposition 35 surrounding Internet identifiers was not "narrowly tailored" and burdened more speech than necessary in at least three ways.[163]

First, in a departure from the lower court, the appellate court held that the Internet identifier requirement was ambiguous and thus unnecessarily chilled protected speech.[164] Second, the ballot measure further

---

[155] *Id.* at *11 (quoting Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 662 (1994)). The district court declined to use strict scrutiny. *Id.* at *10–11.

[156] *Id.* at *12–17.

[157] *Id.* at *17–34. Among other things, the district court expressed concern about the government's ability to release offender's anonymous Internet identifiers to the general public, the twenty-four hour window in which someone is required to report their Internet identifiers, why the government needs to monitor offenders' usage of websites dedicated to the discussion of "public, political, and social issues," and the felony punishment of being jailed for up to three years for failure to comply with the law. *See id.* at *24–32 (quoting White v. Baker, 696 F. Supp. 2d 1289, 1310 (N.D. Ga. 2010)).

[158] *Id.* at *33–34 (internal quotations omitted).

[159] *See* Doe v. Harris, 772 F.3d 563, 583 (9th Cir. 2014).

[160] *See id.* at 571–73. The appellate court noted that the plaintiffs were "not prisoners, parolees, or probationers. [The plaintiffs] were convicted of sex-related crimes more than two decades ago . . . [and] are no longer on the 'continuum' of state-imposed punishments." *Id.* at 571–72 (quoting Samson v. California, 547 U.S. 843, 848 (2006)).

[161] *Id.* at 571–73 (quoting Price v. Johnston, 334 U.S. 266, 285 (1948)).

[162] *Id.* at 574–76.

[163] *Id.* at 577–79.

[164] *Id.* at 578–79. "[N]otwithstanding the State's assurances that it will not prosecute 'honest mistakes,' 'we cannot assume that, in its subsequent enforcement, ambiguities will be

chilled protected speech because it "too freely allow[ed] law enforcement to disclose sex offenders' Internet identifying information to the public" and impermissibly "plac[ed] unbridled discretion in the hands of a government official or agency."[165] This was expressed as particularly problematic because "sex offenders' fear of disclosure in and of itself chills their speech."[166] Third, the requirement for sex offenders to "register within 24 hours of using a new Internet identifier" was found to violate intermediate scrutiny because it "undoubtedly chill[ed] First Amendment Activity" and applied "to all websites and all forms of communication, regardless of whether the website or form of communication is a likely or even a potential forum for engaging in illegal activity[.]"[167] California's unconstitutional Proposition 35 Internet identifier requirements were thus unenforceable.[168]

*Harris* was differentiated from *Shurtleff* on the basis that Utah's limited law prohibited the public disclosure of Internet identifiers and only permitted them to be used to "investigat[e] kidnapping and sex-related crimes[.]"[169] The cases also stand apart in that *Harris* focused more on the overly punitive nature,[170] overbreadth,[171] and possible public disclosure of California's Proposition 35.[172] Both appellate courts did, however, use an intermediate scrutiny analysis,[173] and dealt with laws that were at one point held unconstitutional at the district court level for violating the First Amendment.[174]

---

resolved in favor of adequate protection of First Amendment rights.'" *Id.* at 579 (quoting *NAACP v. Button*, 371 U.S. 415, 438 (1963)).

[165] *Id.* at 579–81 (quoting City of Lakewood v. Plain Dealer Publ'g Co., 486 U.S. 750, 757 (1988)).

[166] *Id.* at 581.

[167] *Id.* at 581–82.

[168] *See id.* at 583.

[169] *See id.* at 580 n.7.

[170] *See id.* at 581. "Although registered sex offenders do not have to register *before* they communicate online, they must register within 24 hours of using a new Internet identifier—a shorter time than is given by registration laws in other jurisdictions . . . . [T]his burden is particularly onerous for sex offenders who live in remote areas or who, like other citizens, have multiple Internet identifiers." *Id. Doe v. Shurtleff*, on the other hand, dismissed the plaintiff's argument that the law was overly punitive. *See* 628 F.3d 1217, 1226–27 (10th Cir. 2010).

[171] *See Harris*, 772 F.3d at 577–78 (finding the law was unconstitutionally overbroad). *But see Shurtleff*, 628 F.3d at 1225–27 (disagreeing with the plaintiff's assessment that the Utah law was unconstitutionally overbroad).

[172] *See Harris*, 772 F.3d at 573–74 (finding the law burdened a sex offender's ability to engage in anonymous speech due to possible public disclosure of internet identifier). *But see Shurtleff*, 628 F. 3d at 1224–25 (disagreeing with the plaintiff's assessment that the Utah allow would allow unrestricted disclosure of information to the general public).

[173] *Shurtleff*, 628 F.3d at 1223; *Harris*, 772 F.3d at 568–69.

[174] *See generally* Doe v. Harris, No. C12-5713 TEH, 2013 U.S. Dist. LEXIS 5428 (N.D. Cal. Jan. 11, 2013) (granting a preliminary injunction against enforcing the CASE act); *see also* Doe v. Shurtleff, No. 1:08-CV-64-TC, 2009 U.S. Dist. LEXIS 73955, at *2 (D. Utah Aug. 20, 2009). Also, the Ninth Circuit ruling is more recent and covers the largest jurisdiction of any federal appellate court in the United States. *See* Andrew Wallender and Madison Alder, *Ninth Circuit Conservatives Use Muscle to Signal Supreme Court*, BLOOMBERG L. (Dec. 8,

### *3.* Cornelio v. Connecticut *(2022 Second Circuit Case)*

The most recent case to apply Internet identifier requirements to a First Amendment speech test is *Cornelio v. Connecticut*.[175] The facts of the case are as follows. In 2005, James Cornelio was convicted of a variety of sex crimes involving children, violating New York state law.[176] Mr. Cornelio subsequently became a resident of Connecticut and was subject to the registry under Connecticut state law.[177] The Connecticut state registry required sex offenders to provide all "Internet identifiers" to a state law enforcement agency and "notify" that agency "in writing" if they "establish[] or change[] an electronic mail address, instant message address or other similar Internet communication identifier."[178] The law did not include any further definitions for what constituted an "Internet identifier" other than the list above.[179]

In early 2018, a warrant for Cornelio's arrest was signed by a judge and executed by law enforcement for Cornelio's alleged violation of the Connecticut Internet identifier law.[180] According to an affidavit, between the years of 2010 and 2015, Cornelio emailed his sex offender officer multiple times from an email account that he did not include on his original verification form.[181] Prosecutors charged Cornelio with a felony that carried with it up to five years in state prison.[182] In August 2018, Cornelio, representing himself, filed a lawsuit against the state of Connecticut for violating his constitutional rights under 42 U.S.C. § 1983.[183] In 2020, the District Court of Connecticut granted the government's motion to dismiss for lack of standing for failure to state a claim.[184] Two years later, the Second Circuit reversed.[185]

In finding that Cornelio had shown a plausible claim that the Internet identifier requirements violated the First Amendment, the Second Circuit Court used the following steps in their analysis of the claim: first, whether Connecticut's Internet identifier disclosure requirements implicated

---

2021), https://news.bloomberglaw.com/us-law-week/ninth-circuit-conservatives-use-muscle-to-signal-supreme-court [https://perma.cc/TEL6-BZ89]. "The California-based Ninth Circuit is the largest of the 12 regional appeals courts. It covers nine states, accounting for 20% percent [sic] of the American population . . . ." *Id.*

[175] *See* Cornelio v. Connecticut, 32 F.4th 160 (2d Cir. 2022). *Cornelio* served as the primary source of inspiration for this Note.

[176] *Id.* at 167.

[177] *Id.*

[178] *Id.* (quoting CONN. GEN. STAT. § 54-253(b) (2011)).

[179] *See id.*

[180] *Id.* at 167–68.

[181] *Id.*

[182] *See id.* at 169.

[183] *Id.* at 168.

[184] *Id.* Cornelio's initial lawsuit under 42 U.S.C. § 1983 included three claims: (1) that the internet identifier disclosure requirements violated the First Amendment, (2) the residence verification provision of the Connecticut law violated the Ex Post Facto Clause, and (3) that the officer who signed the affidavit leading to his arrest engaged in malicious prosecution in violation of the Fourth Amendment. *Id.* The first claim is the only claim at issue in this Note.

[185] *See id.*

"protected speech;" second, what heightened scrutiny was triggered; and third, whether the law ultimately passed or failed that heightened scrutiny.[186] The appellate court found that the Internet identifier disclosure requirement implicated protected speech because it burdened a registrant's "ability and willingness to speak on the Internet,"[187] applied "specifically to speakers engaged in online communication,"[188] and prevented "a registrant from speaking anonymously."[189] The court did not decide whether intermediate or strict scrutiny applied because it found Cornelio's claim plausible under intermediate scrutiny and thus found it unnecessary to parse the difference between the two standards.[190] Ultimately, the court held that "because the disclosure requirement plausibly fail[ed] intermediate scrutiny, Cornelio ha[d] stated a claim for violation of the First Amendment."[191] Did *Cornelio* and *Harris* create a wave of Internet identifier laws being struck down at the appellate level?

## IV. FIRST AMENDMENT ANALYSIS: THE UNCONSTITUTIONALITY OF CURRENT INTERNET IDENTIFIER LAWS

Whether a court applies the reasoning in *Shurtleff*, *Harris*, or, most recently, *Cornelio*, the result of application is predictable: any state Internet identifier law triggers a heightened scrutiny analysis under the First Amendment.[192] This section first analyzes the type of heightened scrutiny that should apply to Internet identifier laws. Then, following the presumption that the application of intermediate scrutiny is established precedent, this section analyzes how many Internet identifier laws today fail intermediate scrutiny and are thus unconstitutional.

### *A. Level of Scrutiny*

All three federal appellate court cases regarding Internet identifier laws applied intermediate scrutiny in conducting a First Amendment analysis.[193] From these cases, it is clear that any Internet identifier law will be subject to *at least* intermediate scrutiny. It is important, however, to understand how and why intermediate scrutiny was applied because it shows a potential pathway for strict scrutiny to be applied in future cases. In *Shurtleff*, the plaintiff argued that the Utah law should be subject to the highest level of scrutiny, strict scrutiny, because "it ha[d] the effect of taking away [Mr.] Doe's right to choose whether to speak anonymously or under

---

[186] *See id.* at 169.
[187] *Id.* at 169 (quoting *Doe v. Harris*, 772 F.3d 563, 572 (9th Cir. 2014)).
[188] *Id.*
[189] *Id.*
[190] *Id.* at 170.
[191] *Id.* at 172.
[192] *See* Doe v. Shurtleff, 628 F.3d 1217 (10th Cir. 2010); Doe v. Harris, 772 F.3d 563 (9th Cir. 2014); *Cornelio*, 32 F.4th at 160.
[193] *See Shurtleff*, 628 F.3d at 1217; *Harris*, 772 F.3d at 568; *Cornelio*, 32 F.4th at 160.

a pseudonym."[194] The court was not persuaded and instead used intermediate scrutiny because it found the law to be content-neutral for two reasons: (1) the Utah law did not say anything about the ideas or opinions that the plaintiff may or may not express,[195] and (2) the law was not aimed at "suppress[ing] the expression of unpopular views."[196]

Four years later, in *Harris*, the Ninth Circuit also applied intermediate scrutiny to the CASE Act (the legislation enacted from Proposition 35), California's Internet identifier law.[197] Unlike the previous decision in *Shurtleff*, *Harris* took greater lengths in weighing whether intermediate scrutiny was more appropriate than strict scrutiny.[198] The court stated that "[a] more difficult question is whether the CASE Act is subject to strict scrutiny because it makes speaker-based distinctions."[199] The court noted the Supreme Court's 2010 holding in *Citizens United v. Federal Election Commission* that "[s]peech restrictions based on the identity of the speaker are all too often simply a means to control content" and thus applied strict scrutiny to political speech even if the ban itself was "content neutral."[200] *Harris* was distinguished from *Citizens United* by explaining that while California's Internet identifier law singled out sex offenders as a category of speakers, it did not target political speech content, nor did it fully ban speech.[201] Lastly, in *Cornelio*, the Tenth Circuit declined to even address what level of scrutiny was appropriate to use because "the level of scrutiny would not alter [the court's] decision."[202]

In the pre-*Citizens United* era, when *Shurtleff* was decided, it was virtually certain that all Internet identifier laws would be decided under an intermediate scrutiny analysis. However, following *Citizens United* and the judicial commentary in *Harris*, or lack thereof in *Cornelio*, there are legitimate arguments to support the application of strict scrutiny to Internet identifier law issues. While it's true that Internet identifier laws do not outright ban speech or directly impact political speech, they could significantly chill speech by a certain group of people and incidentally impact political speech.[203] With the recent blurring of content-neutral versus content-targeted regulations, it is possible that Internet identifier laws could be subject to strict scrutiny soon. Perhaps the unwillingness of the court in

---

[194] *Shurtleff*, 628 F.3d at 1223 (quoting Brief for Appellant at 10) (internal quotations omitted).
[195] *Id.*
[196] *Id.* (quoting Am. Target Adver., Inc. v. Giani, 199 F.3d 1241, 1247 (10th Cir. 2000)).
[197] *Harris*, 772 F.3d at 574–77.
[198] *See id.*
[199] *Id.* at 575.
[200] *See id.* (quoting Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 340 (2010)).
[201] *Id.* at 575.
[202] Cornelio v. Connecticut, 32 F.4th 160, 170 (2d Cir. 2022). When a law "fail[s] even under the [less demanding] test . . . [the Court] need not parse the difference between the two standards in this case." McCutcheon v. FEC, 572 U.S. 185, 199 (2014) (plurality opinion).
[203] Say, for example, a sex offender being required to disclose his anonymous Internet identifier for a news or political discourse website. This could be of particular concern in a situation where he wishes to speak on a political issue directly related to sex offenders or registries.

*Cornelio* to entertain the application of strict scrutiny will serve as an invitation to another appellate court to be the first to do so.

In the unlikely, but no longer impossible, world in which courts begin to apply a strict scrutiny analysis to Internet identifier issues, they would most certainly all fail under such analyses. Because strict scrutiny requires not only that a law is narrowly tailored but *also* is the *least* restrictive means available and is of compelling (highest importance) interest to the government, even Utah's law upheld in *Shurtleff* would falter.[204] Of course, as of now, this is mere conjecture as no court has applied strict scrutiny to an Internet identifier law to date. As such, intermediate scrutiny remains the standard for analyzing Internet identifier laws.

### *B. Intermediate Scrutiny Analysis*

Despite *Shurtleff*, *Harris*, and *Cornelio* applying intermediate scrutiny to Internet identifier laws, how they precisely defined intermediate scrutiny differed.[205] Although some could argue the precise definition does not change the analysis, it is still prudent to acknowledge these minute differences. First, *Shurtleff* defined a law as meeting intermediate scrutiny if "the [law] (1) serves a *substantial government interest* and (2) is *narrowly drawn* to serve that interest *without unnecessarily interfering with First Amendment freedoms*."[206] *Harris* defined a law as meeting intermediate scrutiny if it is "*narrowly tailored* to serve a *significant governmental interest* and . . . . leave[s] open ample alternative channels for communication of the information."[207] Lastly, *Cornelio* defined a law as meeting intermediate scrutiny if it "(1) *advances important government interests* unrelated to the suppression of free speech and (2) does not burden substantially more speech than necessary to further those interests."[208] All three cases noted that intermediate scrutiny, unlike strict scrutiny, does not demand that the law follows the least restrictive means possible.[209]

For this analysis, and consistent with the courts' analyses in the above referenced cases, "substantial government interest," "significant government interest," and "important government interests" are interpreted to have the same weight.[210] In other words, "the government must identify evidence—or, at least, provide sound reasoning that draw[s] reasonable inferences based on substantial evidence" that intermediate scrutiny is met

---

[204] *See* Doe v. Shurtleff, 628 F.3d 1217, 1224 (10th Cir. 2010) (dismissing the plaintiff's contention that the law must be the least speech-restrictive means, but implicitly conceding that the plaintiff may be correct if that were the requirement).
[205] *See Shurtleff*, 628 F.3d at 1223; *Harris*, 772 F.3d at 576–77; *Cornelio*, 32 F.4th at 171.
[206] *Shurtleff*, 628 F.3d at 1223 (emphasis added) (internal quotations omitted).
[207] *Harris*, 772 F.3d at 576–77 (emphasis added) (internal quotations omitted).
[208] *Cornelio*, 32 F.4th at 171 (quoting Time Warner Cable Inc. v. FCC, 729 F.3d 137, 160 (2d Cir. 2013)) (emphasis added) (internal quotations omitted).
[209] *See id.*; *Harris*, 772 F.3d at 577; *Shurtleff*, 628 F.3d at 1224.
[210] *Cornelio*, 32 F.4th at 172.

whether "substantial," "significant," or "important" is used.[211] *Cornelio*'s additional requirement that the law *advances* an important government interest is addressed, specifically, below. The last requirement under intermediate scrutiny is that a law is "narrowly tailored."[212] Putting it all together, under the conditions of the three appellate courts: an Internet identifier law will satisfy intermediate scrutiny if it *serves or advances an important government interest* and is *narrowly tailored.* However, this need not be achieved by the least restrictive means possible.

### *1. Internet Identifier Laws Serve an Important Government Interest*

This Note readily concedes that Internet identifier laws can serve an important government interest. *Shurtleff* found this requirement met in a one-sentence assessment that the court had "no doubt that the State of Utah has a compelling interest in investigating kidnapping and sex-related crimes."[213] Subsequently, *Harris* found this requirement met because

> [u]nquestionably, the State's interest in preventing and responding to crime, particularly crimes as serious as sexual exploitation and human trafficking, is legitimate. We have observed that there is a 'strong link between child pornography and the Internet, and the need to protect the public, particularly children, from sex offenders.' California has a substantial interest in protecting vulnerable individuals, particularly children, from sex offenders, and the use of the Internet to facilitate that exploitation is well known to this Court.[214]

Although it is technically possible that an Internet identifier law could be written in a way that does not serve an important government interest, such as giving law enforcement complete, unfettered discretion to use Internet identifier data, there are no laws on the books that *explicitly* permit this.[215] Internet identifier laws are problematic in a variety of ways, but when an appellate court frames the first question of if the law *serves*, or *is* an important government interest, the answer is almost certainly a resounding "yes." Because of this, the first step of intermediate scrutiny analysis is sometimes a mere formality and nothing of substance to debate.

### *2. But Do They Advance That Interest?*

---

[211] *See id.* (quoting Turner Broad. Sys. v. FCC, 512 U.S. 622, 666 (1994)) (internal quotations omitted).
[212] *See Shurtleff*, 628 F.3d at 1224 (10th Cir. 2010).
[213] *See id.* at 1223.
[214] *See* Doe v. Harris, 772 F.3d 563, 577 (9th Cir. 2014) (internal citation omitted).
[215] However, there are some laws that do not *prohibit* law enforcement officers from having significant discretion in what they do with Internet identifiers. *See generally* MISS. CODE ANN. § 45-33-49 (2011); MISS. CODE ANN. § 45-33-29 (2011).

In a departure from *Shurtleff* and *Harris*, the appellate court in *Cornelio* went further than looking at whether the Internet identifier law served an important government interest and asked whether it *advanced* those interests.[216] The government argued that Connecticut's Internet identifier law *advanced* government interests by deterring registrants from "using the Internet (1) to recruit, groom, entice, or otherwise engage in communications with potential or actual sex abuse victims and (2) to engage in the distribution or exchange of prohibited sexual images."[217] The appellate court was not persuaded that the law did either because the government provided "no evidence that the disclosure requirement materially provides deterrence," and instead engaged in "speculative propositions."[218] While the government is allowed to engage in speculation to meet intermediate scrutiny, it still carries the burden of drawing reasonable inferences based on substantial evidence to back it up.[219]

Under the advancement standard, government actors have an increasingly difficult challenge. They must either show direct evidence that Internet identifier laws are effective or speculate, through substantial evidence, that the law will be effective.[220] The government not only failed to do this in *Cornelio*[221] but governments in other sex offender registry cases have failed to do this as well. For example, the Sixth Circuit found that "a regulatory regime [sex offender registry] that severely restricts where people can live, work, and 'loiter,' that categorizes them into tiers ostensibly corresponding to present dangerousness without any individualized assessment" was unconstitutional.[222] Why? because it was "*all supported by—at best—scant evidence that such restrictions serve the professed purpose of keeping Michigan communities safe* . . . ."[223] Next door, the Seventh Circuit found that the government had to provide "some evidence, beyond conclusory assertions, to justify [a sex offender] regulation."[224]

So what evidence, direct or supportive of speculation, will state officials offer to prove an advancement of an important government interest through Internet identifier laws? The data is growingly shaky, as even a statistic cited by Supreme Court Justice Anthony Kennedy that sex offenders have a "frightening and high risk of recidivism" is completely unfounded.[225] Further, a study of 474,640 formerly incarcerated sex offenders over a twenty-five-year period found that registry requirements

---

[216] Cornelio v. Connecticut, 32 F.4th 160, 172–73 (2d Cir. 2022).
[217] *Id.* (quoting Brief for Appellees at 33) (internal quotations omitted).
[218] *Id.* at 173.
[219] *Id.* at 172.
[220] *Id.* at 173–74.
[221] *Id.* (finding that the government had failed to meet the advancement requirement).
[222] John Does #1–5 v. Snyder, 834 F.3d 696, 705–06 (6th Cir. 2016) (emphasis added).
[223] *Id.* (emphasis added).
[224] Doe v. Prosecutor, 705 F.3d 694, 702 (7th Cir. 2013).
[225] *See* Radley Balko, *How a Dubious Statistic Convinced U.S. Courts to Approve of Indefinite Detention*, WASH. POST (Aug. 20, 2015), https://www.washingtonpost.com/news/the-watch/wp/2015/08/20/how-a-dubious-statistic-convinced-u-s-courts-to-approve-of-indefinite-detention/ [https://perma.cc/W4KN-F6C9].

had "no effect on recidivism."[226] This is not to say that government officials will find no evidence that Internet identifier requirements advance an important government interest, but that it likely will be more challenging, not less, to do so.

One thing is clear: when courts inquire whether the government can provide evidence that an advancement of a government interest occurs, the law will face a much greater hurdle. Whether a court chooses to analyze Internet identifier laws through an *advancement of* an important government interest rather than just *serves/is* an important government interest makes a significant difference.

### *3. Internet Identifier Laws Are Not Narrowly Tailored*

The ultimate fatal error in many Internet identifier laws is that they are not *narrowly tailored*, unnecessarily chilling protected speech. Even if one concedes that Internet identifier laws serve or advance an important government interest, the overly broad and sweeping language of these statutes across the country necessarily fails to meet intermediate scrutiny.[227] In *Harris*, there were at least three reasons the California Internet identifier law was found to unnecessarily chill protected speech: (1) the lack of clarity for what sex offenders must report, (2) the onerous nature of the twenty-four-hour reporting requirement, and (3) the insufficient safeguards preventing the public release of information sex offenders must report.[228] In *Cornelio*, the appellate court opined that the Connecticut law was potentially overbroad because "many platforms that allow communications between users do not reasonably present a vehicle by which a sex offender can communicate with minors or exchange prohibited sexual materials."[229] Additionally, the court argued that the Connecticut law was problematic because it applied to sex offenders who "[n]ever engaged in the sort of illicit online activity that the government seeks to deter."[230]

Compounding all the arguments above, state Internet identifier laws across the country should swiftly be struck down as unconstitutional for not being narrowly tailored. For example, the Internet identifier laws in Alabama, South Carolina, and Montana would be considered overly broad because they apply to a broader set of sex offenders than those that were convicted of Internet-related crimes.[231] Wisconsin's definition of Internet

---

[226] Kristen M. Zgoba and Meghan M. Mitchell, *The Effectiveness of Sex Offender Registration and Notification: A Meta-Analysis of 25 Years of Findings*, J. EXPERIMENTAL CRIMINOLOGY (2021), https://link.springer.com/article/10.1007/s11292-021-09480-z [https://perma.cc/WW5R-T5MD].

[227] *See generally* Doe v. Harris, 772 F.3d 563 (9th Cir. 2014) (holding that the Internet identifier law at issue failed immediate scrutiny); Cornelio v. Connecticut, 32 F.4th 160 (2d Cir. 2022).

[228] *Harris*, 772 F.3d at 578.

[229] *Cornelio*, 32 F.4th at 175.

[230] *Id.*

[231] *See* ALA. CODE § 15-20A-7 (2022); ALA. CODE § 16-20A-5 (2022); S.C. CODE ANN. §23-3-555 (2016); MONT. CODE ANN. § 46-23-504 (2021).

identifier that includes "*every* Internet user name the person uses" would chill more speech than necessary.[232] Mississippi's law, which does not restrict when law enforcement can search or investigate one's Internet identifiers, does not provide sufficient safeguards.[233] Virginia's requirement for someone to notify law enforcement within *thirty minutes* of changing an Internet identifier is *extraordinarily* onerous.[234] Regardless of the region, Internet identifier laws are not narrowly tailored and thus fail intermediate scrutiny.

From proactive, and sometimes overzealous, legislators to government attorneys defending current Internet identifier laws, some will be quick to point out that these laws need not be written in the *least* restrictive means possible.[235] Further, some will point to the Tenth Circuit's conclusion in *Shurtleff* that the Utah Internet identifier law did not unnecessarily chill protected speech.[236] These arguments fail for two reasons. First, Utah's law, previously struck down as unconstitutional, was amended to clarify when law enforcement officers may investigate a sex offender's Internet identifier.[237] Not all other state laws have this clarification, and thus the comparison is moot.[238] Second, and most importantly, the opinion in *Shurtleff*, being the first federal appellate decision on Internet identifier laws, did not ask and thus did not answer the problems brought up in *Harris* and *Cornelio*. While other courts, including the Supreme Court, are not bound by the *Harris* or *Cornelio* rulings, it would defy logic for them to ignore *more recent* case law that more closely reflects the status of Internet identifier laws today. Internet identifier laws will continue to be subject to at least intermediate scrutiny, requiring them to be narrowly tailored, which an overwhelming amount of them are not. These laws violate the Free Speech Clause of the First Amendment, and thus *Harris* and *Cornelio* should become national precedents.

## V. REMEDIES

Despite the myriad of challenges, both legal and practical, presented by Internet identifier rules for those on registries, there are remedies to fix them. However, a starting framework is needed. The remedies discussed below are solely focused on fixing First Amendment conflicts with Internet identifier rules while keeping other registry requirements intact. Thus, the following solutions do not necessitate addressing registry policies before the 2008 KIDS Act, which added the

---

[232] *See* WIS. STAT. 301.45(2)(a)6m (emphasis added).
[233] *See* MISS. CODE ANN. § 45-33-49 (2011); MISS. CODE ANN. § 45-33-29 (2011).
[234] *See* VA. CODE ANN. § 9.1-903(G) (2022).
[235] *See Cornelio*, 32 F.4th at 171; Doe v. Harris, 772 F.3d 563, 577 (9th Cir. 2014); Doe v. Shurtleff, 628 F.3d 1217, 1224 n.5 (10th Cir. 2010).
[236] *See Shurtleff*, 628 F.3d at 1225 (holding that the Internet identifier law "includes sufficient restrictions so as not to unnecessarily chill Mr. Doe's speech.").
[237] *Id.* at 1220–21.
[238] *See, e.g.*, MISS. CODE ANN. § 45-33-49 (2011); MISS. CODE ANN. § 45-33-29 (2011).

Internet identifier registration requirement to the Adam Walsh Act.[239] These solutions are tailored to both legislative bodies that have yet to add Internet identifier registry requirements and those looking to amend current laws to comport with First Amendment and public policy concerns. The three approaches below account for variations in value judgments and political climates. The first approach is broad, which tilts significantly towards promoting civil liberties, eliminating First Amendment issues around Internet identifiers completely. The second approach is narrow, tilting the other direction towards public policy goals of promoting public safety and being "tough" on sex offenders. The last approach is balanced, which attempts to harmonize public safety goals of Internet identifiers while maximizing First Amendment protections.

### *A. Broad Approach: Eliminating Internet Identifier Requirements*

The first approach is the most straightforward, albeit likely not the easiest to effectuate. The broad approach would be to eliminate all Internet identifier requirements for registries, which would remove the First Amendment issue altogether. Per *Cornelio* and other appellate case law, disclosure requirements trigger heightened scrutiny (intermediate or strict) under the First Amendment.[240] In other words, no disclosure requirements mean no risk of chilling online speech and thus no speech for the government to burden.

The removal process of Internet identifier requirements is straightforward: a complete repeal of applicable state and/or federal laws mandating as such. This could be done collaboratively through a repeal of federal and state law, a reformation of the Adam Walsh Act "substantial compliance" by Congress or the U.S. Attorney General, or states going alone and defying federal law. Collaboration would require Congress to repeal the KIDS Act, which includes the "requirement that sex offenders provide certain Internet related information to sex offender registries,"[241] and allow states to then follow suit. If Congress did not wish to repeal the KIDS Act, it could simply exempt the KIDS Act from the funding penalty attached to state non-compliance or, under the Attorney General's authority, find states "substantially compliant" with the Adam Walsh Act

---

[239] *Legislative History of Federal Sex Offender Registration and Notification*, *supra* note 10. This is not to minimize the robust legal arguments for and against non-Internet identifier registry requirements, which have sparked significant debate over the past two decades. *See generally* Susan Oakes, *Megan's Law: Analysis on Whether It Is Constitutional to Notify the Public of Sex Offenders via the Internet*, 17 J. MARSHALL J. COMPUTER & INFO. L. 1133 (1999); Corey R. Yung, *One of These Laws Is Not Like the Others: Why the Federal Sex Offender Registration and Notification Act Raises New Constitutional Questions*, 46 HARV. L. REV. 369 (2009); John F. Howard, *Balancing SORNA and the Sixth Amendment: The Case for a "Restricted Circumstance-Specific Approach,"* 103 MARQ. L. REV. 1565 (2020).

[240] *See Shurtleff*, 628 F.3d at 1223 (applying intermediate scrutiny); *Harris*, 772 F.3d at 568 (applying intermediate scrutiny); *Cornelio*, 32 F.4th at 171 (applying intermediate scrutiny on appeal because the level of scrutiny was an uncontested issue).

[241] *See* Keeping the Internet Devoid of Sexual Predators Act of 2008, Pub. L. No. 110-400, 122 Stat. 4224 (codified as amended in scattered sections of 42 U.S.C.).

without the Internet identifier requirement being met. If all else fails, states could defy the federal government by repealing Internet identifier requirements, fall out of compliance with the Adam Walsh Act, and lose ten percent of the federal funding grant.

The risks and difficulties with such a broad approach are readily apparent. Despite its simplicity, the odds of Congress repealing a law called "Keeping the Internet Devoid of Sexual Predators[]" because they feel sympathetic to constitutional arguments made in defense of sex offenders are likely slim to none.[242] Congress exempting states from losing federal funding for lack of compliance with the Internet identifier requirements, over a full repeal of the laws, might offer slight political cover but probably would not insulate them from the attack ads.[243] A decision by the Attorney General allowing states to be "substantially compliant" with the Adam Walsh Act without implementing Internet identifier requirements would likely be met with lawsuits.[244] Alternatively, in the case of states falling out of substantial compliance with the Adam Walsh Act by refusing to implement Internet identifier requirements, they would both lose funding and be subjected to the aforementioned attacks that federal politicians could face. Absent a Supreme Court mandate that struck down Internet identifier requirements entirely, this straightforward remedy faces enormous challenges.

While some may scoff at the odds of legislative success for a broad approach, there is one potentially salient argument. The elimination of Internet identifier requirements for *registries* does not necessitate the removal of them as conditions under *probation or parole*. Both government actors and plaintiffs have agreed that "speech by sex offenders who have completed their terms of probation or parole enjoys the full protection of the First Amendment."[245] However, First Amendment protections *during probation or parole,* the time in which someone is still serving their sentence*,* are more heavily disputed. The Ninth Circuit described parole as

---

[242] *See generally* Seung Min Kim, Aaron C. Davis, and Paul Kane, *Ketanji Brown Jackson Passionately Defends Her Sentencing of Sex Offenders*, WASH. POST (Mar. 22, 2022), https://www.washingtonpost.com/politics/2022/03/22/ketanji-brown-jackson-sex-offenders/ [https://perma.cc/Y8DT-EAC7] (highlighting the barrage of attacks by federal politicians for now-Justice Ketanji Brown being too "lenient" on sex offenders).

[243] *See generally* Glenn Kessler, *Attack Ad Falsely Claims Lawmaker Helped Sexual Predators 'Hide in the Shadows'*, WASH. POST (Sept. 22, 2020), https://www.washingtonpost.com/politics/2020/09/22/attack-ad-falsely-claims-lawmaker-helped-sexual-predators-hide-shadows/ [https://perma.cc/9Q62-6LJC] (describing a televised attack ad against someone running for Congress who worked for an organization that sought to challenge the constitutionality of sex offender registries).

[244] Selective enforcement of laws and policies can be the source of lawsuits against government officials. *See generally* Amanda Frost, *In Major Immigration Case, Both Sides Look to Academia to Untangle Three Knotty Questions*, SCOTUSBLOG (Nov. 23, 2022), https://www.scotusblog.com/2022/11/in-major-immigration-case-both-sides-look-to-academia-to-untangle-three-knotty-questions/ [https://perma.cc/P9JC-EW8Q] (mentioning the Biden administration being sued for setting priorities in the enforcement of immigration law).

[245] *Harris*, 772 F.3d at 570.

"one step removed from imprisonment," and that while parolees "'should enjoy greater freedom in many respects than a prisoner, . . . the Government may . . . impose restrictions on the rights of the parolee that are reasonably and necessarily related to the [Government's] interests.'"[246] Similarly with probation, "the government may still 'impose reasonable conditions that deprive the offender of some freedoms enjoyed by law-abiding citizens.'"[247] Shifting the restrictive nature of Internet identifier requirements from registries to parole and probation is constitutionally sound.

The argument to shift Internet identifier requirements out of registries to conditions of probation or parole also has strong public policy support.[248] In a comprehensive study of the recidivism rate of formerly incarcerated sex offenders, seventy-five percent of sex offenders that reoffended did so within two to five years of release.[249] Further, "sexual recidivism rates among sex offenders generally decrease as age increase[s]. Offenders aged 20 to 29 ma[k]e up the largest overall proportion of recidivists."[250] Conceding for the sake of argument that Internet identifier requirements can prevent sex crimes, having them attached to conditions of probation or parole,[251] a time where an offender is most likely to re-offend, is a more compelling policy.

A broad approach seeks to maximize civil liberty protections and reduce or fully eliminate First Amendment issues. It also does not require a sacrifice to public safety, even if one believes that Internet identifier requirements work to prevent future sex crimes. Despite being plagued by likely legislative malaise, the broad approach may serve as a compelling roadmap for result-oriented attorneys fighting it out in the judiciary.

### *B. Narrow Approach: Precision in Statutory Construction*

---

[246] *Id.* at 571 (quoting Birzon v. King, 469 F.2d 1241, 1243 (2d Cir. 1972)). The appellate court subsequently offered the example of when it "upheld Internet monitoring as a condition of release for parolees who were convicted of downloading child pornography." *Id.* (citing United States v. Quinzon, 643 F.3d 1266, 1272–73 (9th Cir. 2011)); United States v. Goddard, 537 F.3d 1087, 1090 (9th Cir. 2008)).

[247] *Id.* (quoting United States v. Knights, 534 U.S. 112, 119 (2001)). Criminal and constitutional rights appellate attorneys would likely still argue that Internet identifier requirements for probation or parole are also unconstitutional. Because of the distinctions outlined in *Doe v. Harris*, they are less likely to be successful. *See* Anthony Streveler & Joseph R. Tatar II, *Sex Offender Recidivism After Release From Prison,* WIS. DEP'T OF CORR. (Sept. 2015), https://doc.wi.gov/DataResearch/RecidivismReincarceration/SexualOffenderRecidivismReport.pdf [https://perma.cc/WF46-BAEF].

[248] *See generally* Anthony Streveler & Joseph R. Tatar II, *supra* note 247.

[249] *Id.* at 5.

[250] *Id.*

[251] Conditions of probation and parole, outside of registries, can already last a significant amount of time. *See* MINN. SENT'G GUIDELINES COMM'N, CRIMINAL SEXUAL CONDUCT OFFENSES 19 (Nov. 2014), https://mn.gov/sentencing-guidelines/assets/Crim%20Sex%20Report_tcm30-31370.pdf (finding that, on average, sex offenders in Minnesota served a probation period for thirteen years).

The second approach, unlike the first, is more complex but is most certainly easier to implement as a political matter. The narrow approach would keep Internet identifier requirements for registries in place while working with extreme precision to tweak them in response to recent caselaw. By acting carefully, Internet identifier laws could have a better chance of surviving constitutional challenges without revolutionary change. To better understand what this would look like, a thorough reading of two different Internet identifier statutes is needed.

Virginia's "Registration and registration procedures" statute ("Virginia Identifier Law"), which includes the Internet identifier requirements, states that

> every person required to register . . . shall submit . . . electronic mail address information, any instant message, chat or other Internet communication name or identity information that the person uses or intends to use . . . [and the] local law-enforcement agency shall obtain from the person who presents himself for registration [those same pieces of information]. . . .[252]

Virginia's Identifier Law continues, describing that

> [a]ny person required to register shall reregister either in person or electronically with the local law-enforcement agency where his residence is located *within 30 minutes* following any change of the electronic mail address information, any instant message, chat or other Internet communication name or identity information that the person uses or intends to use, whether within or without the Commonwealth.[253]

The constitutional problems with this law are both readily apparent and significant. First, while "electronic mail address information," "instant message," or "chat" may not need further elaboration, the statute does not define nor limit the scope of "other Internet communication name or identity information."[254] Does this include usernames and passwords? What about information for commercial transactions or pure political speech? Second, the law does not specify what local law enforcement or other government officials can do with the identifier information they receive.[255] Under what circumstances, if any, can they disseminate it to the public? What about for internal use? Can they peruse through identifier information at their own leisure or only to investigate a certain type of crime? Third, how can requiring an individual to disclose their identifier

[252] VA. CODE ANN. § 9.1-903 (B) (2022). Note that the "narrow approach" does not wade into "every person required to register," or the scope of who the statute is applied to. That is discussed in further detail in the subsequent section.
[253] *Id.* § 9.1-903(G) (emphasis added).
[254] *See id.* § 9.1-903(B).
[255] *See id.*

information *within thirty minutes* of an update be seen as anything other than extremely onerous and deeply burdening protected speech?[256] To make matters worse, if an individual was previously convicted of a violent sex offense, failure to meet *any* registration requirements, including the thirty-minute update, could subject them to felony charges.[257]

Even in the Tenth Circuit, which upheld the Utah Internet identifier statute, the Virginia Identifier Law, as written, would likely be struck down as unconstitutional.[258] Fear not, however, because this problematic law can be contoured into something workable with ease. The first step in precision on statutory construction of the Virginia Identifier Law would be to either properly define an "Internet identifier" or "communication name." If that task seems too burdensome, the law could *at least* create a list of what is *not* an "Internet identifier" or "communication name."[259] The amended law must also detail what law enforcement can do with the provided Internet identifier information and under what circumstances, if any, it can be released to the public.[260]

As an example of specific changes, the new law could explicitly say that "all electronic mail address information, instant message, chat or other Internet communication name or identity information used or intended to be used by the registrant shall not be released to the public unless '*x' exception* applies" and that "local law-enforcement, state police, and all other government actors may only exchange information about registrant electronic mail address information, instant message, chat or other Internet communication name or identity information used or intended to be used by the registrant to investigate '*y' crimes*." Another change would be to increase the thirty-minute notification window to *at least* forty-eight hours.[261] In the Virginia statute that governs the charges for violation, a change could also be made to explicitly protect offenders that make a good faith effort in reporting their new or changed Internet identifiers, potentially eliminating some of the chilling effects.[262]

Florida's Internet identifier law ("Florida Identifier Law") is more robust than Virginia's.[263] It takes the definition of "Internet identifier" from the Florida Sexual Predators Act, which defines it as "any designation, moniker, screen name, username, or other name used for self-identification to send or receive social Internet communication. Internet identifier does

---

[256] *See id.* § 9.1-903(G); *see also* Doe v. Harris, 772 F.3d 563, 581 (9th Cir. 2014) (finding a 24-hour notification period too onerous).

[257] *See generally* VA. CODE ANN. § 18.2-472.1.

[258] *See generally* Doe v. Shurtleff, 628 F.3d 1217 (10th Cir. 2010).

[259] *See* FLA. STAT. § 775.21 (2022) (including a list of what an "Internet identifier" is not).

[260] *See Shurtleff*, 628 F.3d at 1225 (finding Internet identifiers may only be used by law enforcement to investigate sex or kidnapping crimes).

[261] A forty-eight-hour requirement would be in line with the reasoning on the time reporting requirements described in *Harris*. *See Harris*, 772 F.3d at 582 (arguing that the twenty-four-hour reporting requirement is too onerous).

[262] *See* VA. CODE ANN. § 18.2-472.1. The statute does already include a "knowing" intent requirement for failure to comply with registry, which is a good first step. *See id.*

[263] *See* FLA. STAT. § 943.0435 (2021).

not include a date of birth, social security number, personal identification number (PIN), or password."[264] Florida's Identifier Law requires "all electronic mail addresses and Internet identifiers, and each Internet identifier's corresponding website homepage or application software name" to be reported to law enforcement "within 48 hours after using such electronic mail addresses and Internet identifiers."[265] A violation of this law can result in a third-degree felony, which permits imprisonment up to five years,[266] and can occur by "knowingly provid[ing] false registration information by act or omission" or otherwise failing, "by act or omission, to comply with the requirements of [the registry]."[267]

Compared to Virginia's Identifier Law, Florida is plagued with far fewer issues. Florida's definition of "Internet identifiers" includes the component of them being used to "send or receive social Internet communication"[268] and lists specific exclusions.[269] By doing this, Florida's law is less ambiguous and more narrowly tailored at the outset. To make it even more constitutionally sound, Florida lawmakers should expand the list of exclusions to Internet identifiers, such as websites that are solely dedicated to news and political topics. Florida does a better job at offering a longer reporting window but should also create a good faith exception from prosecution for individuals that did not intentionally withhold Internet identifiers from law enforcement. Additionally, Florida's Identifier Law should better define if and when law enforcement can disclose identifying information to the public and the procedures for the dissemination of information amongst themselves.

The Florida Identifier Law and the Virginia Identifier Law are just small samplings of the many Internet identifier laws states have implemented across the country. While the Florida Identifier Law shows an example of greater legislative fine-tuning than the Virginia Identifier Law, even the smallest changes to these laws are unlikely to fully eliminate First Amendment problems. Additionally, even tightening Internet identifier statutes fails to fully address another key consideration at the crux of this Note: fully protecting the rights of sex offenders, particularly those that pose no online predatory threat. While precision in statutory construction offsets the problems addressed in the broad approach, it leaves much to be desired in safeguarding core civil liberties.

### *C. Balanced Approach: Narrowly Tailoring Internet Identifier Laws*

To harmonize the important policy goals of maintaining Internet identifier laws with protecting the constitutional rights of sex offenders, the best solution is wedged between the narrow and broad approaches. This

---

[264] *See* FLA. STAT. § 775.21(2)(j) (2022).
[265] *See id.* § 775.21(6)5.a.
[266] *See id.* § 775.21(10); *see also* FLA. STAT. § 775.082(2) (2022).
[267] *See* FLA. STAT. § 775.21(10).
[268] *See* FLA. STAT. § 775.21(2)(j).
[269] *See* FLA. STAT. § 775.21(2)(j).

balanced approach focuses on and fixes the defect mentioned in *Harris* and amplified in *Cornelio*: the necessity for the government to narrowly tailor Internet identifier laws to meet intermediate scrutiny.[270] By narrowly tailoring Internet identifier laws on the front end, *who* the law applies to, and on the back end, *how* that law applies to them, a better way forward is possible. There are two states, California and New York, that illustrate how this can be done.

After California's Internet identifier law, Proposition 35, was halted following the outcome of *Harris*, state lawmakers enacted a law that would be constitutionally sound.[271] Just over five years after the passage of Proposition 35, the California legislature amended the laws significantly. First, the legislature narrowed the Internet identifier law on the front end by having it apply to only three groups of sex offenders: (1) those that used the Internet to collect any private information to identify a victim of a crime to further the commission of the sex crime they committed; (2) those that committed a certain felony (human trafficking) *and* used the Internet to traffic a victim of that crime; or (3) those that were convicted of certain felonies (related to obscene material) "*and* used the Internet to prepare, publish, distribute, send, exchange, or download the obscene matter or matter depicting a minor engaging in sexual conduct."[272] Second, the legislature amended the definition of an "Internet identifier" to an "electronic mail address or user name used for instant messaging or social networking *that is actually used for direct communication between users on the Internet in a manner that makes the communication not accessible to the general public*."[273] Third, any sex offender that is required to disclose Internet identifiers has *thirty days to report* a new or changed identifier, and if they fail to conform with the law, the punishment constitutes a *misdemeanor* (less than a year of jail time) and not a felony.[274] Fourth, law enforcement agencies are not permitted to disclose one's Internet identifiers to the public unless required by court order and cannot be used among law enforcement agents except for investigating human trafficking, a sex-related crime, or kidnapping.[275]

The amendments the California legislature made to Proposition 35 best reflect a balanced approach that narrowly tailored an Internet identifier law to meet intermediate scrutiny. First, by ensuring the amended law only applies to sex offenders that used the Internet as a component of their previous crime, burdening speech rights of only a subset of all registered sex

---

[270] *See* Doe v. Harris, 772 F.3d 563, 569, 576–77 (9th Cir. 2014); Cornelio v. Connecticut, 32 F.4th 160, 172 (2d Cir. 2022).

[271] *See generally* Kathleen A. Kenealy, *Collection of Internet Identifiers from Registered Sex Offenders*, CAL. DEP'T OF JUST. (Jan. 5, 2017), https://oag.ca.gov/sites/all/files/agweb/pdfs/info_bulletins/17-02-cjis.pdf [https://perma.cc/TSE8-SUPG].

[272] *Id.* (emphasis added).

[273] *See id.* (emphasis added). It also excludes "Internet passwords, PIN number(s), date of birth, or social security number." *Id.*

[274] *See id.* (emphasis added).

[275] See *id.* (emphasis added).

offenders, it narrows in its focus. This overlaps with a public safety standpoint as law enforcement officers can focus on individuals that have shown they may have a *modus operandi* for using different Internet identities to commit crimes. The amended law is further narrowly tailored by confining the definition of Internet identifier to only include "direct communication between users on the Internet in a manner that makes the communication not accessible to the general public."[276] This necessarily omits many places where an individual may contribute anonymously to a political or news discussion, such as a New York Times comments section. By giving an individual thirty days to report, and keeping the penalty to a misdemeanor, speech is chilled to a lesser extent because an individual does not have to stress immediate reporting of an identifier or face serious criminal penalty for a violation of the law.

Further, by explicitly prohibiting public disclosure of Internet identifiers outside of a court order and limiting law enforcement's use of them except in investigating sexual, human trafficking, or kidnapping offenses, it prevents law enforcement from having unfettered access to individuals' Internet identifiers. Ultimately, California lawmakers' amendments to Proposition 35 adequately balance public safety concerns while narrowly tailoring the law to comport with First Amendment intermediate scrutiny. Rather than throwing Internet identifier requirements out completely or only marginally changing them to hardly make any difference at all, California's amendments to previously unconstitutional Internet identifier laws should be the first place lawmakers across the country look for meaningful change.

A balanced solution does not necessitate waiting for state legislative bodies to act, as identifier laws can be narrowly tailored through judicial proceedings. In 2008, the New York Governor signed the Electronic Security Targeting of Online Predators Act ("e-STOP") into law, which required, among other things, "convicted sex offenders to register their Internet screen names with the Sex Offender Registry" and "allow[ed] social networking Web sites [sic] to obtain those screen names in order to prohibit those account holders from accessing Web sites [sic] on which they could contact children."[277] The law applied to *all* registered sex offenders, which included roughly 25,000 individuals in New York at the time it was passed.[278] An important note is that while the lawsuit and subsequent remedy mentioned below addressed e-STOP's *complete prohibition of social media use for those on probation and parole*, not Internet identifier

[276] *See id.* (emphasis added).

[277] *New York Governor Paterson Signs e-STOP Act*, GOV'T TECH. (July 27, 2010), https://www.govtech.com/security/new-york-governor-paterson-signs-e-stop-act.html [https://perma.cc/2P2U-78MP] [hereinafter GOV'T TECH. Article]. The law was passed unanimously. Press Release, Off. of the N.Y State Att'y Gen., *The New York State Attorney General's e-STOP Law Removes Additional Sexual Predators From Social Networking Web Sites; Calls On 14 Youth-oriented Sites to Screen Users* (Feb. 2, 2010), https://ag.ny.gov/press-release/2010/new-york-state-attorney-generals-e-stop-law-removes-additional-sexual-predators [https://perma.cc/G2PB-HPRX] [hereinafter Press Release].

[278] *See* GOV'T TECH. Article, *supra* note 277.

requirements post-conviction, it is an important framework because it focuses on narrowly tailoring an Internet registry law to meet intermediate scrutiny.[279]

In 2010, the New York Attorney General boasted that e-STOP had "resulted in the removal of accounts associated with at least 4,336 registered sex offenders from major networking Web sites operating in the United States."[280] Furthermore, he stated that "thousands of sexual predators who had opened thousands of accounts h[ad] been purged from social networking sites," and "8,606 [] offenders ha[d] reported either a screen name or email address [as required by law]."[281] As expected, a group of sex offenders in New York filed a lawsuit, seeking to prevent e-STOP from being enforced on the basis that it violated their First Amendment rights.[282]

The New York Eastern District Court enjoined parts of e-STOP from being enforced on the grounds that it violated the plaintiffs' First Amendment rights.[283] In agreeing with the plaintiffs' argument, Judge Raymond Dearie stated that e-STOP was "not narrowly tailored because it applie[d] to Registrants who d[id] not present a significant risk of recidivating via social media" and did not provide a "mechanism to conduct an individualized assessment as to whether a Registrant poses a risk of misusing social media before imposing the [b]an."[284] Judge Dearie also opined that,

> [i]t may well be that some of the Registrants subject to e-STOP . . . pose a legitimate risk of recidivating using social media. But Defendants' attempt to address this critical concern through a blanket prohibition without first finding that those encumbered are likely to reoffend via social media is incompatible with the First Amendment.[285]

Judge Dearie permitted e-STOP only to be applied to individuals that used the Internet to facilitate the sex offense they were convicted of.[286]

On January 24, 2022, a settlement agreement was reached, expanding upon the injunction ordered by Judge Dearie.[287] The settlement officially ended New York's blanket Internet and social media bans, and it implemented a framework so that "social media and Internet restrictions will be limited to circumstances where there are legitimate and particularized concerns about a person's likelihood of sexually reoffending

---

[279] *See* Jones v. Stanford, 489 F. Supp. 3d 140, 143 (E.D.N.Y. 2020). The lawsuit was focused on the complete prohibition of certain sex offenders from accessing social media websites altogether, but it implicated Internet identifier requirements as well. *See id.*

[280] *See* Press Release, *supra* note 277.

[281] *Id.*

[282] *See* Jones, 489 F. Supp.3d at 143 (E.D.N.Y. 2020).

[283] *See id.* at 143.

[284] *Id.* at 146–47.

[285] *Id.* at 150–51.

[286] *Id.* at 154.

[287] *See New York Ends Blanket Internet and Social Media Bans for People Convicted of Sex Offenses*, NYCLU (Jan. 24, 2022), https://www.nyclu.org/en/press-releases/new-york-ends-blanket-internet-and-social-media-bans-people-convicted-sex-offenses [https://perma.cc/892R-ZG8Q].

by using the Internet or social media or where restrictions are deemed necessary to ensure compliance with a specific goal of rehabilitation."[288] More specifically, the settlement permitted state actors to restrict a registrant's social media access only when

> there are articulable registrant-specific circumstances that: 1) raise a legitimate and particularized concern about the Registrant's risk of reoffending by using social media, and/or 2) indicate the restrictions on a Registrant's access to social media will be the most suitable, least restrictive means of ensuring compliance with a specific goal of rehabilitation.[289]

The settlement agreement reached essentially forced administrative agencies in New York to enforce e-STOP in a narrowly tailored way. While this outcome, again, applied to conditions of complete Internet restrictions for sex offenders on probation or parole, it is demonstrative of how arguments can be successfully made before the judiciary to force changes to state Internet identifier laws. Sex offenders can, and should, continue to challenge state Internet identifier laws and seek injunctions. Courts need not even come to precedential decisions as settlement agreements can push government actors to interpret and enforce parts of registry laws before they cause further harm to the rights of sex offenders.

Narrowly tailoring Internet identifier laws through legislative or judicial action is the best remedy to balance public safety goals of keeping the Internet safe from sexual predators while also protecting the First Amendment rights of all. While not completely immune from *every* potential constitutional or public safety issue, it offers a palatable solution for the widest variety of stakeholders. Ideally, it offers an opportunity for the most committed activists for children's safety and those who defend the constitutional rights of sex offenders to work together and create the best Internet identifier laws possible.

## VI. CONCLUSION

Sex offender registries, like the people they try to regulate, are complicated. Understanding the evolution of these online registries serves as an important foundation to make sense of *how* we got into the situation we are in today. Internet identifiers, only a tiny piece of the registry requirement web, are easier to untangle by following the trajectory of registry laws over the past thirty years. Looking at the collision course of such laws and the Free Speech Clause of the First Amendment through the application and analysis of important federal case law shows *why* important constitutional questions demand resolution. Being solution-oriented to a

[288] *Id.*
[289] Settlement Agreement at 3, Jones *et al.* v. Stanford, No. 1:20-cv-01332-RJD-JRC (E.D.N.Y. Jan. 24, 2022).

variety of remedies to fix these imperfect concoctions from, and through, America's laboratories of democracy, details *where* we go from here.

At the outset of this Note, *hows, whys,* and *wheres* were asked about Internet identifiers. Hopefully, the past few sections have offered a satisfactory answer to all these inquiries. One question not asked, however, is arguably the most important. Putting aside the complex landscape of evolving sex offender registries, cumbersome legal opinions, nuanced political debates, and statutory investigation places one in a moment of ultimate clarity: *why should anyone care*? Sex offenders, by their definition, have committed harms to society that have taken the innocence of children, destroyed families, and traumatized scores of people. They can prey on the most vulnerable, taking advantage in oftentimes unspeakable acts. Even with those that end up on registries for "less egregious" sex crimes, such as exposing one's genitals during public urination,[290] there is a sense of detest for their deviation from acceptable societal conduct.

With the needs of so many in the United States going unmet, why should protecting sex offenders be of priority, let alone consideration? If you asked Mr. Cornelio, he would tell you that "[registry] laws have reached the point where protecting the vulnerable has become secondary to that of further stigmatizing, harassing and punishing society's newest and most reviled outcasts. And who would deny that these results were not entirely unpredictable."[291] But there is a much simpler answer to this question: The American justice system is only as good as it treats those found most contemptible. The moment constitutional liberties and core freedoms are conditioned on whether someone carries the "scarlet letter" of being a sex offender, is the moment the entire foundation of what is known as "justice" begins to quake. *Why care*? Without defenders of those deemed most reprehensible, humanity itself risks perversion.

[290] *See The Ridiculous Laws that put People on the Sex Offender List*, SLATE (Aug. 12, 2014), https://slate.com/news-and-politics/2014/08/mapped-sex-offender-registry-laws-on-statutory-rape-public-urination-and-prostitution.html [https://perma.cc/UH2N-GYW6].

[291] Brief for Appellant at 30, Cornelio v. Connecticut, 32 F.4th 160 (2d Cir. 2022) (No. 20-4106).