EDITOR'S NOTE

Welcome to the second issue of Volume 69 of the Federal Communications Law Journal (FCLJ), the official journal of the Federal Communications Bar Association (FCBA). As the incoming Editor-in-Chief of the FCLJ, I am humbled to serve the oldest communications law journal in the country. I hope that the FCLJ will continue to spur vibrant conversations, substantively add to the scholarship, and act as a resource for practitioners in the communications law field.

This issue contains a collection of pieces on timely and important topics in the field, including the Internet of Things, universal service, cyberbullying, freedom of speech, and online identity abuse issues. Earlier in the spring at The George Washington University Law School, the FCLJ successfully held its first symposium on consumer privacy and the right to be forgotten. As this issue intends to continue the discussion on this topic, the FCLJ is honored to feature an article penned by Jules Polonetsky, the Chief Executive Officer of the Future of Privacy Forum. Mr. Polonetsky's article proposes specific ways in which the Internet of Things can promote accessibility, equality, and inclusion for those who may experience extraneous hurdles and exclusion from the fast-changing world we live in.

In addition to this piece, the FCLJ proudly presents three student Notes. In the first Note, Brian O'Shea explores the problem of cyberbullying, the current legislative shortcomings in tackling this issue, and the insufficiency of a reliance on the right to be forgotten. Mr. O'Shea proposes that the Notice-and-Takedown procedures of the Digital Millennium Copyright Act can potentially restrict content of cyberbullying speech. In the second Note, Melissa J. Morgans analyzes the tension between constitutionally protected free speech and censorable online terrorist speech. She proposes that the "Stop Terrorist Organizations from Promoting Internet Transmissions Act" could regulate such terrorist speech. Lastly, in the third Note, Laura K. Hamilton discusses the need for comprehensive federal legislation to protect online identity that can easily be abused by others. Ms. Hamilton proposes that a federal tort and a federal crime for malicious interference with online identity should be established.

This issue also serves as a transition from the previous FCLJ board to the new one. The incoming board is thankful for the supervision of the FCBA, the hard work of the outgoing board, all of whom have set solid grounds for the incoming board to work with this year. I am confident that the FCLJ is comprised of dedicated, diligent, and detail-oriented individuals who will bring unique perspectives to the new term. As a team, the FCLJ is excited and determined to provide interesting and thought-provoking material to our readers.

Please direct submissions for publication consideration to fcljarticles@law.gwu.edu, and all other questions or comments to fclj@law.gwu.edu. This issue and our archive are available at www.fclj.org.

Jane Lee
Editor-in-Chief

FEDERAL COMMUNICATIONS LAW JOURNAL

VOLUME 69 ISSUE 2

AUGUST 2017

Published by the GEORGE WASHINGTON UNIVERSITY LAW SCHOOL
and the FEDERAL COMMUNICATIONS BAR ASSOCIATION

Federal Communications Law Journal

The *Federal Communications Law Journal* is published jointly by the Federal Communications Bar Association and the George Washington University Law School. The *Journal* publishes three issues per year and features articles, student notes, essays, and book reviews on issues in telecommunications, the First Amendment, broadcasting, telephony, computers, Internet, intellectual property, mass media, privacy, communications and information policymaking, and other related fields.

As the official journal of the Federal Communications Bar Association, the *Journal* is distributed to over 2,500 subscribers, including Association members as well as legal practitioners, industry experts, government officials and academics. The *Journal* is also distributed by Westlaw, Lexis, William S. Hein, and Bloomberg Law and is available on the Internet at http://www.fclj.org.

The *Journal* is managed by a student Editorial Board, in cooperation with the Editorial Advisory Board of the FCBA and two Faculty Advisors.

Federal Communications Bar Association

The Federal Communications Bar Association (FCBA) is a volunteer organization of attorneys, engineers, consultants, economists, government officials and law students involved in the study, development, interpretation and practice of communications and information technology law and policy. From broadband deployment to broadcast content, from emerging wireless technologies to emergency communications, from spectrum allocations to satellite broadcasting, the FCBA has something to offer nearly everyone involved in the communications industry. That is why the FCBA, more than two thousand members strong, has been the leading organization for communications lawyers and other professionals since 1936.

Through its many professional, social, and educational activities, the FCBA offers its members unique opportunities to interact with their peers and decision-makers in the communications and information technology field, and to keep abreast of significant developments relating to legal, engineering, and policy issues. Through its work with other specialized associations, the FCBA also affords its members opportunities to associate with a broad and diverse cross-section of other professionals in related fields. Although the majority of FCBA members practice in the metropolitan Washington, D.C., area, the FCBA has ten active regional chapters: Atlanta, Carolina, Florida, Midwest, New England, New York, Northern California, Pacific Northwest, Rocky Mountain, and Texas. The FCBA has members from across the United States, its territories, and several other countries.

The George Washington University Law School

Established in 1865, the George Washington University Law School is the oldest law school in Washington, DC. The school is accredited by the American Bar Association and is a charter member of the Association of American Law Schools. The Law School is located on the GW campus in the downtown neighborhood familiarly known as Foggy Bottom.

GW Law has one of the largest curricula of any law school in the nation with more than 250 elective courses covering every aspect of legal study. GW Law's home institution, the George Washington University, is a private, nonsectarian institution founded in 1821 by charter of Congress.

The *Federal Communications Law Journal* is published by the George Washington University Law School and the Federal Communications Bar Association three times per year. Offices are located at 2028 G Street NW, Suite LL-020, Washington, DC 20052. The *Journal* can be reached at fclj@law.gwu.edu, and any submissions for publication consideration may be directed to fcljarticles@law.gwu.edu. Address all correspondence with the FCBA to the Federal Communications Bar Association, 1020 19th Street NW, Suite 325, Washington, DC 20036-6101.

Subscriptions: Subscriptions are $30 per year (domestic), $40 per year (Canada and Mexico), and $50 per year (international). Subscriptions are to be paid in US dollars, and are only accepted on a per-volume basis, starting with the first issue. All subscriptions will be automatically renewed unless the subscriber provides timely notice of cancellation. Address changes must be made at least one month before publication date, and please provide the old address or an old mailing label. Please direct all requests for address changes or other subscription-related questions to the journal via email at fcljsubscribe@law.gwu.edu.

Single and Back Issues: Each issue of the current volume can be purchased for $15 (domestic, Canada and Mexico) or $20 (international), paid in U.S. dollars. Please send all requests for single or back issues to fcljsubscribe@law.gwu.edu.

Manuscripts: The *Journal* invites the submission of unsolicited articles, comments, essays, and book reviews mailed to the office or emailed to fcljarticles@law.gwu.edu. Manuscripts cannot be returned unless a self-addressed, postage-paid envelope is submitted with the manuscript.

Production: The citations in the *Journal* conform to the *Bluebook: A Uniform System of Citation* (20th ed., 2015), copyright by the *Columbia*, *Harvard*, and *University of Pennsylvania Law Reviews* and the *Yale Law Journal*. Variations exist for purposes of clarity and at the editors' discretion. The *Journal* is printed by Joe Christensen, Inc.

Citation: Please cite this issue as 69 FED. COMM. L.J. ___ (2017).

FEDERAL COMMUNICATIONS LAW JOURNAL

GW | LAW

FCBA
FEDERAL COMMUNICATIONS BAR ASSOCIATION

VOLUME 69 ISSUE 2

AUGUST 2017

ARTICLE

NOTES

Cyberbullying is a serious public health problem affecting minors across the United States. Debilitating physical, psychological, and educational consequences are commonplace, and the effects carry on into adulthood. Recently, in the European Union, the European Union Court of Justice formally adopted a "right to be forgotten," giving Internet users the right to have certain content "erased" from the Internet—for the purpose of maintaining privacy. Some have argued that the right to be forgotten could be used as a tool against cyberbullying.

Thus far, the United States has responded to the issue of cyberbullying at the state -level. The effectiveness of these state responses, however, has, however, been questioned. Furthermore, the First Amendment stands in the way of any formal recognition of the right to be forgotten. If U.S. policymakers do decide to respond to cyberbullying at the national level, however, the notice-and-takedown provisions contained within the Digital Millennium Copyright Act of 1998 (DMCA) could provide an alternative model for implementing a mechanism similar to the right to be forgotten. Under this proposed model, minors could, through their parent or guardian, petition a provider of online services to erase narrow categories of speech associated with cyberbullying, with appropriate safeguards in place to protect speakers' First Amendment rights.

The Internet of Things as a Tool for Inclusion and Equality

Jules Polonetsky [*]
Stacey Gray [†]

TABLE OF CONTENTS

* CEO, Future of Privacy Forum.
† Policy Counsel, Future of Privacy Forum.
Adapted from comments filed in June 2016 to the National Telecommunications and Information Association (NTIA) by John Verdi & Chanda Marlowe, Future of Privacy Forum.

I. INTRODUCTION

In the next decade, a critical issue for policymakers and regulators will be the advancement and growing ubiquity of cyber-physical systems, or the Internet of Things (IoT). Consumer-facing IoT systems are already delivering benefits to consumers and society.[1] IoT can also be a powerful tool for inclusion and equality, enabling accessibility for many who have traditionally encountered hardship or exclusion because of physical disabilities or other limitations. Through creative forms of notice and flexible application of the Fair Information Practice Principles (FIPPs), policymakers and regulators can find meaningful ways to protect data privacy while promoting beneficial innovation.

II. THE INTERNET OF THINGS AND PRIVACY

As a threshold matter, not all systems in the Internet of Things (IoT) implicate privacy. While many IoT systems are directly consumer facing, many have little or no connection to individuals. For example, an oil company may install sensors to monitor an Alaskan pipeline,[2] a power generation company may use sensors to predict and avoid potential power failures,[3] and an industrial vendor may collect data from jet engines to monitor the environmental impact of aircraft[4]—all examples of machine-to-machine (M2M) connections that do not collect or reveal information about individuals.[5] Policies aimed towards consumer protection must first distinguish between consumer and non-consumer uses of connected devices if they are to avoid unduly affecting beneficial industrial uses of those devices.

Nonetheless, many IoT systems *do* involve data from or about individuals. Information networks created by IoT promise a wide array of consumer benefits, including improvements in healthcare, efficient traffic management, public safety, convenience, environmental protection, and

1. *See generally* Peter Newman, *THE INTERNET OF THINGS 2017 REPORT: How the IoT is improving lives to transform the world*, BUS. INSIDER (Jan. 12, 2017, 12:12 PM), http://www.businessinsider.com/the-internet-of-things-2017-report-2017-1 [https://perma.cc/7JE8-GKTT].

2. *See* Microsoft Corp. Blogs, *Fueling the Oil and Gas Industry with IoT*, MICROSOFT (Dec. 4, 2014), https://blogs.microsoft.com/iot/2014/12/04/fueling-the-oil-and-gas-industry-with-iot/ [https://perma.cc/X225-DKZL].

3. *See* Dan Woods, *What Is GE Predix Really Building?*, FORBES (Sept. 28, 2016, 6:20 AM), https://www.forbes.com/#6b3810e92254 [https://perma.cc/Y8MR-RFFN].

4. *See* Bhoopathi Rapolu, *Internet of Aircraft Things: An Industry Set to be Transformed*, AVIATION WEEK NETWORK (Jan. 18, 2016), http://aviationweek.com/connected-aerospace/internet-aircraft-things-industry-set-be-transformed [https://perma.cc/8FX4-C3VT].

5. *See 50 Sensor Applications for a Smarter World. Get Inspired!*, LIBELIUM (May 2, 2012), http://www.libelium.com/50_sensor_applications/ [https://perma.cc/J57R-3Q4B] (last accessed March 2, 2017).

business innovation.[6] These benefits are enabled when industry is able to layer applications on top of connected devices to create a network of smart systems. Maximizing such benefits necessarily requires collecting, retaining, and sharing information in new ways. Information sharing on the scale generated by IoT implicates privacy risks and security concerns that have not been traditionally associated with consumer devices, such as household items and personal vehicles.[7]

In addition to legal and regulatory frameworks, business-developed standards designed to address security and privacy issues are necessary to ensure that IoT achieves its full potential. If there are lax controls or insufficient oversight of the collection of personal information through connected devices, consumers will lose trust in the evolving technologies. In the words of European Commission Vice-President Neelie Kroes, responsible for the EU Digital Agenda, the industry "cannot innovate in a bubble if citizens are not coming along for the journey."[8]

The Internet of Things raises new issues for the Fair Information Practice Principles (FIPPs), which have long provided the foundation of consumer privacy protection in this country and embody core privacy values.[9] The FIPPs articulate basic protections for handling personal data: (1) Transparency, (2) Individual Control, (3) Respect for Context, (4) Security, (5) Access and Accuracy, (6) Focused Collection, and (7) Accountability.[10] Over time, as technologies and the global privacy context have changed, the FIPPs have been presented in different ways with different emphases.[11] On balance, the FIPPs are not meant to establish rigid

---

6. *See generally* MCKINSEY GLOB. INST., THE INTERNET OF THINGS: MAPPING THE VALUE BEYOND THE HYPE (June 2015), http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.ashx [https://perma.cc/7KZN-FP99].

7. Janna Anderson & Lee Raine, *The Internet of Things Will Thrive by 2025*, PEW RES. CTR. (May 14, 2014), http://www.pewinternet.org/2014/05/14/internet-of-things/ [https://perma.cc/GR2L-XF9Y].

8. Neelie Kroes, Vice-President, Eur. Comm'n responsible for the Dig. Agenda, Speech at the High-level Internet of Things Conference 4 (May 16, 2011), http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=827 [https://perma.cc/L8S3-N64T].

9. *See generally* ORG. FOR ECON. CO-OPERATION & DEV., *infra* note 10; *see also* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD 1 (Feb. 23, 2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf [https://perma.cc/D23T-EEM8] (applying the FIPPs in a Consumer Privacy Bill of Rights).

10. *See generally id.*; ORG. FOR ECON. CO-OPERATION & DEV., OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 14 (2013),https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf [https://perma.cc/C5RL-XJQF].

11. *See* Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Keynote Address at the Technology Policy Institute Aspen Forum: The Privacy Challenges of Big Data: A View from the Lifeguard's Chair (Aug. 19, 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-challenges-big-data-view-lifeguard's-chair/130819bigdataaspen.pdf [https://perma.cc/RM9R-E3RU].

parameters for the processing of information but rather to serve as high-level guidelines.

While the traditional mechanisms—such as presentations of detailed privacy policies and prompts for consents—have served to promote the FIPPs in many contexts, new mechanisms may be appropriate for some implementations of the Internet of Things. New issues around the FIPPs can be addressed with openness to flexibility and new forms of notice.

III. THE INTERNET OF THINGS AND INCLUSION

When the non-profit Pew Research Center queried more than 1,600 experts on the subject, 83 percent predicted that IoT will "have widespread and beneficial effects on the everyday lives of the public by 2025."[12] Among other advantages, IoT devices can improve public health by keeping patients in closer touch with doctors, reducing highway deaths by automatically braking vehicles to avoid crashes, and boosting food supplies by helping farmers tend their crops.[13] Moreover, IoT systems can improve the day-to-day quality of life for individuals – even those who are not connected to the Internet, who do not know what IoT is, or who may not be able to afford IoT-enabled technology, including disadvantaged groups and rural communities. Specifically:

A. For people who are visually impaired

- OrCam: A wearable video camera that attaches to the wearer's eyeglasses and provides artificial vision technology for the visually impaired. It translates written text to audio in real-time (OrCam MyReader) and recognizes stored faces of individuals and other consumer products (OrCam MyEye).[14]
- Dot: The world's first Braille smart watch, which features a series of dull pins that rise and fall at customizable speeds and allows users to read text messages and e-books.[15]
- Cloud-connected shoe insoles: Developed at MIT Media Lab, works with a mobile device to help the user navigate a city without looking at a smartphone for directions.[16]
- Nest: A home automation system, which allows for control of appliances and home thermostat via smartphone.[17]

12. Anderson & Raine, *supra* note 7.

13. *Id.* at 7.

14. OR CAM, http://www.orcam.com/ [https://perma.cc/C8UL-CC3P] (last visited May 20, 2016).

15. DOT, INC., https://dotincorp.com/ (last visited May 20, 2016).

16. Emily Gertz, *Toe Tickling Shoes Let you Navigate the City by Touch*, POPULAR SCIENCE, (May 20, 2016) http://www.popsci.com/article/gadgets/toe-tickling-shoes-let-you-navigate-city-touch [https://perma.cc/N74U-MLCU]. The SuperShoes insoles include small motors that tickle the wearer's toes to indicate which direction to walk, a microcontroller, and a low-power Bluetooth transmitter that wireless connects the insoles with the user's smartphone. *Id.*

- iRobot's Roomba[18]: A smart vacuum cleaner equipped with software and sensors that allow it to efficiently navigate rooms.

B. For people with mobility-related limitations

- Smart Home assistants, such as the Amazon Echo or Google Home, that are "always ready" or able to be activated by a wake phrase, allow users to control things in the home remotely, such as lights, door locks, or security systems.[19]
- Connected vehicle technologies, such as General Motor's Super Cruise driver-assistance technology (scheduled to be introduced in 2017 model Cadillacs), can provide semi-autonomous operation.[20]
- Indoor Location Mapping: Allows the user to identify the location of various services, including ramps, accessible services, and escalators and elevators in public places.[21]

C. For people who are hearing impaired

- Ring[22]: A connected doorbell and home security solution, which alerts users to motion and allows residents to remotely monitor their door.
- Oticon Opn[23]: A connected hearing aid that can be programmed to communicate with a range of other connected devices, such as smoke detectors, baby monitors, or other smart home devices.

D. For older adults and the elderly

- Lively[24]: Sensors that alert relatives when an older family member fails to take medicine, eat, or return home from a walk.

---

17. *Nest app—Your Home in Your Hand*, NEST, https://nest.com/app [https://perma.cc/JS55-7WZM] (last visited May 20, 2016); GLOB. INITIATIVE FOR INCLUSIVE INFO. & COMMC'N TECHS, *Internet of Things: New promises for Persons with Disabilities* (July 2015), http://www.g3ict.org/press/press_releases/press_release/p/id_89 [https://perma.cc/Z9GZ-E4EN].

18. *Roomba–Your Partner for a Cleaner Home,* IROBOT, http://www.irobot.com [https://perma.cc/KPR6-SKUP] (last accessed May 20, 2016).

19. GLOB. INITIATIVE FOR INCLUSIVE INFO. & COMMC'N TECHS, *supra* note 17.

20. *Id.;* Paul Stenquist, *In Self-Driving Cars, a Potential Lifeline for the Disabled*, N.Y. TIMES (Nov. 7, 2014), http://www.nytimes.com/2014/11/09/automobiles/in-self-driving-cars-a-potential-lifeline-for-the-disabled.html?_r=0 [https://perma.cc/4B5B-NVYG].

21. Corinne Iozzio, *Indoor Mapping Lets the Blind Navigate Airports,* SMITHSONIAN.COM (Aug. 8, 2014), http://www.smithsonianmag.com/innovation/indoor-mapping-lets-blind-navigate-airports-180952292/ [https://perma.cc/KPC4-RMF7].

22. *Never Miss a Visitor,* RING, https://ring.com [https://perma.cc/2MEW-DVKY](last visited May 20, 2016).

23. Victoria Woollaston, "These Hearing Aids Link to Smart TVs, Doorbells and Smoke Alarms So Wearers Never Miss a Beat", WIRED (Jan. 2, 2017), http://www.wired.co.uk/article/oticon-smart-hearing-aid [https://perma.cc/5QZK-QTHJ] (last visted June 19, 2017).

E. For those with health concerns

- Continuous Glucose Monitoring (CGM)[25]: A wearable device that displays a constant reading of blood glucose level by inserting a tiny electrode under the skin which then transmits the glucose reading via wireless radio frequency to a display device. Reports may be shared with parents and with care providers.
- Ralph Lauren's Polo Tech Shirt[26]: A shirt with conductive threads and a small snap-on module that relays information like heart rate and breathing data to a Bluetooth-connected mobile device.

F. For people who are hospitalized

- General Electric (GE) Healthcare has developed technology to keep hospitals more sanitary and to reduce medical errors. GE's technology can determine whether soap and sanitizer dispensers are used by medical personnel before and after seeing a patient.[27]
- GE Healthcare technology can also track when patients get in and out of bed to help prevent falls, monitor clinical roundups to ensure that clinicians check on patients at least once per hour, and can help prevent and treat painful pressure ulcers.[28]
- AiCure[29]: A company that combines video facial recognition and artificial intelligence, can help confirm that patients have taken their medication.

---

24. *Lively 24/7 Emergency Medical Alert System,* LIVELY, http://www.mylively.com/how-it-works [https://perma.cc/AZC8-PECN] (last accessed May 20, 2016).

25. *See generally, Continuous Glucose Monitoring,* MEDTRONIC, http://www.medtronicdiabetes.com/products/continuous-glucose-monitoring [https://perma.cc/T2T6-H9YJ] (last accessed May 20, 2016); GLOB. INITIATIVE FOR INCLUSIVE INFO. & COMMC'N TECHS, *supra* note 17.

26. Tim Moynihan, *Your Next Polo Shirt Could Have an Activity Tracker Built Right In*, WIRED (Aug. 27, 2014 6:30 AM), https://www.wired.com/2014/08/ralph-lauren-polo-tech-shirts/ [https://perma.cc/2F24-C3V8].

27. *See GE Scientists Develop Multi-sensing Handheld Probe to Assess and Prevent Pressure Ulcer Formation During Hospital Stays*, GE GLOBAL RES. (Mar. 19, 2015), http://www.geglobalresearch.com/news/press-releases/ge-scientists-develop-multi-sensing-handheld-probe-to-assess-and-prevent-pressure-ulcer-formation-during-hospital-stays [https://perma.cc/N7MQ-6ABV]; *GE Healthcare and Summerville Medical Center Hail AgileTrac Success*, GE HEALTHCARE (Apr.12, 2013), http://newsroom.gehealthcare.com/ge-healthcare-and-summerville-medical-center-hail-agiletrac-success/ [https://perma.cc/S43E-CVT9].

28. *Id.*

29. *See Ai Cure Technologies is Awarded Patent for Interactive Medication Adherence Monitoring System*, AICURE (Dec. 16, 2013), https://aicure.com/ai-cure-technologies-is-awarded-patent-for-interactive-medication-adherence-monitoring-system/ [https://perma.cc/J48T-BXZ5.].

G. For the economically disadvantaged

- Smart meters offer access to detailed consumption data that can assist customers in managing their energy usage, which may save customers money on their energy bills.[30]
- M2M technology: Expands consumers' access to credit by enabling two new payment methods: pay-as-you-go ("PAYG") asset financing, which allows consumers to pay for products over time and prepaid, where consumers pay for services on an as-needed basis.[31]

H. For farmers in rural communities

- Crop sensors can relay information to application machines, which then release the appropriate amount of fertilizers and pesticides.[32] Soil sensors can provide similar information leading to efficient irrigation.[33]
- Real-time equipment maintenance[34]
- Aerial monitoring to detect changes in crop conditions[35]
- Thermal sensors can identify sick livestock by body temperature[36]

I. Improving Interoperability and Access

Many of the devices described above can bring benefits to more than one type of user or fulfill more than one purpose. For example, voice-enabled assistants such as the Amazon Echo can assist people who are visually impaired, but can also be useful for the elderly, or for people with injuries or other physical or mobility-related limitations.

Ultimately, promoting a more inclusive Internet may require using a significant amount of personal data and will almost certainly benefit from

---

30. *See Smart Meters*, SMART GRID CONSUMER COLLABERATION, http://www.whatissmartgrid.org/smart-grid-101/smart-meters [https://perma.cc/X8P7-NCYH] (last visited Apr. 19, 2017).

31. Pat Wilson & Stephanie Pow, *Financial Inclusion and the Internet of Things: How Smart Machines Can Benefit the Poor*, NEXT BILLION (Aug. 4, 2014), http://nextbillion.net/financial-inclusion-and-the-internet-of-things/ [https://perma.cc/H5MW-RVZ4].

32. Christopher Long, *Internet of Things Not Just for Cities*, NEXT BILLION (Nov. 10, 2015), http://www.govtech.com/fs/internet/Internet-of-Things-Not-Just-for-Cities.html [https://perma.cc/R62H-7DL2].

33. *Id.*

34. *Id.* ("[S]ensors embedded in equipment transmit real-time data and alert farmers to any needed maintenance before a breakdown occurs.").

35. *Id.* ("Drones with optical and multi-spectral sensors allow farmers to gather vast amounts of data and remotely monitor the health of their crops. Using this data, farmers can easily assess crop conditions using the Normalized Difference Vegetation Index (NDVI), which has its roots in the space program and measures variances in vegetation.").

36. *Id.*

cloud-based infrastructure. For example, Raising the Floor, a consortium of academic, industry, and non-governmental organizations and individuals, has created the Global Public Inclusive Infrastructure (GPII) Project.[37] "GPII is a software and service enhancement to existing broadband infrastructure designed to . . . improve the interoperability" of assistive technologies by building in "ubiquitous accessibility" features.[38] The system is designed to provide a means for an individual to express accurate and current information about their needs and preferences in a given context and in a common language that can be understood by technical systems and services.[39] Such a storage system for private preferences and permissions would necessarily require significant data collection,[40] but nonetheless holds tremendous promise for expanding Internet accessibility.

IV. EMERGING INDUSTRY STANDARDS AND NORMS

Many of the assistive IoT technologies described above involve connected devices that are worn on the body, like the OrCam or the Dot (Braille smart watch), or comprise elements of an "always ready" Smart Home, like the Amazon Echo or the Google Home. These sub-categories of connected devices are illustrative of the benefits of assistive technology as well as the challenges of regulating IoT to protect consumer privacy.

A. Wearables

Wearable devices, which include fitness trackers, glasses, jewelry, clothing, and other body-worn items incorporating sensors and technology, and their related apps and services ("Wearables") help users track physiological information and hold the potential to improve lives.[41] Wearables deploy sensors to collect environmental, behavioral, and social data for and from their users.[42] Consumer-generated data from these devices is already creating substantial benefits for users by helping individuals manage their fitness, exercise, and biofeedback, improving personal

37. *About the Global Public Inclusive Infrastructure (GPII)*, GLOBAL PUB. INCLUSIVE INFRASTRUCTURE, http://gpii.net/About.html [https://perma.cc/2PFF-Z4F6] (last accessed Mar. 2, 2017).

38. *Id.*

39. *See id.*

40. *Private Preference & Permission System*, GLOBAL PUB. INCLUSIVE INFRASTRUCTURE, http://gpii.net/programs/private-preference-permission-system [https://perma.cc/7UEQ-2DQ7] (last visited Mar. 2, 2017).

41. *See generally* FUTURE OF PRIVACY FORUM, BEST PRACTICES FOR CONSUMER WEARABLES AND WELLNESS APPS & DEVICES 1–3 (Aug. 2016), https://fpf.org/wp-content/uploads/2016/08/FPF-Best-Practices-for-Wearables-and-Wellness-Apps-and-Devices-Final.pdf [https://perma.cc/ELZ5-KR2A]; Janice Phaik Lin Goh, *Privacy, Security, and Wearable Technology*, LANDSLIDE, Nov.–Dec. 2015, https://www.americanbar.org/content/dam/aba/publications/landslide/2015-november-december/ABA_LAND_v008n02_privacy_security_and_wearable_technology.authcheckdam.pdf [https://perma.cc/VM2F-UQU7].

42. *Id.*

productivity and efficiency, and making other technologies simpler and easier to use. Research based on data collected by Wearables could reveal insights that lead to early detection of medical conditions and other broad societal benefits.

If the data collected by Wearables is not properly protected or if used in unethical or illegal ways, individuals' privacy could be at risk. Critics worry that users could find themselves unfairly discriminated against by employers or insurers on the basis of their self-generated information or have their reputations damaged or their safety put at risk by a data breach.[43]

Given the potential benefits that Wearables and consumer-generated wellness data may provide to consumers and society, it is important that this data be subject to privacy controls and used responsibly. Many leading Wearables providers and mobile application (app) developers have already set clear parameters for the collection and use of consumer-generated wellness data.[44] Platforms and devices that enable third-party apps or services to access data have also set forward terms for how those apps or services may use data collected via those devices or platforms.[45]

In many areas, data collected by Wearables is already subject to legal protections. In the United States, these protections include sector-specific regulations such as Children's Online Privacy Protection Act (COPPA), Federal Credit Reporting Act (FCRA), or the Americans with Disabilities Act (ADA), as well as federal and state laws governing insurance and illegal discrimination.[46] In many cases, personal wellness information is covered by Health Insurance Portability and Accountability Act (HIPAA), which imposes certain privacy and security requirements on healthcare providers and their business associates.[47] Medical devices that can be worn or carried like a consumer Wearable are also regulated for safety by the Food and Drug Administration (FDA).[48]

---

43. Patience Haggin, *As Wearables in Workplace Spread, So Do Legal Concerns*, WALL ST. J. (Mar 13, 2016, 10:12 PM ET), https://www.wsj.com/articles/as-wearables-in-workplace-spread-so-do-legal-concerns-1457921550?mg=prod/accounts-wsj&mg=prod/accounts-wsj [https://perma.cc/ACW7-46TW].

44. *See, e.g.*, *CDT and Fitbit Report on Best Privacy Practices for R&D in the Wearables Industry*, CTR. FOR DEMOCRACY & TECH. (May 18, 2016), https://cdt.org/insight/cdt-fitbit-report-privacy-practices-rd-wearables-industry/ [https://perma.cc/TDV4-CJPF].

45. *See, e.g.*, *Healthkit*, APPLE, https://developer.apple.com/documentation/healthkit [https://perma.cc/VW2W-SM7M] (last visited Aug. 7, 2017).

46. *See, e.g.*, *FPF List of Federal Anti-Discrimination Laws*, FUTURE PRIVACY F. (May 21, 2014), https://fpf.org/2014/05/21/fpf-list-federal-anti-discrimination-laws/ [https://perma.cc/E685-MXS4].

47. *See generally* Kristen Lee, "Wearable Health Technology and HIPPA: What Is and Isn't Covered," TECHTARGET (last visited July, 30 2017, 11:26 PM ET), http://searchhealthit.techtarget.com/feature/Wearable-health-technology-and-HIPAA-What-is-and-isnt-covered [https://perma.cc/CHU8-7ZXT].

48. *See generally What is a Medical Device?*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/aboutfda/transparency/basics/ucm211822.htm [https://perma.cc/232F-BG7Z] (last visited July 30, 2017, 11:27 PM ET).

However, many Wearables collect data that is unlikely to be covered by specific sectoral protections. Sometimes this data will be of low sensitivity and of the sort that some users will share with friends or publicly. For example, consumers may feel more comfortable sharing fitness progress data, like how many miles or steps they have taken in a day, as well as broad demographic information like gender. Other times, the data can be of the sort that can reveal highly sensitive facts about users and is information users will expect to be treated confidentially. Depending on the type of app, the types of uses, and the types of controls, the same data may be subject to very different user expectations.[49] In many instances, user expectations for data uses by new apps and new services are still evolving as new benefits and new risks become apparent.

In Europe and other jurisdictions, national (and soon EU-wide) privacy laws set baseline privacy and security expectations. While such laws provide the starting point for data protection, they often also impose higher standards on personal information that is considered especially sensitive, such as health or financial data.[50] In some cases, consumer-generated wellness data is likely to fall within such protected categories. The European Data Protection Supervisor, for example, has noted that:

> "Lifestyle and well-being data will, in general, be considered [sensitive] health data, when they are processed in a medical context…or where information regarding an individual's health may reasonably be inferred from the data (in itself, or combined with other information), especially when the purpose of the application is to monitor the health or well-being of the individual (whether in a medical context or otherwise)."[51]

Where lifestyle or wellness data *is* considered sensitive, additional restrictions on data processing are imposed. As the Article 29 Working Party has noted, however, "on the other side of the spectrum . . . there is a

---

49. *See, e.g.*, Rosie Spinks, *Using a fitness app taught me the scary truth about why privacy settings are a feminist issue*, QUARTZ (Aug. 01, 2017), https://qz.com/1042852/using-a-fitness-app-taught-me-the-scary-truth-about-why-privacy-settings-are-a-feminist-issue/ [https://perma.cc/EGD7-L4R8].

50. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 9, 2016 O.J. (L 119), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 [https://perma.cc/2N6Y-PQHP]. We also note that the recently published draft of the e-Privacy Regulation by the European Commission contains provisions related to the protection of "electronic communications data," and although it is still a draft, the Regulation could be interpreted broadly in coming years. *See Proposal for an ePrivacy Regulation*, EUR. COMMISSION, https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation [https://perma.cc/4JSX-2K4A] (last visited Mar. 2, 2017).

51. Giovanni Buttarelli, *Opinion 1/2015 Mobile Health: Reconciling Technological Innovation with Data Protection*, EUR. DATA PROTECTION SUPERVISOR (May 21, 2015), https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf [https://perma.cc/US9S-RLDQ].

category of personal data generated by lifestyle apps and devices that is, in general, not to be regarded as [sensitive] health data."[52] There are also some apps and devices where "it is not obvious at first sight whether or not the processing of these data should qualify as the processing of health data."[53]

It is important to distinguish between personal data that are, on the one hand, clearly akin to medical information which reveal inherently sensitive details about an individual's health status and, on the other hand, those raw or low-impact personal data that do not expose an individual's private health information. Given the lack of bright lines between sensitive health and non-sensitive lifestyle data, treating all health-related personal data the same would be a mistake. The stringent privacy, security, and safety requirements appropriate for medical devices and medical data would render many commercial fitness devices impractical for everyday consumers. At the same time, it would be a mistake to treat wellness data as if it were generic personal information without any sensitivity.

Rather, we should recognize that these data exist on a spectrum and that privacy protections and legal frameworks should be calibrated to the nature and sensitivity of the data, the social benefits from re-use of the data, controls exercised to protect against misuse of data, and consumers' evolving expectations. Where personal health or wellness data are inherently more sensitive, for example, their collection and use should be based on a narrower specification of purpose; additional consents should be required for each specified use; and all advertising should be based on express consent. But where data are less inherently concerned with health, a specified purpose might appropriately capture a *range* of tightly-related purposes, rather than requiring individualized notices for each and every compatible collection or use of wellness data, and advertising might be presented on an opt-*out* basis. For example, an app that captures a user's steps, height, and weight and whose purpose is to improve users' general fitness and wellness should be able to offer users the opportunity to consent to all compatible wellness or fitness uses of their data at once, rather than requiring additional notices and consents for every related purpose.

In determining where data fall on this spectrum, some relevant factors to consider would include: the context and purpose for which data are collected and used; whether data are inherently/clearly medical data; whether the data is made available to a member of the medical community; whether there is a clear and close link between the data and a user's health status; whether data is used to measure or predict health risks and/or to enable medical follow-up; whether conclusions are or can be reasonably drawn about the health status of a user based on the data; the compatibility of the use; and the existence of appropriate safeguards.[54] Practical guidance

52. EUR. COMISSION, ARTICLE 29 WORKING PARTY, ANNEX–HEALTH DATA IN APPS AND DEVICES 3, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf [https://perma.cc/6FAS-GY6F] (last visited July 30, 2017).

53. *Id.*

54. *See id.*

that can be further tailored to meet local requirements can build upon existing legal expectations. Apps and devices that capture other personally identifiable information should look to existing best practices and guidance documents, such as the FTC *Internet of Things Report*,[55] the Article 29 Working Party *Opinion on the Recent Developments on the Internet of Things*,[56] or the FPF-CDT *Best Practices for Mobile Application Developers*.[57]

B. "Always Ready" Home Devices

"Speech recognition—the ability to speak naturally and contextually with a computer system in order to execute commands or dictate language"[58]—has improved dramatically in recent years. Although the technology is far from perfect—the accuracy is diminished by background noise and recording quality, and certain accents are often more easily understood than others[59]—consumers in 2017 can now interact reasonably well via speech with a range of devices. This includes waking up and asking, "what's on my calendar?" to calibrating a connected thermostat, to dictating a text message or starting a browser search with the likes of "OK, Google," "Hey, Siri," "Hi Alexa," or "Hey, Cortana."

The benefits of speech recognition technology can be especially life-changing for people with disabilities, physical limitations, or visual impairments. Devices like the Amazon Echo, in part due to their affordability, provide a tool of independence even for routine tasks such as adjusting the lights, scheduling appointments, or ordering groceries.[60]

---

55. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/98AN-VMEU].

56. Article 29 Protection Working Party, *Opinion 8/2014 on the Recent Developments on the Internet of Things*, EUR. COMMISSION (Sept. 16, 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf [https://perma.cc/SK5L-U9FL].

57. FUTURE OF PRIVACY FORUM & CTR. FOR DEMOCRACY & TECH., BEST PRACTICES FOR MOBILE APPLICATION DEVELOPERS (2011), https://www.cdt.org/files/pdfs/Best-Practices-Mobile-App-Developers.pdf [https://perma.cc/3KAP-DYY3].

58. STACEY GRAY, FUTURE OF PRIVACY FORUM, ALWAYS ON: PRIVACY IMPLICATIONS OF MICROPHONE-ENABLED DEVICES 4 (2016), https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf [https://perma.cc/U87G-LEAH].

59. Speech recognition expert Marsal Gavaldà calls this diminished accuracy for children, seniors, and people with accents "the speech divide." *See* Nora Young, *Here's Why Your Phone Can't Understand Your Accent*, CBC RADIO (Sept. 13, 2015), http://www.cbc.ca/radio/spark/292-what-you-say-will-be-searched-why-recognition-systems-don-t-recognize-accents-and-more-1.3211777/here-s-why-your-phone-can-t-understand-your-accent-1.3222569 [https://perma.cc/98FG-N7KG]; *see also* Daniela Hernandez, *How Voice Recognition Systems Discriminate Against People with Accents*, SPLINTER (Aug. 21, 2015, 7:00 am), http://fusion.net/story/181498/speech-recognition-ai-equality/ [https://perma.cc/K78Y-JH8P].

60. *See* Allen St. John, *Amazon Echo Voice Commands Offer Big Benefits to Users with Disabilities*, CONSUMER REP. (Jan. 20, 2017),

A key feature is that by sending data to the cloud, where powerful computing can be applied, speech recognition services can improve over time.[61] Making use of the huge advancements in data processing in recent years, voice-to-text technologies can now adapt to your speech patterns over time and are getting better at understanding speech in context.[62] This aspect led early voice recognition pioneer Raj Reddy to predict that voice recognition technologies would pass the Turing Test in our lifetimes.[63]

"The same feature of speech recognition technology that makes it useful—its ability to bring voice control into our everyday lives—is the feature that is now understandably raising privacy concerns, as microphone-enabled devices become integrated into our homes and daily environments."[64] Speech activated "always ready" devices, such as the Amazon Echo or the Google Home, use the power of "energy efficient processors to remain in an inert state of passive processing for a pre-set 'wake phrase'."[65] "The device buffers and re-records locally, without transmitting or storing any information, until it detects the word or phrase that triggers the device to begin actively recording".[66] This key feature is critical to enabling greater digital access to people with disabilities or physical limitations: rather than requiring the user to manually turn the device on, or designing it transmitting data constantly, the device can be activated verbally such that it only transmits data when the user wants it to do so.

In contrast, other devices are designed to truly be "always on." "Always on devices are those designed to record and transmit data all of the time."[67] "Most prominently, this includes home security cameras and baby monitors but also includes a range of new devices."[68] "Cities can now detect gunfire via microphone networks and there are microphones that can detect termite infestations by listening to audio outside of the range of the human ear."[69] "These devices, because they are designed to be always on, evoke different privacy concerns from those that are manually or speech activated, and call for notice and consent frameworks in sync with the more extensive data collection that they enable."[70]

---

http://www.consumerreports.org/amazon/amazon-echo-voice-commands-offer-big-benefits-to-users-with-disabilities/ [https://perma.cc/5SWB-6QS9].

61. *See generally* Xuedong Huang, James Baker & Raj Reddy, *A Historical Perspective of Speech Recognition*, COMM. ACM, Jan. 2014, at 94, http://cacm.acm.org/magazines/2014/1/170863-a-historical-perspective-of-speech-recognition/abstract [https://perma.cc/DW97-9BBM].
62. *Id.*
63. *Id.*
64. GRAY, *supra* note 58.
65. *Id. at 5.*
66. *Id.*
67. *Id.*
68. *Id.*
69. *Id.*
70. *Id.* at 6.

"Microphones and specifically voice data retain unique social and legal significance."[71] "In some instances, laws that protect biometric information may apply."[72] "In general, sector-specific laws and regulations will also apply on the basis of the content of the voice communications."[73] "The collection of certain voice characteristics for the purpose of recognizing an individual, for example, implicates a range of laws".[74] **"**At the federal level, a 'voice print' is considered either a biometric or personal record in the context of the Privacy Act,[75] [Federal Educational Rights and Privacy Act (FERPA)],[76] and HIPAA,[77] and thus subjected to greater regulatory restrictions."[78] "Similarly, several states have expanded their legal definitions of personally identifiable information in certain identity theft or breach notification laws to include some form of biometrics."[79]

However, "the majority of speech-enabled devices on the market today are not designed for the purpose of uniquely identifying a person through the biometric characteristics of her voice."[80] "Instead, they aim to create products for which speech is a useful interface for engagement."[81] "In the future, however, it can be foreseen that unique voice recognition might become a useful consumer tool—for example, to permit only a specific person to access a device, or to enable parental controls by distinguishing between user accounts."[82] "Companies considering adding such features should be aware of the increasing number of federal and state laws regarding biometric identification."[83]

---

71. *Id.*
72. *Id.*
73. *Id.*
74. *Id.*
75. 22 C.F.R. § 308.3 (2017) ("Record means any document, collection, or grouping of information about an individual maintained by the agency, including but not limited to . . . any other personal information which contains . . . a finger or voiceprint.").
76. 34 C.F.R. § 99.3 (2017) ("Biometric record, as used in the definition of personally identifiable information, means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include . . . voiceprints.").
77. 45 C.F.R. § 164.514 (2017) (listing "[b]iometric identifiers, including finger and voice prints" as examples of personal information that must be removed from a data set before that data set can be considered properly de-identified and thus no longer subject to HIPAA regulations).
78. GRAY, *supra* note 58, at 6–7.
79. *Id.*; *see, e.g.*, CONN. GEN. STAT. ANN. § 38a-999b (West 2017); IOWA CODE ANN. § 715C.1 (West 2017); NEB. REV. STAT. ANN. § 87–802 (West 2017); N.C. GEN. STAT. ANN. § 7566 (West 2017); OR. REV. STAT. ANN. §§ 165.800, 336.184 (West 2017) (regulating student educational records); WIS. STAT. ANN. § 943.201 (West 2017); WYO. STAT. ANN. § 6–3–901 (West 2017).
80. GRAY, *supra* note 58, at 7.
81. *Id.*
82. *Id.*
83. *Id.*; *see* 22 C.F.R. § 308.3 (2017) ("Record means any document, collection, or grouping of information about an individual maintained by the agency, including but not limited to . . . any other personal information which contains . . . a finger or voiceprint."); 34 C.F.R. § 99.3 (2017) ("Biometric record, as used in the definition of personally identifiable information means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include

"Moving forward it will be important to recognize that voice data is unique in its historical protection, communicative content, and biometric features."[84] "Useful guiding principles are beginning to emerge",[85] and companies can take many steps to build trust in these devices, including: (1) strong security measures, including encryption of data at rest and in transit; (2) hardware-level "on/off" switches, to address concerns about remote access; and (3) access to and ability to delete audio data.

Conversations will continue to evolve on this subject as social norms shift about when and where we should expect to be able to speak to our devices. In considering the benefits of speech-enabled devices in parallel to their legitimate privacy implications, forward-looking companies will be well-served to use the power of technology itself to enable the power of speech recognition while protecting consumer privacy and control.

V. CONCLUSION

When developing policies for IoT, policymakers must involve all stakeholders, including members of disability communities. Increasingly, privacy laws and regulations have an impact on assistive technologies, and policy discussions benefit from the involvement of those who are directly affected. For example, state laws restricting the collection of biometric identifiers might unintentionally hamper technologies that enable devices like the OrCam.[86] These devices and others—such as self-driving cars, cloud based screen readers, home monitoring systems, and many more—may rely on data-supported IoT technologies to deliver services.

Policymakers also need to allow for the fact that it will not always be practical to address the collection and use of personal information via traditional notice and choice mechanisms. Many connected devices will not have screens or interfaces that readily present privacy notices or allow consumers to select specific data practices. As a result, a flexible approach to the FIPPs will be needed. Many IoT devices are beginning to provide notice of data collection through visual, auditory, and tactile cues.[87]

. . . voiceprints"); 45 C.F.R. § 164.514 (2017) (listing "[b]iometric identifiers, including finger and voice prints" as examples of personal information that must be removed from a data set before that data set can be considered properly de-identified and thus no longer subject to HIPAA regulations).

84. GRAY, *supra* note 58, at 10.

85. *Id.*; LYNN TERWOERD ET AL., VOICE PRIVACY GUIDING PRINCIPLES, (2016), http://c.ymcdn.com/sites/www.ewf-usa.com/resource/collection/CAA076AF-9566-4E1E-9F07-6421154DE0EA/Voice_Privacy_Guiding_Principles_Public_(final).pdf [https://perma.cc/7WL5-6TNC].

86. *E.g.*, 740 ILL. COMP. STAT. 14/1 to 14/99 (2017).

87. The Amazon Echo, for example, uses a light ring to visually communicate its status. *See Alexa and Alexa Device FAQs*, AMAZON, http://www.amazon.com/gp/help/customer/display.html?nodeId=201602230 [https://perma.cc/Q7JM-Y22S] (last visited July 31, 2017). When the light is solid blue, the device is transmitting audio data. *See Id.* When all lights are off, the device is active and waiting for the user's request. *See Id.* Those who want to know more about the Echo's

Flexible and design-centered approaches such as these will help pave the way towards effective, consumer-protective policies for the Internet of Things. With the FIPPs as a guide to notice and consent frameworks, and a firm understanding of the nuances of the many devices entering the market, policymakers can protect consumer privacy while encouraging IoT as a tool for inclusion.

---

privacy policy can ask, "Alexa, are you spying on me?" and in response the device will state, "I only send audio back to Amazon when I hear you say the wake word. For more information and to view Amazon's privacy notice, visit the help section of your Alexa app." *See Id.*

A New Method to Address Cyberbullying in the United States: The Application of a Notice-and-Takedown Model as a Restriction on Cyberbullying Speech

Brian O'Shea *

TABLE OF CONTENTS

* J.D., The George Washington University Law School, May 2017. Notes Editor, *Federal Communications Law Journal*, 2016–17. B.A., Saint Anselm College. The author would like to thank his mother Karen and the rest of his family and friends for their constant love and support.

I. INTRODUCTION

Ghyslain Raza. His story is one many may not want to remember—but should never forget. One day, while at school in Quebec, Canada, Raza was going about his day like any typical 14-year-old. He had countless things to look forward to: spending time with friends, high school, and enjoying what are supposed to be some of the best years of life. His teenage innocence, however, was about to be ripped away from him far too soon.

As part of a school project, Raza entered a television studio at his school and had someone film him reenacting a lightsaber scene from *Star Wars*. Raza submitted the seemingly harmless and inconsequential video in his class and then went on with his life.[1]

A year later, the video was posted on YouTube, without Raza's consent, and quickly went "viral." Within days of its posting, the video was well on its way to becoming the most popular Internet video of all time. But rather than enjoying his newfound celebrity, Raza was faced with a massive cyberbullying onslaught from people he did not know.[2] "What I saw was mean. It was violent. People were telling me to commit suicide," Raza said of the video's release.[3] Raza further commented that "no matter how hard I tried to ignore the people telling me to commit suicide, I could not help but feel worthless, like my life was not worth living."[4] Raza was subjected to so much bullying that he lost the few friends he did have, he transferred schools, was diagnosed with depression, and eventually was forced to enter a children's psychiatric facility.[5]

Raza's story is just one case in what has become an alarmingly common phenomenon of online bullying, popularly known as "cyberbullying." Today, almost half of all minors in the United States report being victims of cyberbullying.[6] Between four to twenty-one percent of minors admit to having been perpetrators.[7] While popular websites like Facebook, Instagram, and Twitter all have anti-cyberbullying policies in place,[8] these policies alone

---

1. *"Star Wars" Kid Breaks Silence on Cyberbullying*, FOX NEWS: TECH (May 10, 2013), http://www.foxnews.com/tech/2013/05/10/star-wars-kid-breaks-silence-on-cyberbullying/ [https://perma.cc/7SAK-VXUZ].
2. *Id*.
3. *Id*.
4. *Id*.
5. *See* Maureen O'Connor, *Star Wars Kid Is All Grown Up and Becoming a Lawyer* (Oct. 5, 2015, 1:53 PM), http://gawker.com/5554731/stars-wars-kid-is-all-grown-up-and-becoming-a-lawyer [https://perma.cc/N5XQ-LJXB].
6. Bethan Noonan, *Developments in the Law: Technology and Social Media in the 21st Century: Solutions for Minimizing the Risk to Children: Crafting Legislation to Prevent Cyberbullying: The Use of Education, Reporting, and Threshold Requirements*, 27 CONTEMP. HEALTH L. & POL'Y 330, 335 (2011).
7. *Id*.
8. *Community Standards*, FACEBOOK, https://www.facebook.com/communitystandards [https://perma.cc/6VTC-C75D] (last visited Jan. 28, 2017); *Community Guidelines*, INSTAGRAM, https://help.instagram.com/477434105621119/ [https://perma.cc/BG6N-28NK] (last visited

are not sufficient. Young people continue to bully each other, often through the posting of images and videos designed to publicly shame or humiliate the subjects.[9] Unlike with words, where the subject may be more covert, the subject of an image or video may be far more visible. The subject of visual content can often be readily identified by observers, creating the potential for more bullying in the virtual and physical worlds.[10] Most disturbing of all, when the content is posted, there is often no way of getting it down from the Internet.[11] For people like Raza (whose video remains readily available online) and other victims, there is no escape.

Due to the Internet's ubiquity,[12] cyberbullying is not going to disappear anytime soon. Any young person, Internet user or not, is in danger of becoming a victim. While there is no obvious or perfect solution to this issue, a 2014 ruling by the European Court of Justice (ECJ) allowing individuals to petition to have certain content removed from the Internet due to a so-called "right to be forgotten."[13] Adopting the ECJ's petition process may change the landscape for those seeking to restrict cyberbullying speech in the United States.

Currently, there is no right to be forgotten in the United States, and the constitutionality of such a right is in some doubt due to its potential to restrict, or chill, free speech.[14] However, there already exists a comparable mechanism in the form of copyright notice-and-takedown procedures, which allows

---

Jan. 28, 2017); *Online Abuse*, TWITTER, https://support.twitter.com/articles/15794 [https://perma.cc/PH93-2GAS] (last visited Jan. 28, 2017).

9. *See* NAT'L CRIME PREVENTION COUNCIL, STOP CYBERBULLYING BEFORE IT STARTS, http://www.ncpc.org/resources/files/pdf/bullying/cyberbullying.pdf [https://perma.cc/2Z9H-YGBV]; Temitayo Fagbenle, *Online "Shaming" A New Level of Cyberbullying for Girls*, NPR (Feb. 12, 2016, 4:46 PM ET), http://www.npr.org/2013/01/07/168812354/online-shaming-a-new-level-of-cyberbullying-for-girls [https://perma.cc/MX3G-LYXG].

10. Kimberly J. Mitchell et al., *Prevalence and Characteristics of Youth Sexting: A National Study*, 129 PEDIATRICS 13, 17 (2012) (stating that 70% of study's respondents who appeared in or created sexting images and 63% of respondents who received sexting images reported feeling "very" or "extremely" upset, embarrassed, or afraid, and that such images can lead to increased mental and emotional stress and most seriously suicide).

11. Caroline Hewitt Fischer, Comment, *GoldieBlox and the Three Beastie Boys: The Emerging Trend of Fair Use Appropriation of Protected Material as a Business Marketing Strategy*, 17 TUL. J. TECH. & INTELL. PROP. 255, 258 (2014) ("Unlike television or print media, digital media is very difficult to control and is almost impossible to eliminate after a user uploads it to the Internet.").

12. *See generally* AMANDA LENHART, PEW RESEARCH CENTER, TEENS, SOCIAL MEDIA & TECHNOLOGY OVERVIEW 2015 (2015), http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/ [https://perma.cc/CT4K-9RCR] (detailing social media use by American teenagers in 2015).

13. *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, para. 100(2) (May 13, 2014), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 [https://perma.cc/GF7V-6PBJ] ("[T]he operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person . . . .").

14. *See* Emily Adams Shoor, Note, *Narrowing the Right to Be Forgotten: Why the European Union Needs to Amend the Proposed Data Regulation*, 39 BROOKLYN J. INT'L L. 487, 492-94 (2014).

copyright owners to easily remove unauthorized content from the Internet.[15] If policymakers in the United States decide to grant cyberbullying victims a similar remedy, minors, through their guardians, other agents, or even on their own, could easily remove certain embarrassing or malicious content from the Internet.

This Note argues that if policymakers in the United States wish to implement cyberbullying policies similar to the European Union's "right to be forgotten," they should look to the notice-and-takedown provisions of the Digital Millennium Copyright Act (DMCA) as a model.[16] An analogous framework for cyberbullying could enable users to petition providers of online services for the removal of images and videos where the subject can be personally identified, and the content was posted for the purpose of bullying.

Section II of this Note introduces the growing problem of cyberbullying and the need for a legal solution. Section III details the United States' current approach to cyberbullying and criticisms of that approach. Section IV discusses Europe's right to be forgotten as a potential response to cyberbullying, and why the right is not likely to survive First Amendment scrutiny in the United States. Section V discusses the notice-and-takedown procedures of the DMCA and how policymakers could use these procedures as a model for the purpose of restricting cyberbullying speech. Finally, Section VI proposes a notice-and-takedown mechanism based on the DMCA, discusses why the mechanism will likely survive First Amendment scrutiny, and addresses potential counterarguments and the need for future scholarship.

II. THE PROBLEM OF CYBERBULLYING AND THE NEED FOR A LEGAL SOLUTION

The Internet may be the greatest forum for the exercise of free speech in history.[17] Unlike broadcast or print media, where communication is a one-way street, the Internet facilitates a "true marketplace of ideas"[18] where individuals are able to interact with each other and share content with the rest of the world.[19] It is the "most participatory form of mass speech yet developed."[20] Unfortunately, with all of the benefits that have accompanied the growth of the Internet, there have been several unintended

15. *See* Lauren Yamamoto, Note and Comment, *Copyright Protection and Internet Fan Sites: Entertainment Industry Finds Solace in Traditional Copyright Law*, 20 LOY. L.A. ENT. L. REV. 95, 126–27 (2000).

16. *See* 17 U.S.C. § 512(c)(1) (2012).

17. *See* Anthony Ciolli, *Chilling Effects: The Communications Decency Act and the Online Marketplace of Ideas*, 63 U. MIAMI L. REV. 137, 137 (2008).

18. *Id*.

19. *See* Sarah B. Evans, Note, *Hear No Evil, Speak No Evil, See No Evil: Protecting the Nation's Children from Sexually Explicit Material on the Internet*, 13 TEMP. POL. & CIV. RTS. L. REV. 253, 282 (2003).

20. Nicholas P. Dickerson, Comment, *What Makes the Internet So Special? And Why, Where, How, and by Whom Should Its Content Be Regulated*, 46 HOUS. L. REV. 61, 62 (2009).

consequences.[21] One of these consequences has been the growth of cyberbullying.[22]

Cyberbullying occurs "when a child, preteen, or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen, or teen using the Internet, interactive and digital technologies, or mobile phones."[23] Cyberbullying, therefore, can occur in a variety of ways and can result in a range of different harms. Moreover, cyberbullying can be conducted through a number of different media forms including emails, online videos, mobile messaging, and posts on social media sites.[24] For example, text messages or images may be shared and distributed among an individual's friends, peers, or people they do not even know.[25] With America's teenagers, the main victims of cyberbullying,, becoming more digitally connected over the last decade,[26] consequentially, cyberbullying has been recognized as a serious public health problem due to the substantial and long-lasting impact it can have on its victims.[27]

Although a lack of scientific research has prevented a comprehensive understanding of the prevalence of cyberbullying,[28] the available statistics paint a disturbing picture.[29] Since 2015, nationwide, almost twenty-percent of American high school students report having been victims of cyberbullying.[30]

---

21. *Cf.* Jay Wexler, Book Review, 16 STAN. ENVTL. L.J. 334 (1997) (reviewing EDWARD TENNER, WHY THINGS BITE BACK: TECHNOLOGY AND THE REVENGE OF UNINTENDED CONSEQUENCES (1996)).

22. *See What Is Cyberbullying, Exactly?*, STOPCYBERBULLYING, http://www.stopcyberbullying.org/what_is_cyberbullying_exactly.html [https://perma.cc/82DR-7594] (last visited Jan. 28, 2017).

23. *Id*.

24. *See* Noonan, *supra* note 6, at 331.

25. *See* Clay Calvert, *Fighting Words in the Era of Texts, IMS, and Emails: Can a Disparaged Doctrine Be Resuscitated to Punish Cyberbullies?*, 21 DEPAUL J. ART TECH. & INTELL. PROP. L. 1, 15-16 (2010). *See also* Kathleen Conn, *Sexting and Teen Suicides: Will School Administrators Be Held Responsible?*, 261 ED. LAW REP. 1 (2010) ("Cyberbullies can use the anonymity of cellphones to repeatedly text and torment their teachers, school administrators, or classmates; disseminate sensitive personal information or lies; or pretend to be someone else to torment that person.").

26. *See* Lauren A. Newell, *Redefining Attention (And Revamping the Legal Profession?) for the Digital Generation*, 15 NEV. L.J. 754, 775–76 (2015) (citing MARY MADDEN ET AL., PEW RES. CTR., TEENS AND TECHNOLOGY 2013, at 2, 3 (2013), http://www.pewinternet.org/Reports/2013/Teens-and-Tech.aspx [https://perma.cc/L8SL-PVEY] (stating that approximately 95% of teens use the Internet, approximately 93% of teens own or have access to a computer at home, and approximately 75% of teens own a cellphone or smartphone)).

27. *See* Alison Virginia King, Note, *Constitutionality of Cyberbullying Laws: Keeping the Online Playground Safe for Both Teens and Free Speech*, 63 VAND. L. REV. 845, 849 (2010) (citing Corinne David-Ferdon & Marci Feldman Hertz, *Electronic Media, Violence and Adolescents: An Emerging Public Health Problem*, 41 J. ADOLESCENT HEALTH S1, S5 (2007) (stating that the CDC considers cyberbullying to be an "emerging public health problem.")).

28. *See* Mary Sue Backus, *OMG! Missing the Teachable Moment and Undermining the Future of the First Amendment—TISNF!*, 60 CASE W. RES. L. REV. 153, 160 (2009) (stating that "little research has been done on the phenomenon of cyberbullying, both as to its prevalence and its potential harm").

29. *See* Noonan, *supra* note 6, at 335–36.

30. Ctrs. for Disease Control & Prevention, U.S. Dep't Health & Human Servs., *Youth Risk Behavior Surveillance—United States, 2015*, MMWR SURVEILLANCE SUMMARIES, June

Equally as troubling is that between four to twenty-one percent of youths in the same age range have reported being perpetrators of cyberbullying.[31] The problem is so prevalent that, according to a Harvard-directed study conducted at the behest of state attorneys general, "the most frequent threat minors face, both online and offline, is not sexual predators or harmful content, but rather bullying and harassment, most often by peers."[32]

As observed by one scholar, "[c]yberbullying can be harmful to children in a number of ways, including negatively impacting their health, education, and social lives."[33] It can result in severe psychological harm including depression, anxiety, fear, and low self-esteem.[34] Cyberbullying can also lead to poor academic performance, increased absences from school, or even dropping out of school all together.[35] "In some cases, [cyberbullying can] lead to extreme violent behavior including murder and suicide."[36]

The effects of cyberbullying do not end upon entering into adulthood—nor are they limited to victims. Adults who were once perpetrators of cyberbullying can suffer long-term depression, emotional distress, and anxiety as a result.[37] Dealing with the behavioral health effects of cyberbullying can be a lifelong struggle. Policymakers in the United States have begun to take notice and have attempted to provide much needed relief to address this crisis.

III. STATE RESPONSES TO CYBERBULLYING AND LEGISLATIVE SHORTCOMINGS

As of January, 2016, all fifty states have passed anti-bullying legislation.[38] Approximately half of the states have enacted specific anti-cyberbullying statutes.[39] Federal legislation specifically tailored to respond to cyberbullying had been proposed in the past in the U.S. House of

---

10, 2016, at 10, https://www.cdc.gov/healthyyouth/data/yrbs/pdf/2015/ss6506_updated.pdf [https://perma.cc/S4J9-QQ3G].

31. Noonan, *supra* note 6, at 335–36.

32. Backus, *supra* note 28, at 160.

33. Bryan Morben, Note, *The Fight Against Oppression in the Digital Age: Restructuring Minnesota's Cyberbullying Law to Get with the Battle*, 15 MINN. J.L. SCI. & TECH. 689, 694 (2014) (source refers to a proposed piece of federal anti-cyberbullying legislation called the "Megan Meir Cyberbullying Prevention Act," which was named after a young girl who committed suicide after being bullied while on MySpace).

34. *Id.*

35. *Id.*

36. *Id.*

37. *See id.* at 695.

38. *See* SAMEER HINDUJA & JUSTIN W. PATCHIN, STATE CYBERBULLYING RESEARCH CENTER, STATE CYBERBULLYING LAWS: A BRIEF REVIEW OF STATE CYBERBULLYING LAWS AND POLICIES 1 (2016), http://cyberbullying.org/Bullying-and-Cyberbullying-Laws.pdf [https://perma.cc/FF6E-R6JV].

39. *Bullying and Cyberbullying Laws*, MEGAN MEIR FOUND., http://www.meganmeierfoundation.org/laws.html [https://perma.cc/5S9M-VRKH] (citing HINDUJA & PATCHIN, *supra* note 38) (defining an anti-cyberbullying law as one that specifically includes terms "cyberbullying" or "cyber-bullying," and not just "electronic harassment or bullying using electronic means")).

Representatives, but the proposal never made it out of committee as of this writing.[40]

A. The United States' Response to Cyberbullying Has Occurred at the State Level

Without a national directive, states have been given the freedom to respond to cyberbullying in a variety of different ways—with some responding more aggressively than others. North Carolina, for example, has criminalized the act of cyberbullying when the victim is a minor.[41] Other states, however, have put the onus on school districts to implement plans to combat cyberbullying. Massachusetts has required school districts to implement plans to respond to and report bullying to the state's Department of Secondary and Elementary Education.[42] If a school district fails to take proper action, the state can take punitive action.[43] Florida has decided to condition the dissemination of safe schools funds to its school districts contingent upon its Department of Education's approval of each district's bullying and harassment policies.[44] These individual state responses have not come without their share of controversy, with some states arguing that significant reforms are needed.[45]

B. Criticism of State Cyberbullying Responses and the Need for National Action

State responses to cyberbullying have been a source of criticism for several reasons. First, states have been criticized for not doing more to combat cyberbullying that occurs off school property.[46] While students can be punished for engaging in lewd or obscene speech while on school grounds, the school's reach is typically much more limited when such conduct occurs

40. *See* Megan Meier Cyberbullying Prevention Act, H.R. 1966, 111th Cong. (2009).

41. N.C. GEN. STAT. § 14-458.1 (2015). The North Carolina anti-cyberbullying statute prohibits a variety of conduct on the Internet when the perpetrator's intent is to intimidate or torment a minor, including: constructing a fake website, posing as a minor in a chatroom, email, or instant message, posting or encouraging others to post private, personal, or sexual information pertaining to a minor, and posting real or doctored images of a minor on the Internet. Cyberbullying is punishable as a Class 1 misdemeanor if the perpetrator is over 18 years of age and as a Class 2 misdemeanor if the perpetrator is under 18 years of age. *See id*.

42. MASS. GEN. LAWS ch. 71, § 370 (2010).

43. *Id*.

44. *See* Jamie Wolf, Note, *The Playground Bully Has Gone Digital: The Dangers of Cyberbullying, the First Amendment Implications, and the Necessary Responses*, 10 CARDOZO PUB. L. POL'Y & ETHICS J. 575, 595 (2012). This mechanism in the State of Florida incentivizes schools to develop effective anti-bullying policies. Safe schools funds accounted for a total of $64,456,019 for the 2015-16 fiscal year and $62,660 per school district. See FLA. DEP'T OF EDUC., 2015-16 FUNDING FOR FLORIDA SCHOOL DISTRICTS 17 (2015), http://www.fldoe.org/core/fileparse.php/7507/urlt/Fefpdist.pdf.

45. *See* Backus, *supra* note 28, at 183–85 (providing an overview of state cyberbullying statutes and discussing criticisms).

46. *See* Wolf, *supra* note 44, at 590–92.

outside of the school or school-related functions.[47] This is problematic because most cyberbullying occurs outside of school hours.[48] Second, many statewide anti-bullying efforts concentrate on traditional disciplinary techniques designed to deter individuals from engaging in cyberbullying rather than targeting the harmful content itself.[49] Targeting the harmful content is a challenge for states because of the fear of subjecting themselves to legal action due to interfering with an individual's free speech rights.[50] Finally, with a multitude of states having their own anti-cyberbullying statutes, there is an obvious risk of inconsistent results.[51] Certain online conduct may be considered cyberbullying in one state but, due to a different definition, it may not be cyberbullying in the state next door.[52] This is problematic because cyberbullying is a national issue.

Rather than individual state responses, a legislative response to cyberbullying at the national level may be what is required.[53] As the evidence shows, cyberbullying is a growing public health problem with an impact across the United States.[54] The effects are serious and not only affect victims in their younger years but can affect them well into their adult lives.[55] From a policy perspective, it is essential to develop a single, uniform mechanism to address cyberbullying effectively nationwide.[56]

IV. THE RIGHT TO BE FORGOTTEN AS A POTENTIAL RESPONSE TO CYBERBULLYING AND WHY IT LIKELY WILL NOT SURVIVE FIRST AMENDMENT SCRUTINY IN THE UNITED STATES

As an alternative to the patchwork approach currently in force in the United States, some have argued that the E.U.'s right to be forgotten could provide an innovative method for combatting cyberbullying by targeting the

47. *Id*. at 584.

48. Deborah Ahrens, *Schools, Cyberbullies, and the Surveillance State*, 49 AM. CRIM. L. REV. 1669, 1695 (2012).

49. *See* Wolf, *supra* note 44, at 594–95.

50. *See* Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 506 (1969) (stating that students and teachers do not "shed their constitutional rights to freedom of speech or expression at the schoolhouse gate" and, as a result, in order for free expression to be curbed, the expression must result in a "substantial disruption of or material interference with school activities").

51. *See* Jason A. Wallace, Note, *Bullycide in American Schools: Forging a Comprehensive Legal Solution*, 86 IND. L.J. 735, 743 (2011) (discussing how different anti-bullying laws from different states produce different legal results specifically in the context of anti-gay bullying).

52. *See* Adam J. Speraw, Note, *No Bullying Allowed: A Call for a National Anti-Bullying Statute to Promote a Safer Learning Environment in American Public Schools*, 44 VAL. U.L. REV. 1151, 1153 (2010) (stating that a national anti-bullying law would bring needed consistency for the states that have passed anti-bullying legislation).

53. *Id*.

54. *See* King, *supra* note 27, at 849.

55. *See* Morben, *supra* note 33, at 694.

56. *See* Speraw, *supra* note 52, at 1153.

content itself and making it inaccessible in search results.[57] For the right to be forgotten to become legally enforceable in the United States, however, it would likely have to survive strict scrutiny under the First Amendment.[58] Due to the broad scope of the right to be forgotten and its ability to restrict speech that is not associated with cyberbullying, it is not likely to become a legally enforceable right in the United States.

A. The Right to be Forgotten, Criticisms of the Right, and Its Impact on Speech in the E.U.

In *Google Spain SL v. Agenda Española de Protectión de Datos*, the ECJ recognized, for the first time, a legally binding "right to be forgotten" online.[59] In this case, the Court held that citizens of E.U. member states could petition Google, and other search engines engaged in the processing of personal data, to remove links to webpages containing personal information about the citizen that appears "to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the [data] processing."[60]

Since the *Google Spain SL* ruling, Google has evaluated over 1.8 million links for removal based on over 660,000 requests.[61] Approximately forty-three percent of evaluated URLs have been removed to date.[62] As a result, critics of the right to be forgotten have argued that the policy is a serious infringement upon the right to free speech and the right to freely access information.[63] Rather than restricting online speech through takedown

---

57. *See* Scott H. Greenfield, *Cyberbullying: We'll Know It When We See It*, SIMPLE JUSTICE (Feb. 10, 2012) http://blog.simplejustice.us/2012/02/10/cyberbullying-we-know-it-when-we-see-it/ [https://perma.cc/3DY5-3FT7]; *see also* Michelle Ghoussoub, *Censorship Versus Privacy: The Implications of the "Right to be Forgotten,"* DIGITAL TATTOO (May 21, 2014), http://digitaltattoo.ubc.ca/2014/05/21/censorship-versus-privacy-the-implications-of-the-right-to-be-forgotten-online/ [https://perma.cc/SJN7-N39F].

58. *See, e.g.*, Burson v. Freeman, 504 U.S. 191, 208–10 (1992).

59. *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, (May 13, 2014), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 [https://perma.cc/W5DB-6M2A]. The newly passed EU Data Protection Regulation codifies much of the right to be forgotten online that was originally created by the ECJ. This information can be found within Article 17 of the Regulation. *See Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012) [hereinafter Data Protection Regulation], http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [https://perma.cc/J4P8-5HSZ].

60. *See Google S.L.*, Case C-131/12, at paras. 92–94.

61. *European Privacy Requests for Search Removals*, GOOGLE, https://www.google.com/transparencyreport/removals/europeprivacy/ [https://perma.cc/9WF2-HPX9] (last visited Feb. 4, 2017) [hereinafter *Google Transparency Report*]

62. *Id*.

63. *See* Stephen C. Bennett, *The "Right to be Forgotten": Reconciling EU and US Perspectives*, 30 BERKELEY J. INT'L L. 161, 169 n.30 (2014) (citing FRANZ WERRO, THE RIGHT TO INFORM V. THE RIGHT TO BE FORGOTTEN: A TRANSATLANTIC CLASH 286, 298–99 (2009), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1401357 [https://perma.cc/4QMB-X9DW] (suggesting that "the right to be forgotten is unprotected" in the United States and

requests, critics argue that a greater emphasis should be placed on education and personal responsibility while on the Internet.[64]

In order to determine which takedown requests should be granted, Google has put together an Advisory Council made up of members of its legal team, as well as individuals from the media, the legal community, government, and other sectors.[65] In the event that an individual's takedown request is denied by Google, which occurs a little more than half of the time for evaluated links,[66] the requesting individual is notified and can appeal the decision to her country's data protection agency.[67] If a search engine is found not to be fulfilling its duty to enforce the right to be forgotten, it can face a monetary sanction of up to €500,000, or, for an enterprise, one percent of its annual worldwide turnover.[68]

The right to be forgotten, while still in its infancy, could allow Internet users to erase speech connected with their cyberbullying experience. Allowing victims to detach themselves from insulting and harmful content through a takedown request could provide them with an opportunity to heal and to reclaim control of their online identities.[69] However, differences between the U.S. and E.U. legal systems, specifically on the issue of freedom of speech, might prevent the wholesale importation of the right to be forgotten into the United States.

B. The Right to be Forgotten, as Implemented in Europe, Would Face Serious First Amendment Challenges in the United States

The First Amendment states that "Congress shall make no law . . . abridging the freedom of speech."[70] While the language may seem to indicate otherwise, the right to free speech is not absolute.[71] Rather, the U.S. Supreme

---

"noting 'a fairly dramatic transatlantic schism in the law of privacy,' regarding right to be forgotten, and explaining cultural and historical sources of divergence.")).

64. John Walsh, *When It Comes to Facebook, EU Defends "Right to Disappear,"* CHRISTIAN SCI. MONITOR (Apr. 6, 2011), http://www.csmonitor.com/World/Europe/2011/0406/When-it-comes-to-Facebook-EU-defends-the-right-to-disappear [https://perma.cc/X2WR-FKQL].

65. GOOGLE ADVISORY COUNCIL, REPORT OF THE ADVISORY COUNCIL TO GOOGLE ON THE RIGHT TO BE FORGOTTEN (2015), https://www.google.com/advisorycouncil/ [https://perma.cc/65DH-EJJM].

66. *See* Google Transparency Report, *supra* note 61.

67. *See* Danny Sullivan, *How Google's New "Right to be Forgotten" Form Works: An Explainer*, SEARCH ENGINE LAND (May 30, 2014, 2:54 AM), http://searchengineland.com/google-right-to-be-forgotten-form-192837 [https://perma.cc/K6X6-6RGF]; Loek Essers, *Right to Be Forgotten "Dashboard" to Help EU's Data Protection Authorities*, PC WORLD (Sept. 18, 2014, 8:25 AM PT), http://www.pcworld.com/article/2685732/righttobeforgotten-dashboard-to-help-eus-data-protection-authorities.html [https://perma.cc/HMC6-LG9A].

68. Data Protection Regulation, *supra* note 59, at art. 79(5)(c).

69. *See* Ghoussoub, *supra* note 57.

70. U.S. CONST. amend. I.

71. *See* Gitlow v. New York, 268 U.S. 652, 666 (1925); *see also* John M. Beahn, *Recent Decision: Reno v. ACLU: The Communications Decency Act Hits a Red Light on the Information Superhighway*, 47 CATH. U.L. REV. 333, 333 (1997) ("Although the language of

Court has ruled that the federal and state governments have the power to restrict the exercise of free speech in certain limited circumstances.[72] Low-value speech—including "the lewd and obscene, the profane, the libelous, and the insulting or 'fighting' words"—can generally be restricted without violating the First Amendment.[73] But these categories of low-value speech are narrow.[74] If the government wishes to restrict the content of speech outside of these limited categories, the restriction must survive strict First Amendment scrutiny, meaning the restriction must be narrowly-tailored to achieve a compelling government interest.[75] The questions that must be answered, therefore, are: (1) what type of speech is cyberbullying, and (2) what level of scrutiny will be applied by a reviewing court.

1. Low-Value Speech Can Be Restricted by the Government with Minimal First Amendment Scrutiny

Low-value speech, which includes libel,[76] obscenity,[77] and fighting words,[78] does not receive heightened constitutional protection.[79] This is because low-value speech forms "no essential part of any exposition of ideas," and possesses "such slight social value as a step to truth that any benefit that may be derived from [its expression is] clearly outweighed by the social interest in order and morality."[80]

Some scholars consider fighting words, a limited category of low-value speech, to be the closest analog to cyberbullying.[81] Fighting words are words "which by their very utterance inflict injury or tend to incite an immediate breach of the peace."[82] This means that fighting words are limited to speech that has "a direct tendency to cause acts of violence by the person to whom . . . the remark is addressed."[83] As a result, words "conveying disgrace" or "harsh, insulting language" are not fighting words because, even though these words could have a debilitating effect on the subject in the long-run, these are not words "which by their very utterance . . . tend to incite an immediate

---

the First Amendment appears absolute, the Supreme Court has never held the First Amendment to confer an absolute right to free speech.").

72. *See, e.g.*, Chaplinsky v. New Hampshire, 315 U.S. 568, 571–72 (1972).

73. Roth v. United States, 354 U.S. 476, 483 (1957); Beauharnais v. Illinois, 343 U.S. 250, 266 (1952).

74. *See* Genevieve Lakier, *The Invention of Low-Value Speech*, 128 HARV. L. REV. 2166, 2173 (2015).

75. *See, e.g.*, R.A.V. v. St. Paul, 505 U.S. 377, 403 (1992).

76. N.Y. Times Co. v. Sullivan, 376 U.S. 254 (1964).

77. *See Roth*, 354 U.S. at 486.

78. *See* Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1972).

79. Lakier, *supra* note 74, at 2168.

80. *Chaplinsky*, 315 U.S. at 572.

81. *See, e.g.*, Katherine McCabe, *Founding Era Free Speech Theory: Applying Traditional Speech Protection to the Regulation of Anonymous Cyberspeech*, 24 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 823, 826 (2014) (stating that "cyberbullying is analogous to fighting words").

82. *Chaplinsky*, 315 U.S. at 571–72.

83. Gooding v. Wilson, 405 U.S. 518, 523 (1972).

breach of the peace."[84] Given the narrow definition of fighting words particularly the requirement of immediacy, it may be difficult to successfully argue that cyberbullying speech can be categorically restricted in the same way as fighting words.[85]

2. Restrictions on Speech That Is Not Low-Value Are Subject to Strict Scrutiny Under the First Amendment

The government is not limited only to restricting the content of speech that is low-value. Rather, the government can restrict the content of higher-value speech if the restriction survives strict First Amendment scrutiny.[86] Strict scrutiny means that the government can restrict the content of higher-value speech if the restriction is narrowly-tailored to achieve a compelling government interest.[87] This determination is an "ends and means" inquiry by which, "[t]he [c]ourt makes a normative judgment about the ends: Is the interest important enough to justify a speech restriction?"[88] The court will then make a judgment about the means: "[i]f the means do not actually further the interest, are too broad, are too narrow, or are unnecessarily burdensome, then the government can and should serve the end through a better-drafted law."[89] If both prongs of the test are met, then the restriction passes the strict scrutiny test and is upheld as constitutional.[90]

The Supreme Court has stressed that a compelling government interest is a rigorous standard to meet.[91] It includes "only those interests of the highest order."[92] One compelling government interest that has been recognized by the Court is the protection of "the physical and psychological well-being of minors."[93] This interest exists because "a democratic society rests, for its continuance, upon the healthy, well-rounded growth of young people into full maturity as citizens."[94] In order to protect this interest, the Court has upheld

84. *Id.* at 525 (quoting *Chapinksky*, 315 U.S. at 571–72).

85. Susan S. Bendlin, *Far from the Classroom, the Cafeteria, and the Playing Field: Why Should the School's Disciplinary Arm Reach Speech Made in a Student's Bedroom*, 48 WILLAMETTE L. REV. 195, 238 (2011) (stating that hostile language does not generally constitute fighting words and that it would be difficult to argue that fighting words constitute cyberbullying).

86. *See* Burson v. Freeman, 504 U.S. 191, 208–10 (1992) (upholding under strict scrutiny a content-based restriction on certain speech at polling places).

87. *See* R.A.V. v. St. Paul, 505 U.S. 377, 403 (1992) (J. White, concurring).

88. Eugene Volokh, *Freedom of Speech, Permissible Tailoring and Transcending Strict Scrutiny,* 144 U. PA. L. REV. 2417, 2418 (1996) (citing Sable Comm. v. FCC, 492 U.S. 115, 126 (1989)).

89. *Id.* at 2491.

90. *See Burson*, 504 U.S. at 208–10.

91. Derek L. Gaubatz, *RLUIPA at Four: Evaluating the Success and Constitutionality of RLUIPA's Prisoner Provisions*, 28 HARV. J.L. & PUB. POL'Y 501, 540 (2005).

92. *Id.* (citing Wisconsin v. Yoder, 406 U.S. 205, 215 (1972)).

93. *Sable Comm.*, 492 U.S. at 126 (citing Ginsberg v. New York, 390 U.S. 629, 639–40 (1968)).

94. Prince v. Massachusetts, 321 U.S. 158, 168 (1944).

legislation aimed at protecting the physical and emotional well-being of youth, even when such laws have affected the right to free speech.[95]

Courts striking down content-based speech restrictions, however, primarily rely on the narrowly-tailored prong of the strict scrutiny test rather than the compelling government interest prong.[96] Generally, four elements must be met to convince a reviewing court that a speech restriction is narrowly tailored.[97] First, the government must prove that the law advances the interest at issue.[98] If the government does not make a common-sense showing that the law will advance its interest, the restriction is not narrowly tailored.[99] Second, the law must not restrict "a significant amount of speech that does not implicate the government interest."[100] Third, the government must use the least restrictive means to address the interest at issue.[101] If there are less restrictive means available that would serve the government's interest just as well as the speech restriction, then the restriction is not narrowly tailored.[102] Finally, the law cannot "fail[] to restrict a significant amount of speech that harms the government interest to about the same degree as does the restricted speech."[103] Put differently, if there is a significant amount of speech that harms the government interest to a similar degree and manner, but is not regulated, then the restriction is not narrowly-tailored due to its under inclusiveness.[104] In sum, under this two-step strict scrutiny analysis, it is difficult to develop a law restricting the content of speech that is not considered low-value.

---

95. *See* New York v. Ferber, 458 U.S. 747, 757–64 (1982) (upholding constitutionality of New York statute that made it a criminal offense to knowingly promote a sexual performance by a child under the age of 16 by distributing material which depicted such a performance because the threat such material posed to children and its intrinsic relation to child sexual abuse outweighed any de minimis interest in protecting the speech); *see also* Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 513 (1969) (recognizing as part of the compelling government interest in the well-being of minors, the importance of maintaining order and discipline in schools which, therefore, justifies a speech restriction).

96. Volokh, *supra* note 88, at 2421.

97. *See id.* at 2421–23.

98. *Id.* at 2422 n.30 (citing Meyer v. Grant, 486 U.S. 414, 426 (1988); FEC v. Mass. Citizens for Life, Inc., 479 U.S. 238, 262 (1986); Globe Newspaper Co. v. Superior Court for Norfolk, 457 U.S. 596, 609–10 (1982); First Nat'l Bank v. Bellotti, 435 U.S. 765, 789–90 (1978); Buckley v. Valeo, 424 U.S. 1, 45–47, 53 (1976)).

99. *Id.* at 2422 n.31 (citing Burgson v. Freeman, 504 U.S. 191, 211 (1992) (stating that government can make simple common-sense argument to show law is narrowly-tailored); s*ee also* Williams-Yulee v. Florida Bar, 135 S. Ct. 1656, 1666 (2015) (holding that a restriction on judges personally soliciting campaign contributions complied with First Amendment because the restriction was narrowly-tailored to achieve the State's compelling concern of maintaining public confidence in the impartiality of the judiciary).

100. *Id.* at 2422 n.32 (citing Simon & Schuster, Inc. v. Members of the N.Y. State Crime Victims Bd., 502 U.S. 105, 120–21 (1991); FEC v. Nat'l Conservative Political Action Comm., 470 U.S. 480, 500-01 (1985); *First Nat'l Bank*, 435 U.S. at 794).

101. *Id*. at 2422.

102. *Id.* at 2422 n.33.

103. *Id.* at 2423 n.39.

104. *Id*.

C. Due to Its Chilling Effect on the Content of a Wide Range of Speech, the Right to Be Forgotten Is Not Likely to Survive Strict First Amendment Scrutiny in the United States

Assuming that a reviewing court determines that a right to be forgotten statute is broader than restricting low-value speech like libel, obscene speech and fighting words, the statute would likely have to survive strict First Amendment scrutiny by being deemed a narrowly-tailored restriction of speech designed to achieve a compelling government interest.[105] While some have made the argument that cyberbullying should be restricted like fighting words and receive lower First Amendment scrutiny,[106] most cyberbullying—although insulting and sometimes threatening—is not face-to-face in a way that it would tend to incite an immediate breach of the peace under traditional fighting words jurisprudence.[107] Therefore, a right to be forgotten statute on par with the E.U.'s recognized protection would likely have to survive the two-pronged strict-scrutiny test.

As previously discussed, cyberbullying has the potential to inflict devastating physical, psychological, and educational consequences on victims as well as perpetrators.[108] It is possible that a reviewing court would conclude that a right to be forgotten, implemented for the purpose of preventing cases of cyberbullying or mitigating their effects, would pass the compelling government interest prong of the analysis.

The overriding problem with the right to be forgotten, however, is that it is not a narrowly-tailored speech restriction designed to respond to the issue of cyberbullying. Due to the broad nature of the ECJ's ruling, countless individuals have been given the opportunity to petition Google and other search engines to remove links to webpages containing personal information.[109] Out of more than 630,000 takedown requests received by Google, approximately half have been granted, which has resulted in the blocking of access to a large amount of information contained on the Internet.[110]

Although Americans and Europeans may have varying expectations when it comes to privacy, no evidence suggests that Americans would be any less likely to avail themselves of a right to be forgotten. The chilling of speech could be substantial and result in the removal of speech that has little or nothing to do with cyberbullying. Therefore, application of the right to be forgotten—at least as implemented in the European Union—likely could not

105. *See* R.A.V. v. St. Paul, 505 U.S. 377, 403 (1992).

106. *See* McCabe, *supra* note 81, at 849.

107. *See* Gooding v. Wilson, 405 U.S. 518, 523 (1972) ("The test is what men of common intelligence would understand would be words likely to cause an average addressee to fight . . . . Derisive and annoying words can be taken as coming within the purview of the statute . . . only when they have this characteristic of plainly tending to excite the addressee to a breach of the peace.").

108. *See* Morben, *supra* note 33, at 694–95.

109. *See Google Transparency Report*, *supra* note 61.

110. *See id*.

be justified as a speech restriction that is narrowly-tailored to the interest of protecting minors from the harms of cyberbullying.

A mechanism that is more narrowly-tailored towards addressing the specific harm of cyberbullying content on the Internet likely stands a better chance at surviving strict scrutiny. Policymakers, however, do not have far to go to find a model for such a mechanism. There already exists a notice-and-takedown mechanism in the DMCA that, like the right to be forgotten, allows individuals to petition to have certain information removed from the Internet.[111] This mechanism, with appropriate protections and procedures put in place, could provide policymakers with a model to restrict the content of speech associated with cyberbullying without violating the First Amendment.

V. POLICYMAKERS SHOULD LOOK TO THE NOTICE-AND-TAKEDOWN PROCEDURES OF THE DIGITAL MILLENNIUM COPYRIGHT ACT, WHICH MAY PROVIDE A CONSTITUTIONAL MEANS FOR RESTRICTING THE CONTENT OF SPEECH

The notice-and-takedown procedures contained within the DMCA,[112] although in the context of copyright law, may provide policymakers with effective guidance on how to develop a takedown mechanism comparable to the right to be forgotten for the purpose of restricting the content of certain images and videos associated with cyberbullying. Rather than a broad speech restriction that happens to restrict cyberbullying speech, a notice-and-takedown mechanism would put the onus on targeting specific content, and the content would only be removed if it meets certain required elements. A speech restriction modeled after the notice-and-takedown procedures of the DMCA could thus provide policymakers with a tool to limit cyberbullying and its effects.

A. Background on the DMCA and Its Notice-and-Takedown Provisions

Congress enacted the DMCA to provide greater protection to copyright holders by allowing for the removal of material posted on the Internet that infringes upon their intellectual property rights.[113] The DMCA's notice-and-takedown procedures are contained in Title II of the statute, which discusses certain "safe harbors" for online service providers to avoid liability for unknowingly hosting infringing material.[114] These procedures require that a provider of online services, such as a website or a similar entity, expeditiously remove or disable access to material in its system upon receiving notice from the copyright holder or her agent that it is hosting copyright infringing

111. *See* 17 U.S.C. § 512(c)(1) (2012).
112. *Id*.
113. *See* Yamamoto, *supra* note 15, at 126–27.
114. *See* 17 U.S.C. § 512(c)(1), (3).

material.[115] Importantly, if the provider, upon receiving notice that it is hosting infringing material on its domain, moves expeditiously to remove or disable access to the infringing material, the provider is not liable for any monetary, injunctive, or equitable relief resulting from its hosting or removal of the material.[116]

Notice is given to the provider through the submission of a takedown notice.[117] The takedown notice must include:

(1) the signature of the copyright owner or someone authorized to act on the owner's behalf; (2) identification of the copyrighted work(s) claimed to have been infringed upon; (3) identification of the infringing material and information reasonably sufficient to permit the provider to locate the material; (4) the contact information of the infringing party; (5) a statement that it is the good faith belief of the complaining party that the use of the material at issue is not authorized by the copyright owner; and, (6) a statement that the information in the notification is accurate and that the complaining party is authorized to act on behalf of the copyright owner.[118]

If the notification does not include this information, the material at issue does not have to be removed by the provider.[119] If the complainant is found to have knowingly misrepresented the infringing nature of the material, that party is liable for damages and fees incurred by the copyright owner or the provider of online services who is injured due to relying on the misrepresentation when removing or disabling access to the material.[120]

The notice-and-takedown procedure does contain a reactive measure for subscribers of a service provider to submit a counter-notification, arguing that material was improperly removed and that access should be restored.[121] A counter-notification requires the same measure of accountability in order to assign liability for erroneous takedown requests.[122] Upon receiving this counter-notification, the provider must both promptly provide the person who filed the initial takedown notification with a copy of the counter-notification and restore access to the material identified in the counter-notification in no less than ten and in no more than fourteen business days.[123] If there are misrepresentations in the counter-notification, the party who submitted the counter-notification can be held liable for damages if such misrepresentations were knowingly made.[124] Additionally, the provider cannot be held liable for copyright infringement by complying with the provisions of a counter-notification.[125]

115. *Id.* § 512(c)(1)(C).
116. I*d.* § 512(c)(1), (g)(1).
117. *Id.* § 512(c)(3)(A).
118. *Id.*
119. *Id.* § 512(c)(3)(B).
120. *Id.* § 512(f).
121. *Id.* § 512(g)(2), (3).
122. *Id.* § 512(g)(2), (3).
123. *Id.* § 512(g)(2)(B)–(C).
124. *Id.* § 512(f)(2).
125. *Id.* § 512(g)(4).

B. The Argument That the DMCA's Notice-and-Takedown Procedures Provide for a Potentially Unconstitutional Restriction of Speech

Some have argued that the DMCA's notice-and-takedown regime is an unconstitutional infringement upon the right to free speech.[126] These critics assert that "if notices are sent when copyright infringement is alleged but unclear, or defective notices are the norm . . . [this notice-and-takedown regime] may represent a wolf in sheep's clothing, allowing information protected by the First Amendment to be removed from the Internet cheaply, expeditiously, and without check."[127] In fact, it has been asserted that as much as thirty percent of DMCA takedown notices are improper.[128] Additionally, a recent study concluded that out of more than twenty-five million allegedly infringing URLs over a six month period, including more than thirteen million URLs sent to site operators, only eight counter-notifications were received, thereby allowing for material to be removed from the Internet that potentially never should have been removed in the first place.[129] Finally, the fairness of the extrajudicial removal of information from websites has been called into question.[130] Critics argue that courts should be making the decision on whether to remove allegedly infringing material rather than copyright owners and providers of online services.[131]

These arguments are unconvincing. The DMCA's notice-and-takedown regime is constitutional because it reinforces the "constitutional directive to 'promote the [p]rogress' of knowledge and learning."[132] As Justice O'Connor famously said in *Harper & Row, Publishers, Inc. v. Nation Enterprises*, copyright is the "engine of free expression."[133] Copyright

126. *See* Kathleen Brennan Hicks, Note, *The Right to Say, "I Didn't Write That": Creating a Cause of Action to Combat False Attribution of Authorship on the Internet*, 22 J. INTELL. PROP. L. 375, 398 (2015) (citing Wendy Selzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, 24 HARV. J.L. & TECH. 171 (2010)).

127. *See id*.

128. *See* Hannibal Travis, *WIPO and the American Constitution: Thoughts on a New Treaty Relating to Actors and Musicians*, 16 VAND. J. ENT. & TECH. L. 45, 90 n.239 (2013) (citing Brief of Electronic Frontier Foundation as Amicus Curiae Supporting Defendant-Appellee and Urging Affirmance at 29, Sony BMG Music Entm't v. Tenenbaum, 660 F.3d 487 (1st Cir. 2011) (No. 10-1883) ("One 2006 study estimated that fully one-third of DMCA takedowns were improperly asserting infringement claims; indeed with media companies sending as many as 160,000 takedown notices at a time, it could hardly be otherwise."), https://www.eff.org/files/filenode/inresonybmgetal/EFFamicustenenbaum.pdf [https://perma.cc/5EWJ-TPVW].

129. *See* BRUCE BOYDEN, CTR. FOR THE PROT. OF INTELL. PROP., THE FAILURE OF THE DMCA NOTICE AND TAKEDOWN SYSTEM: A TWENTIETH CENTURY SOLUTION TO A TWENTY-FIRST CENTURY PROBLEM (2013), http://cpip.gmu.edu/wp-content/uploads/sites/31/2013/08/Bruce-Boyden-The-Failure-of-the-DMCA-Notice-and-Takedown-System1.pdf [https://perma.cc/2DN9-AJFE].

130. Hicks, *supra* note 126, at 398.

131. *See id*.

132. Brian Leary, Note, *Safe Harbor Startups: Liability Rulemaking Under the DMCA*, 87 N.Y.U. L. REV. 1135, 1164 (2012) (citing U.S. CONST. art I, § 8, cl. 8).

133. Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 558 (1985).

balances the holder's monopoly entitlement with the public's interest in the dissemination and distribution of information.[134] While free speech is restricted to a certain extent, society has an interest in promoting the dissemination of materials that add to scholarship, and, to incentivize the production of this material, the author is granted exclusive rights through copyright.[135] An individual with something significant to add to the collective knowledge is less likely to go through the effort of developing the material if she knows that she will not have any exclusive right to it.[136] Without new ideas and developments, the growth of a vibrant civil society is hindered by a lack of contributions to the expansion of public knowledge.[137] A similar argument should be true for protecting Internet users from cyberbullying, because greater privacy rights online, and a greater ability to manage one's online profile, promote "diversity of speech and behavior," and the "expression of eccentric individuality."[138]

VI. APPLICATION OF THE DMCA NOTICE-AND-TAKEDOWN MECHANISM AS AN ALTERNATIVE MODEL TO RESTRICT THE CONTENT OF CYBERBULLYING SPEECH

The DMCA's notice-and-takedown procedures could provide a model for implementing something similar to a right to be forgotten in the United States. The framework proposed in this Note, which is designed for the specific purpose of protecting minors from the harmful effects of cyberbullying, would allow minors, through their guardians or potentially through another adult, such as a teacher or other care provider, to request that online service providers remove specific online images or video content from their domains. As discussed in the following sections, this proposal is more likely to survive strict scrutiny than the European Union's right to be forgotten due to the compelling government interest in preventing cyberbullying and protecting minors from its harmful effects, combined with the fact that this mechanism only targets a narrow range of content and contains multiple layers of protection for free speech.

---

134. *Id*.

135. *See* David M. Morrison, *Bridgeport Redux: Digital Sampling and Audience Recoding*, 19 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 75, 76 (2008).

136. *See id*.

137. *See* Neil Weinstock Netanel, *Copyright and a Democratic Civil Society*, 106 YALE L.J. 283, 349–51 (1996) (stating that for citizens to participate in a rich cultural, social, and political life, they must have wide latitude to express and reformulate ideas embodied in copyrighted expression).

138. Daniel J. Solove, *The Virtues of Knowing Less: Justifying the Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 991 (2003) (quoting Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as an Object*, 52 STAN. L. REV. 1373, 1425–26 (2000)).

A. The Elements of This Proposed Notice-and-Takedown Mechanism

Under this proposed model, Congress would enact a law enabling minors, through their guardian, other adult caretaker, or even on their own, who are the subject(s) of online images or video content posted without their consent, to submit a takedown request to the applicable online service provider. If granted, the request would result in "erasing" the content from the service provider's domain. The notice-and-takedown request would contain multiple required elements, including:

1. The signature of the minor's guardian, other agent, or the minor herself who is seeking to have content taken down due to its association with cyberbullying;
2. Identification of the image or video that contains personally identifiable information on the subject (the minor) and was posted without the minor's consent;
3. A statement, citing specific evidence, on why it is the complaining party's good faith belief that the image or video at-issue was posted with the specific intent to torment, threaten, harass, humiliate, embarrass, or otherwise inflict significant emotional harm upon the subject; and
4. The contact information of the complaining party.[139]

If the takedown request contains all of these elements, the provider must remove the content in an "expeditious" manner.[140] If the provider does remove the material expeditiously, it is immune from any potential civil liability for previously hosting the material. Additionally, signing the request certifies that the request is being submitted in good faith. Similar to the DMCA, policymakers could introduce various sanctions against the complaining party—including damages to the posting party and/or costs and fees to the online service provider—if it is determined that a request is not submitted in good faith.

The next step in the proposed mechanism is to allow the party who originally posted the content at issue to submit a counter-notification seeking to have access to the content restored. For the counter-notification to be granted, it would have to contain:

1. The signature of the party who posted the image or video, or an agent or guardian if the poster is a minor;
2. Identification of the image or video at issue;
3. The party's contact information; and

---

139. *Cf.* 17 U.S.C. § 512(c)(1), (3) (2012) (the elements of the proposed notice-and-takedown test are derived from the notice-and-takedown elements of the DMCA).

140. *Cf. id*. § 512(c)(1)(C) (upon notification of the claimed infringement, the posting-party must expeditiously remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity).

4. A statement, in good faith, explaining why the content was not posted with the intent to torment, threaten, harass, humiliate, embarrass or otherwise target the complaining party.

Once the provider of online services receives the counter-notification, the provider must review the notification in order to determine whether it contains the required information. Once the provider determines that the counter-notification does contain the required information, the provider must expeditiously restore access to the material. If the provider does not restore access to the material, it opens itself to the potential for civil liability for its failure to repost.

B. Why This Mechanism Is a Constitutional Speech Restriction

The essential constitutional question is whether this mechanism is a narrowly-tailored speech restriction designed to achieve a compelling government interest.[141] In order to be narrowly-tailored, the proposed mechanism must advance the interest at issue, avoid restricting a significant amount of speech that does not implicate the government interest, be the least restrictive means to accomplish the interest at issue, and avoid the failure to restrict a significant amount of speech that harms the government's interest to about the same degree as does the restricted speech.[142] This section addresses these elements in turn.

First, this proposed notice-and-takedown mechanism could do a great deal to prevent cases of cyberbullying and mitigate their effects. While there are statutes currently in existence that seek to construct strong anti-bullying policies and punish individuals who engage in cyberbullying,[143] this mechanism is unique because it provides for a guaranteed right, across the Internet, to petition providers of online services to remove harmful and malicious content. When victims of cyberbullying, like Raza, grow up and attempt to move on from their past, current laws do not fully capture the reality that Internet content is virtually impossible to remove once it has been uploaded.[144] This mechanism will change that reality. Upon receiving the takedown request from the complaining party, the provider is *required* to remove the identified material unless it receives a valid counter-notification. By utilizing this proposed mechanism, victims of cyberbullying stand a chance to distance themselves from their cyberbullying experiences.

Second, this proposed mechanism avoids restricting a significant amount of speech unrelated to the interest in protecting minors from cyberbullying. By way of contrast, Europe's right to be forgotten law is more broadly construed to include restricting speech associated with cyberbullying, speech among adults (which receives greater First Amendment deference),

141. *See* Burson v. Freeman, 504 U.S. 191, 198 (1992).

142. *See* Volokh, *supra* note 88, at 2423.

143. *See, e.g.*, N.C. GEN. STAT. § 14-458.1 (2012); MASS. GEN. LAWS ch. 71, § 37O (2010).

144. *See* Fischer, *supra* note 11, at 258.

and speech that has nothing to do with cyberbullying.[145] By successfully submitting a notice-and-takedown request, the complaining party is identifying a specific online image or video and meeting multiple layers of protection designed to ensure that cyberbullying speech, rather than other forms of speech, is what is being restricted. Also, if non-cyberbullying speech is removed, the posting party can easily submit a counter-notification to have the content restored. If the counter-notification meets the required elements, access to the content must be restored or the provider opens itself to civil liability. This complementary provision would evince the government's intent to find the least restrictive means available for furthering its compelling interest.

Finally, this notice-and-takedown regime does not exclude a substantial amount of speech associated with cyberbullying. There would be a strong argument that the mechanism excluded speech (and is therefore under inclusive) if it had been limited just to low-value speech like fighting words. While fighting words could be considered cyberbullying, not all speech that constitutes cyberbullying counts as fighting words.[146] Cyberbullying includes harassing speech, tormenting speech, and embarrassing speech that is abusive, but not likely to result in an immediate breach of the peace.[147] This mechanism, by seeking to restrict expression beyond the narrow category of fighting words, encompasses much, if not all, of the speech that constitutes cyberbullying. It is unlikely that a substantial amount of cyberbullying speech will fall through the cracks. This proposed notice-and-takedown mechanism, when compared to the right to be forgotten, is in greater alliance with the First Amendment and can provide victims of cyberbullying with a unique remedy unlike anything currently in force today.

While the mission to protect privacy is a noble one, a European-style right to be forgotten poses a threat to a vibrant civil society by restricting too much speech.[148] Search engines have had to put together large legal teams in order to respond to the flood of takedown requests;[149] and, in theory, anything

145. *Interview / Peter Fleischer: Google Performs Balancing Act Over the Right to be Forgotten*, ASAHI SHIMBUN (Aug. 24, 2016, 5:05 JST), http://www.asahi.com/ajw/articles/AJ201608240005.html [https://perma.cc/HX42-37NB] (discussing popular takedown requests received by Google, including requests from doctors and dentists seeking to have information related to past malpractice convictions removed, businesses seeking to remove information related to past fraud accusations, an art seeking to remove information related to a past conviction for forgery, and government officials seeking to have information related to past political views removed when their views have changed).

146. *See* Evie Blad, *Free Speech at Issue in New York Cyberbullying Case*, ED. WEEK: BLOG (June 17, 2014, 4:10 PM), http://blogs.edweek.org/edweek/rulesforengagement/2014/06/free_speech_at_issue_in_new_york_cyberbullying_case.html [https://perma.cc/EBC4-NBD7].

147. Jacqueline D. Lipton, *Combating Cyber-Victimization*, 26 Berkeley Tech. L.J. 1103, 1109 (2011).

148. *See* WERRO, *supra* note 63.

149. *See* GOOGLE ADVISORY COUNCIL, *supra* note 65.

that is posted online, at the point that it becomes no longer relevant, could be removed.[150]

In contrast, the proposed notice-and-takedown mechanism both actively seeks to restrict cyberbullying speech, but also contains institutional mechanisms to protect speech essential for public knowledge, a vibrant culture, and political engagement. Furthermore, this notice-and-takedown mechanism is going to reduce the burden on providers of online services. By restricting the content of online images and videos, rather than all online speech, there is not likely to be a flood of takedown requests as was the case in the weeks and months after the right to be forgotten was approved.[151] A significant showing is required to have online content removed under this notice-and-takedown mechanism and the need for a large team of lawyers to analyze takedown requests would be minimized.

C. Potential Counterarguments and the Need for Further Scholarship

There are potential counter-arguments, however, against the mechanism proposed in this note that should be addressed. These arguments include: (1) the fact that most websites already have policies in place within their terms of use designed to address cases of cyberbullying on their platforms and (2) the need for a robust appeals process.

1. Websites Already Have Protections in Place

In response to some high-profile cases of cyberbullying, many websites have made the decision to develop their own notice-and-takedown mechanisms to allow users to request that certain content be removed from their platforms.[152] Some may argue that, as a result, the notice-and-takedown mechanism proposed by this Note is unnecessary. Websites are dealing with cyberbullying on their own through their terms of use policies and it is unnecessary to add another level of bureaucracy.[153]

Leaving the response to cyberbullying in the hands of the private sector, however, is a flawed solution. While these terms of use do exist, having a federal mechanism to set a uniform policy across the board for providers of online services, and to potentially hold them liable for not complying, is very important. An example of why this is the case can be found in the case of Rebecca Ann Sedwick, a young woman who committed suicide after being tormented by embarrassing images and messages on ASKfm.[154] While

150. *See* C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, paras. 92–94 (May 13, 2014), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 [https://perma.cc/ZBL3-6H7L].

151. *See* GOOGLE ADVISORY COUNCIL, *supra* note 65.

152. *See* Tijana Milosevic, *Social Media Companies' Cyberbullying Policies*, 10 INT'L. J. COMMC'N 5164, 5165 (2016).

153. *Id.* at 5174.

154. *See Rebecca Ann Sedwick, 12 Year Old Florida Girl, Commits Suicide After Online Bullying*, HUFFINGTON POST (Sept. 12, 2013),

ASKfm does have an anti-harassment policy in its terms of use, several suicides have nonetheless been linked to cyberbullying on the online application.[155] ASKfm's terms of use simply were not strong or effective enough to protect Rebecca,[156] and the bullying she experienced on the platform directly contributed to her death.[157]

The solution proposed here is necessary, even with many websites having terms of use in place, because the health and wellbeing of some of this country's most vulnerable citizens should not be left in the hands of for-profit websites. Cyberbullying is a public issue that should be addressed by public authorities as it not only affects victims while they are young, but it can affect a victim well into adulthood.[158] Like what occurred with Rebecca, cyberbullying can ruin an innocent victim's life. It has been recognized as a growing public health problem,[159] and, because of the continued growth of the Internet, the problem is not going to go away anytime soon. The reality is that the lives of young people are at stake and it is society's solemn duty to protect them. In fact, by protecting providers from civil liability if they expeditiously comply with takedown requests, providers are incentivized to take cyberbullying more seriously and to be a part of the solution. Finally, rather than being at the mercy of an individual website's terms of service, this mechanism provides much needed uniformity across the Internet—something that is sorely lacking today. Terms of use, by themselves, are not an adequate solution for remedying the harm associated with cyberbullying.

2. The Need for an Appeals Process

A second foreseeable counterargument is that this mechanism requires a meaningful appeals process beyond the notification and counter-notification process. In Europe, where Google has rejected removal requests for almost one-million web links, an appeals process has been put in place to ensure that all takedown requests are properly considered.[160] This notice-and-takedown mechanism should have a comparable appeals process to provide the same protection.

---

http://www.huffingtonpost.com/2013/09/12/rebecca-ann-sedwick-bulli_n_3915883.html [https://perma.cc/QW76-8DZZ].

155. *See* Jessica Guynn & Janet Stobart, *Ask.fm, New Social Site, Same Bullying*, L.A. TIMES (Aug. 20, 2013), http://articles.latimes.com/2013/aug/20/business/la-fi-britain-cyber-bullying-20130820 [https://perma.cc/32R6-3ZNM].

156. *See Terms of Use*, ASKFM (last visited Feb. 11, 2017), http://about.ask.fm/legal/en/terms.html [https://perma.cc/U85A-EJVA] (ASKfm's terms of use provide that "we reserve the right, at any time and without prior notice, to remove or disable access to any content that we, for any reason or no reason, consider to be objectionable, in violation of the TOU or otherwise harmful to the Services or our users").

157. *See The Story of Rebecca Ann Sedwick*, NOBULLYING.COM (last modified Aug. 6, 2015), https://nobullying.com/rebecca-ann-sedwick/ [https://perma.cc/4JVJ-KFMW].

158. Morben, *supra* note 33, at 695.

159. King, *supra* note 27, at 849.

160. *See* Natasha Lomas, *Europe Seeks a Common Appeals Process for the "Right to be Forgotten,"* TECHCRUNCH (Sept. 19, 2014), https://techcrunch.com/2014/09/19/rtbf-appeals-guidelines/ [https://perma.cc/UW4P-KUJ7].

Additionally, an appeals process is important to prevent abuse on both sides of the equation. Not only could it be possible for an individual to submit a counter-notification to ensure that a victim continues to be tormented online, but an alleged victim may submit a notice-and-takedown request to have an image or video removed just because he does not like what it depicts. It should not be the job of Google or Facebook to adjudicate these disputes. Also, if a complaining party may be fined for submitting a notice-and-takedown request in bad faith, some appeals process is necessary to ensure that the fine is paid.

However, the answer to the question of what this appeals process should look like is unclear. One potential solution could be to allow the original complaining party to make a further showing, by clear and convincing evidence to a third-party adjudicator, that the content was posted with the intent to "torment, threaten, harass, humiliate, embarrass, or otherwise inflict significant emotional harm upon the subject."[161] If this showing is successfully made, then the adjudicator could order the material to be removed. For example, the adjudicator could be an administrative law judge at the Federal Communications Commission (FCC) due to the agency's expertise, independence, and its recent decision to regulate the Internet under Title II of the Communications Act.[162]

The complaining party could also potentially have access to a remedy in court. If Congress was to write a statute containing the proposed notice-and-takedown procedure, the complaining party could sue the posting party directly, thereby allowing the website hosting the content to get out from the middle of the dispute after fulfilling its initial responsibilities in the notice and counter-notice phase. In court, the complaining party would have to make a showing by clear and convincing evidence that the content was posted with the requisite intent. Upon making the required showing, the court would be able to issue an order requiring that the content at issue be removed within a specified period of time. To reach the point of ultimately having content taken down from the Internet, the complaining party must communicate a significant amount of evidence to the court to show why the speech constitutes cyberbullying. The posting party, of course, will have an opportunity in court to show why the speech at-issue is not cyberbullying. As a result, it is possible that an appeals process will result in many takedown requests ultimately being denied due to the built-in mechanisms designed to protect free speech. The ultimate question of exactly how to develop this appeals process remains open for future scholarship.

VII. CONCLUSION

Cyberbullying is a serious public health problem in the United States that deserves the utmost attention from policymakers, the media, and the public. While the Internet has brought society many benefits, the growth of cyberbullying has been an unintended consequence. Cyberbullying has led to

161 *See* 17 U.S.C. § 512(c)(1), (3) (2012).

162. *See* Protecting and Promoting the Open Internet, *Report and Order*, 30 FCC Rcd 5601 (2015).

devastating physical and psychological harm for victims, the majority of whom are minors. As society comes to grips with the problem of cyberbullying and seeks to address the problem in future years, this Note provides an innovative notice-and-takedown mechanism modeled after the DMCA, to address cyberbullying on a national level. In contrast to past efforts, this proposed mechanism goes directly after the source of the harm—the online content itself. A notice-and-takedown mechanism where cyberbullying speech can be removed from the Internet would provide victims with a meaningful opportunity to move on with their lives. This is the least we can do for some of the most vulnerable members of our society.

Freedom of Speech, The War on Terror, and What's YouTube Got to Do with it: American Censorship During Times of Military Conflict

Melissa J. Morgans *

TABLE OF CONTENTS

* J.D., The George Washington University Law School, May 2017. Senior Articles Editor, *Federal Communications Law Journal*, 2016–17. B.A., History and American Studies, The University of Virginia, 2014. The author would like to extend her gratitude to everyone who helped in the drafting and editing of this Note. She would like to dedicate this Note to her grandfather, Dave Morgans, who gave her the invaluable gift of education.

> Our liberty depends on the freedom of the press and that cannot be limited without being lost.[1]
>
> —Thomas Jefferson.

I. INTRODUCTION

On August 19, 2014, the extremist group, Islamic State of Iraq and Syria (ISIS), uploaded the beheading of American journalist James Foley on YouTube captioned as, "A Message to America."[2] The "Message" spread to other social media sites, including Twitter and Instagram, within minutes.[3] *New York Times* writer Hanna Kozlowska called the video a "modern guillotine execution spectacle."[4] Following the upload, a user-based movement, #ISISMediaBlackout, swelled in an attempt to stop the circulation of the video.[5] Instead of uploading the video or screenshots from the video onto social media platforms, users were encouraged to post the #ISISMediaBlackout hashtag along with photographs of Foley.[6] Foley's sister, Kelly Foley, tweeted in response to the video: "Please honor James Foley and respect my family's privacy. Don't watch the video. Don't share it. That's not how life should be."[7] On August 20, 2014, YouTube and Twitter removed the gruesome video citing their corporate take-down policies.[8]

---

1. Letter from Thomas Jefferson to James Currie (Jan. 28, 1786), *reprinted in* THE PAPERS OF THOMAS JEFFERSON 239, 239 (Julian P. Boyd ed., 1954), *in Developments in the Law: The Law of Media*, 120 HARV. L. REV 990, 990 (2007).

2. *See* Walter Reich, *Show the James Foley Beheading Video: A Lesson Drawn from the Holocaust*, WASH. POST (Aug. 29, 2014), https://www.washingtonpost.com/posteverything/wp/2014/08/29/why-facebook-and-youtube-should-show-the-james-foley-beheading-video/ [https://perma.cc/VC73-NDYD].

3. *See* James Foley, *How Social Media is Fighting Back Against ISIS Propaganda*, THE GUARDIAN (Aug. 20, 2014, 11:06 EDT), https://www.theguardian.com/technology/2014/aug/20/james-foley-how-social-media-is-fighting-back-against-isis-propaganda [https://perma.cc/75XW-4382].

4. Hanna Kozlowska, *Should We Be Seeing Gruesome Acts? And If So, Where*?, N.Y. TIMES: BLOG (Aug. 25, 2014, 5:30 AM), http://op-talk.blogs.nytimes.com/2014/08/25/should-we-be-seeing-gruesome-acts-and-if-so-where/ [https://perma.cc/9KAW-RXGU].

5. *See* #isismediablackout, TWITTER (Aug. 19, 2014), https://twitter.com/hashtag/isismediablackout [https://perma.cc/F2LX-SRZY].

6. *See, e.g.*, Tahar (@laseptiemewilay), TWITTER (Aug. 19, 2014, 4:35 PM), https://twitter.com/laseptiemewilay/status/501875153006231553 [https://perma.cc/YFB2-EYRY].

7. Hannah Jane Parkinson, *James Foley: How Social Media is Fighting Back Against ISIS Propaganda*, THE GUARDIAN (Aug. 20, 2014), http://www.theguardian.com/technology/2014/aug/20/james-foley-how-social-media-is-fighting-back-against-isis-propaganda [https://perma.cc/L9W5-9VMU].

8. *See* E.W., *Twitter, Terror and Free Speech: Should Twitter Block Islamic Snuff Videos?*, THE ECONOMIST:BLOG (Aug. 21, 2014, 11:17 AM), http://www.economist.com/blogs/democracyinamerica/2014/08/twitter-terror-and-free-speech [https://perma.cc/62GK-W3UN].

The posting and subsequent removal of Foley's video implicates the age-old First Amendment debate on the scope of freedom of speech. To Thomas Jefferson, and those like him, freedom of speech was a uncompromising and universal democratic right.[9] It remains one of the greatest hallmarks of the Bill of Rights.[10] However, during times of war, military conflict, or prolonged hostilities, civil liberties, such as freedom of speech, rival the need for order and authority.[11] Fear of military defeat scales the balance towards order, resulting in the restriction of an individual's right to freedom of speech.[12] Today, this historical tension is further complicated by modern forms of media, and begs the question whether videos like the one posted about Foley should be considered censorable by the government or constitutionally protected free speech.[13]

This Note addresses the current wartime speech issue: terrorist speech on the Internet. First, Part II evaluates the historical practice of wartime censorship, tracing wartime censorship to two root causes: active anti-government speech and uniquely intrusive visual mediums. Second, Part II then analyzes the United States Supreme Court's reaction to restrictions on free speech, looking at its strict scrutiny test and the separate doctrine of incitement. Part III analyzes how this historical practice of censorship during times of war justifies a government-based censorship initiative of terrorist speech on the Internet.

Part IV proposes and analyzes a potential Act, Stop Terrorist Organizations from Promoting Internet Transmissions (STOP IT,) that would regulate terrorist speech on the Internet. The proposal in Part IV will address whether the Federal Communications Commission (FCC) could serve as an appropriate regulator of terrorist speech, assuming congressional support. It concludes by suggesting that the historical pattern of wartime censorship is unlikely to change, and that legislation empowering the FCC power to regulate certain forms of terrorist speech on the Internet would be a step in the right direction of matching the historical practice of censorship with the legal doctrine of free speech. If "STOP IT" were to fail constitutional scrutiny, an alternative tactic could involve developing a uniform "Code of Ethics" for all major social media sites that could be implemented on a voluntary basis to curb the influence of terrorist speech.

---

9. *See* Letter from Thomas Jefferson to James Currie, *supra* note 1, at 239.

10. *See* GEOFFREY R. STONE, PERILOUS TIMES: FREE SPEECH IN WARTIME: FROM THE SEDITION ACT OF 1789 TO THE WAR ON TERRORISM 5–7, 14 (2004).

11. *See generally* WILLIAM H. REHNQUIST, ALL THE LAWS BUT ONE: CIVIL LIBERTIES DURING WARTIME 218 (1998).

12. *See* DANIEL HALLIN, THE UNCENSORED WAR: THE MEDIA AND VIETNAM 215 (1986) (asserting that "[e]very society must maintain a balance between democracy and authority").

13. *See generally* Tom Hentoff, *Speech, Harm, and Self-Government: Understanding the Ambit of the Clear and Present Danger Test*, 91 COLUM. L. REV. 1453, 1462 (1991).

II. BACKGROUND

The Internet is the new frontier for First Amendment expression.[14] News can "go viral," and be viewed by millions of people within hours.[15] This fast-paced, ubiquitous medium is now being used by terrorist groups to solicit members and inflict fear by sharing extremely violent videos.[16] In response to this trend, theorists have responded by testing ideas that either over or under regulate Internet speech.[17]

A. There is a Growing Issue of Terrorist Speech on the Internet Due to the Viral Nature Internet-Based Speech.

Terrorist groups use the Internet to spread their messages quickly to large audiences by posting content that "goes viral,"[18] which results in videos, comments, and all types of expression appearing on peoples' computer screens within minutes.[19] When a video goes viral, as a consequence of social network structures and "word of mouth pressure,"[20] Internet users view the material involuntarily through a whirlwind of headlines, video clips, and articles circulating on Facebook, on Twitter, through e-mail, on web browsers, and more.[21] This phenomenon of fast-paced viral media has led to terrorist organizations actively recruiting and spreading videos of violence, like Foley's video, through mass media Internet sources.[22] In 2012, Al-Qaeda used Internet forums, such as the forum Shumukh al-Islam, to recruit people willing and able to perform terrorist attacks.[23] In 2014, ISIS managed to recruit over 6000 new members over the Internet in just one month.[24] ISIS, in

14. *See Developments in the Law: The Law of Media*, 120 HARV. L. REV. 990, 996–97 (2007).

15. *See* Iris Mohr, *Going Viral: An Analysis of YouTube Videos*, 8 J. MARKETING DEV. & COMPETITIVENESS 43, 43–44 (2014) (comparing news media to an "infectious disease").

16. *See* Hannah Jane Parkinson, *James Foley: How Social Media is Fighting Back Against ISIS Propaganda*, THE GUARDIAN (Aug. 20, 2014), http://www.theguardian.com/technology/2014/aug/20/james-foley-how-social-media-is-fighting-back-against-isis-propaganda [perma.cc/JLQ3-HMHQ].

17. *See* Peter Margulies, *The Clear and Present Internet: Terrorism, Cyberspace, and the First Amendment*, 4 UCLA J.L. & TECH 1, 1–5 (2004).

18. *See* Ryan Reilly, *If You're Trying to Join ISIS Through Twitter, The FBI Probably Knows About It*, HUFFINGTON POST (July 9, 2015, 3:32 PM), http://www.huffingtonpost.com/2015/07/09/isis-twitter-fbi-islamic-state_n_7763992.html [https://perma.cc/ZQ9L-9SU7].

19. *See* Morh, *supra* note 15.

20. *Id.* at 44.

21. *See id*. at 43.

22. *See FBI Issues Warning: ISIS Using Social Media to Recruit Young Americans*, CBS DC (Mar. 6, 2015, 11:35 AM), http://washington.cbslocal.com/2015/03/06/fbi-issues-warning-isis-using-social-media-to-recruit-young-americans/ [https://perma.cc/AF5A-DL8Z].

23. *See* Diana Secara, *The Role of Social Networks in the Work of Terrorist Groups, The Case of ISIS and Al-Qaeda*, 3 RES. & SCIENCE TODAY 77, 81–82 (2015).

24. *See* Christopher J. Bolan, *Commentaries & Replies: On "Priming Strategic Communications: Countering the Appeal of ISIS*," 44 PARAMETERS 141, 141 (2014).

particular, as acknowledged by former FBI Director James Comey, is "very effective in using Twitter and other social media to communicate with potential recruits and spread its message online."[25] In response to ISIS's campaign, the United Kingdom (UK) has responded with an Internet-based anti-terrorism initiative to report online terrorist communications.[26]

The UK's Counter Terrorism Internet Referral Unit uses URL blocking to block website content that is deemed censorable by the current terrorist-based regulation: content that incites or glorifies terrorist actions.[27] Examples of content that satisfy this standard are: "articles, images, speeches or videos that promote terrorism; content encouraging people to commit acts of terrorism; websites made by terrorist organizations; and videos of terrorist attacks."[28] These types of expression are deemed censorable because of their "extraordinary" effect on the public.[29] First, videos of terrorist attacks are easily and quickly sent around the Internet to glorify acts of violence.[30] Studies demonstrate that exposure to violence through mass media significantly increases aggressive behavior of adults and children.[31] Second, websites made by terrorist organizations and videos that promote terrorism have the real effect of glorifying acts of terror as well as recruiting members to their cause.[32]

Both the issues of violent videos and terrorist recruitment have been addressed by social media websites themselves.[33] Individual websites employ

---

25. Ryan Reilly, *If You're Trying to Join ISIS Through Twitter, The FBI Probably Knows About It*, HUFFINGTON POST (July 9, 2015), http://www.huffingtonpost.com/2015/07/09/isis-twitter-fbi-islamic-state_n_7763992.html [https://perma.cc/4S5F-94T5]. In order to combat information spreading on the Internet through censorship, the goals of openness, accountability, transparency, and narrowness are valuable. *See* Derek E. Bambauer, *Cybersieves*, 149 BOOKLYN L. SCH. LEGAL STUD. RES. PAPERS 1, 13–25 (2009).

26. *See Tackling Extremism in the UK*: *Report from the Prime Minister's Task Force on Tackling Radicalization and Extremism*, H.M. GOVERNMENT 1, 1 (2013); *Report Online Terrorist Material*: *Reporting Crimes and Getting Compensation*, UK GOV., https://www.gov.uk/report-terrorism (last updated Sept. 23, 2016) [https://perma.cc/3RTV-9BZL.

27. *See Report Online Terrorist Material*: *Reporting Crimes and Getting Compensation*, UK GOV., https://www.gov.uk/report-terrorism (last updated Sept. 23, 2016) [https://perma.cc/3RTV-9BZL].

28. *Id*.

29. Ryan Reilly, *If You're Trying to Join ISIS Through Twitter, The FBI Probably Knows About It*, HUFFINGTON POST (July 9, 2015), http://www.huffingtonpost.com/2015/07/09/isis-twitter-fbi-islamic-state_n_7763992.html [https://perma.cc/7DWY-U93S].

30. *See id*.

31. *See* L. Rowell Huesmann, *The Impact of Electronic Media Violence: Scientific Theory and Research*, 41 J. ADOLESCENT HEALTH, S1, S7 (2007).

32. *Compare Who Are Britain's Jihadists?*, BBC NEWS (Oct. 10, 2016), http://www.bbc.com/news/uk-32026985 [https://perma.cc/9Y4F-ZGKS], *with* Simone Molin Friis, '*Beyond anything we have ever seen:' beheading videos and the visibility of violence in the war against ISIS*, 91 INT. AFF. 725, 737–38 (2015) (commenting on the UK's reaction to ISIL videos and Prime Minister David Cameron's "redoubling all efforts" against terrorist media).

33. *See Help Center: The Twitter Rules: Abusive Behavior Policy*, TWITTER, https://support.twitter.com/articles/20169997 [https://perma.cc/K5E8-M7S2].

their own take-down policies to regulate forms of expression on their websites.[34] YouTube's "Don't Cross the Line Policy," Facebook's "Reporting Abuse Policy," and Twitter's "Abusive Behavior Policy" are examples of corporate policies that are regularly enforced to take down user content.[35] Facebook receives thousands of government requests to take down material.[36] Facebook publishes the number of government requests worldwide it receives on a semi-annual basis,[37] with government data requests "to restrict or pull content" climbing by eleven percent in their 2015 report.[38] Twitter recently announced that since the middle of 2015 over 125,000 accounts have been suspended due to promoting terrorism or extremist activities.[39] The company posted: "As the nature of the terrorist threat has changed, so has our ongoing work in this area."[40] In other words, the threat of terrorist speech to the Internet is real.

B. The United States Government Has Historically Censored Speech During Times of War.

The United States is a nation founded upon freedom of speech and press, yet it is also a nation that has consistently restricted these rights.[41] During times of war, freedom of speech has been restricted through acts of federal authority, by the media, from citizens to other citizens, and even by self-censorship.[42] These forms of censorship have created a traceable historical practice of restricting certain types of speech during war: the furthering of perceived anti-government or anti-American ideas, and the visual indications of the woes of war—gruesome photographs of American war dead.

---

34. *See, e.g.*, *id.*

35. *Id.*; *see also Community Guidelines*, YOUTUBE, http://www.youtube.com/yt/policyandsafety/communityguidelines.html (last visited Mar. 31, 2017) [https://perma.cc/R3D4-7P92]; *Reporting Abuse*, Facebook, https://www.facebook.com/help/1417189725200547/ [https://perma.cc/3X5Z-HTM5].

36. *See* Parmy Olson, *Facebook: Government Data Requests Still Climbing*, FORBES (Mar. 16, 2015), http://www.forbes.com/sites/parmyolson/2015/03/16/facebook-government-data-requests-still-climbing/ [https://perma.cc/PG54-AU4A].

37. *See United States Law Enforcement Requests for Data, Jan. 2015- June 2015*, FACEBOOK, https://govtrequests.facebook.com/country/United%20States/2015-H1/# [https://perma.cc/G39Y-UC6W].

38. *See* Parmy Olson, *Facebook: Government Data Requests Still Climbing*, FORBES (Mar. 16, 2015), http://www.forbes.com/sites/parmyolson/2015/03/16/facebook-government-data-requests-still-climbing/ [https://perma.cc/QD5Q-HMF9].

39. *See* Karl Stephan, *Twitter & Terrorism*, PDD (Feb. 9, 2016), http://www.pddnet.com/blog/2016/02/twitter-terrorism [https://perma.cc/Y77X-MWCB].

40. Twitter (@Twitter), *Combating Violent Extremism*, TWITTER (Feb. 5, 2015), https://blog.twitter.com/2016/combating-violent-extremism [https://perma.cc/EW5Y-ZKVQ].

41. *See* STONE, *supra* note 10, at 5.

42. *See id.* at 5, 12.

Media censorship has existed from the birth of the United States.[43] During the Revolutionary War, Patriots stole "Loyalist" and British newspapers such as the *New Hampshire Gazette* and *New York Packet*, while continuing the delivery of Patriot newspapers.[44] Fifteen years after the end of the Revolutionary War, the Sedition Act of 1798 was enacted to criminalize statements that were critical of the federal government.[45]

During the Civil War, the federal government imposed various measures to censor Confederate viewpoints and gruesome images of the exhausting four-year conflict.[46] United States Marshals seized Confederate and pro-Southern newspapers regularly.[47] President Abraham Lincoln ordered the "seiz[ure] of telegraph lines in the North."[48] Sketches of Civil War artists were "toned down," such as Alfred Waud's sketches at the Battle of Antietam for bringing explicit images from the war to the home,[49] and editors of newspapers were arrested for the publications they issued.[50]

In World War I, wartime communications and photographs of Americans who died in the war continued to be censored.[51] During the first nineteen months of American involvement in World War I the federal government disallowed publication of all photographs of American war dead.[52] Press that followed American troops into the trenches of Europe, if given access to that front, were taken on specific tours or paired with an American serviceman at all times.[53] The Espionage Act of 1917 criminalized the intent to interfere, or actual interference, with operations of the United States Armed Forces and promoting the success of American enemies.[54] The Sedition Act of 1918, repealed two years later, extended the range of the Espionage Act by criminalizing "disloyal, profane, scurrilous, or abusive language" in relation to the United States government and troops.[55] As current events newsreels rose in popularity, members of the judiciary, such as Judge

43. *See* MICHAEL LINFIELD, FREEDOM UNDER FIRE: U.S. CIVIL LIBERTIES IN TIMES OF WAR 15–16 (1990).

44. *Id*.

45. *Id.* at 16–17; Sedition Act of 1798, 50 U.S.C. §§ 21–24 (1798) (This Act was later repealed by President Thomas Jefferson).

46. *Compare* JOHN COOKE, REPORTING THE WAR 49, 49 (2007), *with* GEORGE H. ROEDER, JR., THE CENSORED WAR 29, 8 (1993).

47. COOKE, *supra* note 46, at 49–50.

48. MARY S. MANDER, PEN AND SWORD: AMERICAN WAR CORRESPONDENTS, 1898–1975, at 24 (2010).

49. *See* ROEDER, *supra* note 46, at 29.

50. *See* MANDER, *supra* note 50, at 24; *see also* Menahem Blondheim, *"Public Sentiment Is Everything": The Union's Public Communications Strategy and the Bogus Proclamation of 1864*, 89 J. AM. HIST. 869, 877 (2002).

51. *See* ROEDER, *supra* note 46, at 8. *see also* MANDER, *supra* note 50, at 46–49.

52. *See id.* (a result of the Committee of Public Information which controlled information that entered to and from the country).

53. *See* MANDER, *supra* note 50, at 42.

54. *See* Espionage Act of 1917, 18 U.S.C. § 792 (2012).

55. *See* Sedition Act of 1918, Pub. L. 65–150, 40 Stat. 553 (1918) (repealed 1920).

Hinman in New York, began to distinguish between censorship of film versus censorship of print because the impact of film far outweighed print media.[56]

In World War II, censorship of photographs, letters, and press coverage of the war increased significantly and became more strategic.[57] The Office of Censorship issued wartime practices to keep the press's access and content in check.[58] These voluntary guidelines requested that stateside press preserve the confidentiality of soldier "locations, strength, and destination[s]."[59] Other guidelines issued by the Supreme Headquarters, Allied Expeditionary Force (SHAEF) prohibited the release of photographs showing men in poor mental health or showcasing the "horrific nature" of the war.[60] Private letters sent home from those serving in the Navy were censored and "all news from the Southeast Pacific had to pass through General Douglas MacArthur's headquarters."[61]

During the Cold War, restrictions on press publications, and particularly visual forms of media, increased.[62] The Smith Act of 1940 and Communist Control Act of 1954 criminalized advocacy of "overthrowing" the United States government.[63] Television proliferated in the years following World War II.[64] American homes went from having 3.6 million television sets between 1941–49 to 67.1 million sets sold to date in 1959.[65] Despite this expanding media landscape, journalists did not report on the bombings of Cambodia or meetings between Henry Kissinger and Le Duc Tho.[66] Reporters had to sign government contracts as the Saigon Press Corps or receive Military Assistance Command, Vietnam (MACV) accreditation in order to report in Vietnam and travel with military units.[67]

After the Cold War, strict regulations for wartime correspondents continued, as did television media self-censorship.[68] During the Gulf War, CNN journalist Peter Arnett reported on the Iraqi government from Baghdad, "one of the few Western journalists" to do so, leading critics in the United

56. *See* ROEDER, *supra* note 46, at 17 (citing Pathe Exch., Inc. v. Cobb, 202 App. Div. 450, 456 (N.Y. App. Div. 1922) ("But the moving picture attracts the attention so lacking with books or even newspapers, particularly so far as children and the illiterate are concerned, and carries its own interpretation.").

57. *See* MANDER, *supra* note 50, at 55; *See also* ROEDER, *supra* note 46, at 15–16.

58. *See* MANDER, *supra* note 50, at 58.

59. *Id.*

60. ROEDER, *supra* note 46, at 16.

61. MANDER, *supra* note 50, at 61–62.

62. *Compare* HALLIN, *supra* note 12, at 106–09 *with* NANCY E. BERNHARD, U.S. TELEVISION NEWS & COLD WAR PROPAGANDA, 1947–60, at 47 (1999).

63. *See* Smith Act of 1940, 18 U.S.C. § 2385; Communist Control Act of 1954 §§ 841–844 (2012).

64. *See* BERNHARD, *supra* note 62, at 47.

65. *See id.*

66. *See* HALLIN, *supra* note 12, at 211–12.

67. *See* MANDER, *supra* note 50, at 66–67.

68. *See generally* COL. JAMES P. TERRY, THE WAR ON TERROR: THE LEGAL DIMENSION 178 (2013).

States to nickname CNN, "Saddam Network News."[69] Both Operations Enduring Freedom and Operation Iraqi Freedom had "embedded and unilateral journalists."[70] Embedded journalists received access to everything the unit they were with received, but little access to anything else, while unilateral journalists were able to question Iraqi citizens and get a wider scope of the war, but little combat exposure.[71]

The War on Terror has ushered in a new wave of regulations on First Amendment freedoms.[72] President George W. Bush addressed the nation in 2001, claiming "you are with us or with the terrorists" regarding the quick passage of the USA PATRIOT ACT (Patriot Act) which gives greater investigatory powers to the federal government and its agencies.[73] Since 2001, the definition of "war" to the American public has evolved from a conflict between two sovereigns on a battlefield to a broader conflict, rooted in ideology, against diverse, loosely aligned enemies and even targeting civilian populations.[74]

Formally, the United States could only declare war through congressional action.[75] However, this constitutional authority has not been exercised since World War II.[76] In the 1960s and 1970s, the chambers of Congress did not declare war against Vietnam; however, massive troops were deployed across South East Asia.[77] In the 1990s, Congress did not declare war on Iraq, but American troops saturated Kuwait and Saudi Arabia in the Persian Gulf.[78] Today, with the War on Terror, we live in a world where war "last[s] indefinitely."[79] Defining wartime in 2017 requires also defining terrorism. International terrorism refers to activities that meet three key characteristics:

> (A) Involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any state; or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; (B) appear to be intended-- (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass

69. W. LANCE BENNETT & DAVID L. PALETZ, TAKEN BY STORM: THE MEDIA, PUBLIC OPINION, AND U.S. FOREIGN POLICY IN THE GULF WAR 5 (1994).

70. *Id.*

71. *Id*.

72. *See* STONE, *supra* note 10, at 554.

73. *Id.* at 551.

74. *See generally* RALPH STEINHARDT ET AL., INTERNATIONAL HUMAN RIGHTS LAWYERING 1065 (2008).

75. U.S. CONST. art. I, § 8, cl. 11.

76. *See* REHNQUIST, *supra* note 11, at 218.

77. *Id*.

78. *See* BENNETT & PALETZ, *supra* note 69, at xi; *See also* REHNQUIST, *supra* note 11, at 218.

79. STONE, *supra* note 10, at 554 (quoting former President George W. Bush).

> destruction, assassination, or kidnapping; and (C) occur primarily outside the territorial jurisdiction of the United States . . . .[80]

This Note assumes a more contemporary definition of war, which extends beyond congressionally declared war to militant, hostile situations such as the Vietnam War, and to all armed conflicts against terrorist entities, such as the War on Terror.

C. Despite This Historical Precedent, the First Amendment Permits Censorship of Speech Only in Limited Circumstances.

An American's right to freedom of speech is not absolute.[81] The First Amendment guarantees that "Congress shall make no law . . . abridging the freedom of speech, or of the press."[82] These words, although broad, are understood by the United States Supreme Court to exclude certain types of speech.[83] In *Chaplinksy v. New Hampshire*, the Court held that there are certain types of speech that the Constitution does not have a legitimate interest in protecting.[84] Justice Frank Murphy asserted "[t]here are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which have never been thought to raise any constitutional problem."[85] In practice, however, the Court has struggled to define what categories of speech are unprotected, how a form of speech even receives entry into that category, and what level of scrutiny applies to each category.[86]

To determine whether an individual's right to freedom of speech has been infringed upon due to the speech's specific content the Supreme Court generally applies a strict scrutiny test. [87] Strict scrutiny requires that any such law be "narrowly tailored to serve a compelling state interest."[88] In determining whether such state action is constitutional, the Court applies this high standard as a two-part test to inquire: (1) whether the act is narrowly tailored, and (2) whether the act serves a compelling state interest.[89] The Court first analyzes whether the government interest at issue is compelling, stating in *Holder v. Humanitarian Law Project* that national security and

---

80. 18 U.S.C. § 2331(1) (2012).

81. *See, e.g.*, Virginia v. Black, 538 U.S 343, 358 (2003); *See also* GREGORY MAGGS & PETER SMITH, CONSTITUTIONAL LAW, A CONTEMPORARY APPROACH 860 (2d ed. 2011).

82. U.S. CONST. amend. I, § 1.

83. Chaplinksy v. New Hampshire, 315 U.S. at 571–72.

84. *Id.* at 572–73.

85. *Id.* at 571–72.

86. *See* Maggs, *supra* note 81, at 860–65.

87. Richard H. Fallon, Jr., *Strict Judicial Scrutiny*, 54 UCLA L. REV. 1267, 1304 (2007) (quoting Gerald Gunther's epic "'strict' in theory and fatal in fact.").

88. Eugene Volokh, *Freedom of Speech, Permissible Tailoring and Transcending Strict Scrutiny*, 144 U. PA. L. REV. 2417, 2418 (1996) (quoting Austin v. Mich. Chamber of Commerce, 494 U.S. 652, 655 (1990)).

89. *See id.*

foreign affairs satisfy this high bar.[90] While it is often easier for the Supreme Court to identify a compelling state interest, "[m]ost cases striking down speech restrictions . . . rely primarily on the narrow tailoring prong."[91] A law is narrowly tailored if it *actually* advances a compelling state interest, is not over or under-inclusive, and demonstrates the least-restrictive government alternative possible.[92]

Examples of acts that have failed to meet this test are the Communications Decency Act (CDA) and the Child Online Protection Act (COPA). Both acts target minors' access to pornography on the Internet.[93] The CDA imposed criminal liability for a child's exposure to indecent or obscene materials on the Internet, and COPA required commercial distributors to restrict access to their sites by minors.[94] These acts, however, failed to meet the narrowly tailored prong of the strict scrutiny test because they targeted all Internet users in order to protect children, making them over inclusive and discriminatory towards adults.[95] A similar act, the Children's Internet Protection Act (CIPA), passed constitutional muster because it specified a ban on certain Internet sites in K-12 schools and libraries.[96] The Court held this was limited enough in scope to be considered narrowly tailored.[97]

While strict scrutiny disfavors content-based speech restrictions, the Supreme Court has created other tests for other forms of content-neutral speech and content-based "low-value speech."[98] One of those unprotected content-based speech categories is incitement, formerly known as "clear and present danger."[99] Many of the early cases applying the clear and present danger doctrine dealt with wartime speech.[100] A former test for clear and

90. Holder v. Humanitarian Law Project, 561 U.S. 1, 36 (2010) ("Given the sensitive interests in national security and foreign affairs at stake, the political branches have adequately substantiated their determination that, to serve the Government's interest in preventing terrorism, it was necessary to prohibit providing material support in the form of training, expert advice, personnel, and services to foreign terrorist groups . . . .").

91. Volokh, *supra* note 88, at 2421.

92. *See id.* at 2422–23.

93. *See generally* Communications Decency Act of 1996, 47 U.S.C. § 230 (2012); Child Online Protection Act, 47 U.S.C. § 231 (2012).

94. *See* 47 U.S.C. § 223(d) (2012); *See also* Child Online Protection Act § 231.

95. *Compare* Reno v. American Civil Liberties Union, 521 U.S. 844, 882 (1997) (ruling the Communications Decency Act § 223 unconstitutional), *with* Ashcroft v. American Civil Liberties Union, 535 U.S. 564, 585 (2002) (ruling the reliance on community standards by Child Online Protection Act § 231 to identify what material "is harmful to minors" does not by itself make the statute substantially overbroad).

96. *See* Children's Internet Protection Act, Pub. L. 106–554. Title XVII, §§ 1701- 1741; *cf.* United States v. Am. Library Ass'n, Inc., 539 U.S. 194, 195 (2003).

97. *See id*.

98. *See* Tom Hentoff, *Speech, Harm, and Self-Government: Understanding the Ambit of the Clear and Present Danger Test*, 91 COLUM. L. REV. 1453, 1456–59 (1991); *see also* Chaplinksy v. New Hampshire, 315 U.S. 568, 574 (1942); FCC v. Pacifica Found. (*Pacifica*), 438 U.S. 726, 726 (1978).

99. *See* Tom Hentoff, *Speech, Harm, and Self-Government: Understanding the Ambit of the Clear and Present Danger Test*, 91 COLUM. L. REV. 1453, 1457 (1991).

100. *See* Schenck v. United States, 249 U.S. 47, 52 (1919).

present danger "whether the gravity of the 'evil,' discounted by its improbability, justifies such invasion of free speech as necessary to avoid the danger."[101] This test, as quoted in *Dennis v. United States*, was used to uphold the conviction of USA Communist General Secretary Eugene Dennis for violating the anti-Communist Smith Act.[102]

The clear and present danger exception to the First Amendment referred to direct, active wartime speech, not passive anti-government speech.[103] The defendants in *Schenck v. United States* met this active speech requirement when they publicly distributed anti-World War I leaflets because it could presently incite illegal behaviors of draft-age men.[104] Justice Oliver Wendell Holmes wrote "when a nation is at war, many things that might be said in time of peace are such a hindrance to its effort that their utterance will not be endured so long as men fight, and that no Court could regard them as protected by any constitutional right."[105] However, the defendants in *Yates v. United States*, USA Communist Party members who violated the Smith Act, did not meet the clear and present danger test because of the difference between *direct* advocacy dedicated to overthrow the government, and the *abstrac*t idea of overthrowing the government.[106] The former is potentially unprotected speech, while the latter is generally protected.[107]

In *Brandenburg v. Ohio* the Court refined the clear and present danger test to its present form – incitement.[108] The current test for incitement bars states or the federal government from "forbid[ding] or proscrib[ing] advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action."[109] Although not expressly defined, "lawless action" refers to serious crimes.[110] "Imminent," although not formally defined by the Supreme Court, refers to the timeline of the crime.[111] For example, mail fraud is a slow-results producing crime and does

101. Dennis v. United States, 341 U.S. 494, 510 (1951) (*citing* United States v. Dennis, 183 F.2d 201, 212 (2d Cir. 1950)).

102. *Id.*at 517.

103. *See* Yates v. United States, 354 U.S. 300, 324–26 (1957).

104. *See Schenck*, 249 U.S. at 52.

105. *Id.*

106. *Id.*

107. *Id.*

108. *See* Brandenburg v. Ohio, 395 U.S. 444, 447–48 (1969). The Court a few years later would also hand down a stricter version in another doctrinal test, fighting words, in *Cohen v. California*, 403 U.S. 15, 16 (1971), where the Court held the ability of the public to shield their faces when Cohen walked by in a jacket that said "Fuck the Draft" was important in determining the jacket was protected under the First Amendment.

109. *Id.*

110. The Supreme Court has not officially held seriousness as a requirement, but it is an assumed remnant of the Court's test in *Dennis v. United States*. *See* Bradley Pew, *How to Incite Crime with Words: Clarifying Brandenburg's Incitement Test with Speech Act Theory*, 2015 BYU L. REV. 1104 (2015).

111. *See* Hess v. Indiana, 414 U.S. 105, 108 (1973) (holding that "advocacy of illegal action at some indefinite future time" does not meet the standard of imminent under the incitement doctrine); *see also* Pew, *supra* note 110, at 1088–89.

not meet the imminent requirement for incitement.[112] In their incitement doctrine, the United States Court of Appeals for the Fifth Circuit (Fifth Circuit) highlighted the importance of the publicity of the activity, finding that "[t]he root of incitement theory appears to have been grounded in concern over crowd behavior."[113] The Supreme Court after the *Brandenburg* decision has yet to invoke the doctrine in favor of restricting speech.[114] The Court has, however, restricted speech in contexts where incitement may have applied, but the Court declared the speech to be unprotected without invoking a formal test.[115]

Another content-based restriction on speech outside of the Supreme Court's strict scrutiny test is broadcast obscenity under 18 U.S.C. § 1464.[116] Section 1464 regulates language on broadcast radio and television, namely criminalizing the utterance of obscene, indecent, or profane language.[117] This Act was held to be constitutional in *FCC v. Pacifica Foundation* when applied to broadcast television.[118] *Pacifica* affirmed the FCC's authority to regulate indecent material over broadcast because the Act specified that it was limiting indecent material to times when children were more likely to be in the broadcast audience.[119] The Court commented on the importance of broadcast media while making this decision, stating that "broadcast media ha[s] established a uniquely pervasive presence in the lives of all Americans. . . . Because the broadcast audience is constantly tuning in and out, prior warnings cannot completely protect the listener or viewer from unexpected program content."[120]

The Supreme Court echoed this language in *Red Lion Broadcasting Co. v. FCC* calling broadcast media unique in that it invades the privacy of the home and is particularly accessible to children.[121] The *Pacifica* view of the media has been critiqued in the years after the decision, but has not been overturned.[122] One such critique is that broadcast media, in part due to the

112. *See* Brandenburg, 395 U.S. at 447; United States v. Rowlee, 899 F.2d 1275, 1280 (2d Cir. 1990).

113. Herceg v. Hustler Magazine, Inc., 814 F.2d 1017, 1023 (5th Cir. 1987).

114. *See* Tom Hentoff, *Speech, Harm, and Self-Government: Understanding the Ambit of the Clear and Present Danger Test*, 91 COLUM. L. REV. 1453, 1456–59 (1991).

115. *Id*.; s*ee also* United States v. Williams, 553 U.S. 285, 288 (2008).

116. 18 U.S.C. § 1464. ("Whoever utters any obscene, indecent, or profane language by means of radio communication shall be fined under this title or imprisoned not more than two years, or both.") The test was developed by the Supreme Court in *Miller v. California*, 413 U.S. 15 (1973).

117. *Id*.

118. *See* FCC v. Pacifica Found. (*Pacifica*), 438 U.S. 726, 748 (1978).

119. *Id*.

120. *Id*.

121. *See* Red Lion Broadcasting Co. v. FCC (*Red Lion*), 395 U.S. 367, 390 (1969).

122. *See* Lili Levi, *The FCC's Regulation of Indecency*, 7 FIRST AMEND. CTR. 1, 1–10 (2008); *see also* Leslie Kendrick, G. Edward White, Frederick Schauer, *Is It Legal? The FCC's Authority to Regulate Broadcast Indecency*, UVA LAW (Jan. 10, 2012), http://www.law.virginia.edu/html/news/2012_spr/fcc_indecency.htm [https://perma.cc/93UY-YE99].

rise of cable television, is no longer uniquely "pervasive," and that the Internet should now carry this burden.[123]

III. TERRORIST SPEECH ON THE INTERNET SHOULD BE CENSORABLE BY THE GOVERNMENT.

Through acts of Congress, executive orders, judicial rulings, and the decisions of private citizens, the censorship of certain materials during wartime is consistent. As previously discussed, this censorship has taken two main forms: first, the censoring of speech relating either to government opposition or to allegedly anti-American doctrines; and second, the censorship of the most visually intrusive forms of media as they showcase the grislier aspects of war.[124] Because the Internet is now one of the most prominent mass media channels for visual forms of terrorist speech, the United States is justified in censoring online terrorist speech.[125]

A. Censoring Terrorist Speech Today is Consistent with the Tradition of Restrictions on Anti-Government Wartime Speech.

Speech associated with anti-government positions has traditionally been subject to heightened governmental censorship in times of war, despite constitutional protection for free speech.[126] Whether this censorship is confiscating enemy-sympathizing publications, such as the *New Hampshire Gazette* during the American Revolution,[127] or restricting information from the front lines, such as the government-registered press in World War I, II, and Vietnam,[128] censorship of perceived anti-government speech is consistent and predictable throughout American history. These types of restrictions have also been present in congressional acts (and judicial opinions interpreting them), ranging from the Sedition Act of 1789 to the Communist Control Act of 1954.[129]

Given this historical practice, the Supreme Court has established First Amendment doctrine to identify contexts for protecting certain categories of

123. *See* Leslie Kendrick, G. Edward White, Frederick Schauer, *Is It Legal? The FCC's Authority to Regulate Broadcast Indecency*, UVA LAW (Jan. 10, 2012), http://www.law.virginia.edu/html/news/2012_spr/fcc_indecency.htm [https://perma.cc/BSY8-5P5J].

. The FCC indicated their interest in the Internet as well in: *In the Matter of Protecting and Promoting the Open Internet*, FCC (Feb. 26, 2015), ¶1–6 and *Universal Service*, FCC, https://www.fcc.gov/general/universal-service.

124. *See* discussion *supra* Section II(B).

125. *See* Mohr, *supra* note 15, at 43.

126. *See* discussion *supra* Section II(B).

127. *See* LINFIELD, *supra* note 43, at 15.

128. *See* MANDER, *supra* note 48, at 45, 61, 67.

129. *See generally* Sedition Act of 1789, 50 U.S.C. §§ 21–24 (2012); Communist Control Act of 1954, 50 U.S.C. §§ 841–844 (2012); s*ee also* Espionage Act of 1917, 18 U.S.C. § 792 (2012); Sedition Act of 1918, Pub. L. 65–150 § 3 (1918); Smith Act of 1940, 18 U.S.C. § 2385 (2012).

speech.[130] As a legal trend, the Court has moved away from "overreactions" during wartime hostilities, such as the harsh Communist Control Act of 1954, and has invalidated acts of censorship that it deems to be excessive.[131] As a historical trend, however, censorship is pervasive. As recent as the Operation Enduring Freedom in Iraq, American communications on the warfront were plagued by press restriction.[132] The Patriot Act continues to criminalize speech that is anti-American.[133] The War on Terror presents another time in American history where anti-United States government, anti-American interests are at issue.[134]

Censorship restricting terrorist speech for the War on Terror is consistent with the doctrine of censoring active anti-government speech because active terrorist speech is akin to anti-government wartime speech. Beyond falling within the category of anti-government wartime speech, terrorist speech is a more refined, narrower category than previous, broader forms of wartime censorship, such as under the Office of Censorship in World War II.[135] Under the Office of Censorship, wartime speech was broadly defined as encompassing solider locations, military resources, and destination of any armed forces.[136] Terrorist speech refers to actual acts of terrorism online, videos of terrorist activities, or active recruitment to terrorist organizations.[137] It is doctrinally distinct from constitutionally protected discussions and opinions on terrorism and the War on Terror. Like the Court's distinction regarding the Smith Act of 1940, where the Court refused to invalidate all communist forms of speech, but asserted a difference between communist speech discussing overthrowing the government and an active communist plot to overthrow the government, there is a difference between discussions of acts of terror and speech inciting the acts themselves.[138]

The former, voices of opposition, emerging from the press and public alike, have historically contributed to a valuable national discourse.[139] Given the political environment in the United States in 2017, these voices are imperative. However, this is not the type of speech currently at issue. Videos of torture do not spark significant contributions to the marketplace of ideas where constitutionally protected speech thrives, because their purpose is to terrorize and, by definition, to intimidate.[140] Intimidation and cruelty are not

130. *See* discussion *supra* Section II (C).

131. *See generally* Snyder v. Phelps, 562 U.S. 443 (2011); Tinker v. Des Moines Independent Community School District, 393 U.S. 503 (1969).

132. *See* Terry, *supra* note 68, at 178.

133. *See* 18 U.S.C. § 2339A (2012); s*ee also* STONE, *supra* note 10, at 551.

134. This Note does not condone all of the censorship practices of the United States government, nor does it assert they all have been legally accomplished. Rather, it asserts that given the widespread practice of government censorhip in the two outlined categories, measures should be taken to hold the government accountable for the materials they censor.

135. *See* MANDER, *supra* note 48, at 58.

136. *Id*.

137. *Infra* at Section IV(A).

138. *See* Dennis v. United States, 341 U.S. 494,510 (1951).

139. *Id*. at 9 (discussing the First Amendment's purpose in the marketplace of ideas).

140. *See* Friis, *supra* note 32, at 729.

introduced into the marketplace to spark knowledge, nor does this form of mass media result in a productive conversation on terrorism.[141] Instead, it produces grieving families, like James Foley's, and exposes vulnerable families across the United States whose lives are impacted by terrorist organizations.[142]

Terrorism also presents new challenges deviating from this typical model of anti-government wartime censorship because it implicates the abstract territory of the Internet. The War on Terror is not only being fought on a physical battlefield, where the government can limit press access, it is being fought online.[143] On the Internet, one cannot always avert their eyes from the information displayed on their screen (such as viral news video, an advertisement or a pop-up) in the way a passerby could avert their eyes from Cohen's jacket which read "Fuck the Draft."[144] Employing a censorship model based on the Saigon Press Corps would not be an effective means for the government to control information online.[145] When a decapitation video is posted online, it is infeasible to criminalize the reposting of the link in the same manner that the Sedition Act of 1918 criminalized anti-government speech. Because the Internet is an intrusive medium and is less censorable than a print newspaper,[146] the War on Terror cannot rely on historical models for censoring anti-government speech.

B. Targeting Internet-Based Speech is Consistent with the Tradition of Restrictions on Uniquely Invasive Media.

Visual forms of media are censored more frequently than other types of media because they expose the most shocking aspects of war to the American public.[147] How Americans receive their news and the type of speech at issue are significant factors in determining the level of censorship to be applied.[148] During the American Revolution, print newspapers like the *New Hampshire Gazette* were routinely censored as the dominant form of media, despite being relatively noninvasive.[149] By the time of the Civil War, sketch artists like Alfred Waud experienced censorship because he showed the more visual

141. *Id.*

142. *See* Hannah Jane Parkinson, *James Foley: How Social Media is Fighting Back Against Isis Propaganda*, THE GUARDIAN (Aug. 20, 2014, 11:06 AM EDT), http://www.theguardian.com/technology/2014/aug/20/james-foley-how-social-media-is-fighting-back-against-isis-propaganda [https://perma.cc/JLQ3-HMHQ].

143. *See Report Online Terrorist Material*: *Reporting Crimes and Getting Compensation*, UK GOV., https://www.gov.uk/report-terrorism (last Accessed Aug. 10, 2015) [https://perma.cc/3RTV-9BZL].

144. *See* Cohen v. California, 403 U.S. 15, 21 (1971).

145. *See* MANDER, *supra* note 48, at 65.

146. *See* Philip Bennett & Moises Naim, *21st-Century Censorship*, COLUM. JOURNALISM REV. (Jan. 22, 2017, 3:52 PM), http://www.cjr.org/cover_story/21st_century_censorship.php [https://perma.cc/5GRU-S623].

147. *See* FCC v. Pacifica Found. (*Pacifica*), 438 U.S. 726, 748 (1978).

148. *Id.*

149. *See* LINFIELD, *supra* note 43, at 15–17.

aspects of the war—the dead, the fallen, and the disgraced.[150] This trend continued when radios, television, and movies came into existence and grew in popularity.[151]

Television and current events newsreels during World War I and World War II became the most visual and popular forms of media and therefore were subject to widespread censorship.[152] They invaded the minds and eyes of Americans in a way print newspapers could not.[153] By 1959 television news programs had progressed significantly in the homes of the average American, as 43.9 million American families owned television sets as opposed to 3.6 million just ten years earlier.[154] In response to the growing trend of broadcast television, censorship of non-wartime speech increased as well.[155] It is not surprising that only five years after the United States left Vietnam, the Supreme Court upheld the FCC's indecency speech restrictions, finding that "broadcasting is uniquely intrusive, and that viewers or listeners would have no way of avoiding in advance the language or images that might offend them."[156] This theme of unavoidability is now more relevant for viral media forms on the Internet. Today, viral social media exhibits the same characteristics of television that the Court observed in *Pacifica*.[157]

Although television remains an important source for news, a majority of people use the Internet and social media to serve this function.[158] The ability of news to "go viral" and be shared millions of times with people around the world has made the Internet as uniquely intrusive as the Supreme Court found broadcast media to be in *Pacifica*.[159] In 1978, the Court held in *Pacifica* that broadcasting is uniquely intrusive.[160] In the 1970s, broadcast media was becoming increasingly popular, especially after the Vietnam War.[161] The Court in *Pacifica* understood that these new forms of technology presented a different beast than print media proposed.[162] This view of the uniqueness of broadcast media invading the home and the lifestyles of Americans was presented to the Court in *Red Lion* almost a decade earlier.[163]

---

150. *See* ROEDER, *supra* note 46, at 29.

151. *See* BERNHARD, *supra* note 62, at 46.

152. *See* ROEDER, *supra* note 46, at 17; BERNHARD, *supra* note 62, at 47.

153. *See* ROEDER, *supra* note 46, at 17 (citing Pathe Exch., Inc. v. Cobb, 202 App. Div. 450, 456 (N.Y. App. Div. 1922)).

154. *See* BERNHARD, *supra* note 62, at 47.

155. *See* FCC v. Pacifica Found. (*Pacifica*), 438 U.S. 726,748 (1978); Red Lion Broadcasting Co. v. FCC (*Red Lion*), 395 U.S. at 390.

156. Brian McNeill, *The FCC's Authority to Regulate Broadcast Indecency,* UVA LAW (Jan. 10, 2012), http://content.law.virginia.edu/news/2012_spr/fcc_indecency.htm [https://perma.cc/K2MK-WHVF].

157. *See generally Pacifica*, 438 U.S. at 748.

158. Jeffrey Gottfried & Elisa Shearer, *News Use Across Social Media Platforms 2016*, PEW RES. CTR. (May 26, 2016), http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/ [https://perma.cc/Z9H9-JRU2].

159. *See Pacifica*, 438 U.S. at 748.

160. *See id*.

161. *See* BERNHARD, *supra* note 62, at 47.

162. *See Pacifica*, 438 U.S. at 748.

163. *See* Red Lion Broadcasting Co. v. FCC (*Red Lion*), 395 U.S. 367, 386–88 (1969).

This same reasoning from *Red Lion* and *Pacifica* is now applicable to the Internet, which poses an analogous threat of transmitting graphic videos and other forms of terrorist propaganda into American households without the consent of viewers.[164]

When a video goes viral, clips of its content appear everywhere: shared by friends on Facebook, posted on online news sites, and shared in emails.[165] This mass media effect cannot be contained by the same means employed in the Civil War, when President Lincoln ordered the seizure of telegraph wires to inhibit the transmission of Confederate communications and news.[166] President Lincoln was successful because alternative routes of information—such as horseback, train, or on foot—were inherently slower and less reliable.[167] Here, we are dealing with mass media as opposed to horseback.[168] One of the modern critiques of the *Pacifica* decision is that broadcast media no longer represents a unique form of communication, given the influence of the Internet.[169] This supports, then, that the Internet has filled this gap and should be given extra consideration as this pervasive type of media.[170] Social media, in particular, presents an exceptional situation.[171] In her article about ISIS's online media presence, Simon Molin Friis explains that "transformations in the way in which images can be produced and circulated increase visual interconnectivity across borders and facilitate new ways of communicating the horrors of war."[172]

Therefore, while specific media technologies have changed over time, censorship restrictions that shield the gruesome nature of warfare or certain forms of anti-government speech have survived. At every stage of America's wartime history, freedom of speech was never truly free.[173] Today, America is engaged in a War on Terror of "indefinite" duration.[174] This war is being waged in person, but also electronically.[175] The number of government data requests in 2015 rose eleven percent.[176] Meanwhile, "ISIS has managed to recruit [over] 6000 new members in June of 2014 alone."[177] The problem is not going away. Mass media sites featuring videos like James Foley's

164. *See* Friis, *supra* note 32, at 729.

165. *See generally* Mohr, *supra* note 15, at 43.

166. *See* MANDER, *supra* note 48, at 24.

167. *Id*.

168. Mohr, *supra* note 15 at 43.

169. FCC v. Pacifica Found. (*Pacifica*), 438 U.S. 726, 748 (1978).

170. *Id.*

171. *See generally* Leslie Kendrick, G. Edward White & Frederick Schauer, *Is It Legal? The FCC's Authority to Regulate Broadcast Indecency*, UVA LAW (Jan. 10, 2012) http://www.law.virginia.edu/html/news/2012_spr/fcc_indecency.htm [https://perma.cc/HN4D-N5MM].

172. *See* Friis, *supra* note 32, at 726.

173. *See* STONE, *supra* note 10, at 12–13.

174. *See* STONE, *supra* note 10, at 554 (quoting former President George W. Bush).

175. *See* Mohr, *supra* note 15, at 43.

176. *See United States Law Enforcement Requests for Data, Jan. 2015- June 2015*, FACEBOOK, https://govtrequests.facebook.com/country/United%20States/2015-H1/# (last visited Mar. 27, 2017) [https://perma.cc/Y5PC-RW24].

177. Bolan, *supra* note 24, at 141.

penetrate computer screens across the nation, achieving ubiquity at the expense of shocked audiences.[178] Now is the time for the legal, formalized practice of wartime censorship. Regulating terrorist speech online—speech that expressly represents an act of terror, such as the beheading of an American national or the recruitment of American citizens to terrorist forces—should be within the discretion of the United States government to regulate.[179] The political waltz between the past actions of the federal government and the unfulfilled promises of the First Amendment needs to step in a new direction to combat the sinister issue of terrorist speech on the Internet.

IV. THE "STOP TERRORIST ORGANIZATIONS FROM PROMOTING INTERNET TRANSMISSIONS ACT" COULD PERMISSIBLY REGULATE TERRORIST SPEECH ONLINE.

The most effective measure for regulating terrorist speech on the Internet would be through congressional action, granting a body, such as the FCC, the power to order removal of online terrorist speech. However, if legislative actions fail to materialize, another option could be to establish a uniform "Code of Ethics" agreed upon by owners of mass media sites.

A. STOP IT: The Stop Terrorist Organizations from Promoting Internet Transmissions Act Would Give the FCC the Power to Regulate Terrorist Speech Online.

The proposal for the "Stop Terrorist Organizations from Promoting Internet Transmissions Act" (STOP IT) would specifically define the bodies implementing the Act, the speech covered under the Act, and the technological methods the Act would use.[180] The proposed body for STOP IT's implementation would be the FCC, the definition of covered terrorist speech would derive from the United State Code's definition of terrorism, and URL blocking would likely be the most effective method of enforcement.

For the FCC to censor terrorist speech, Congress would need to pass legislation (i.e., the STOP IT Act) to give the FCC express authority to regulate expressions of terror, or terrorist speech, present on the Internet.[181] The definition of terrorist speech would derive from the codified definitions of international and national terrorism.[182] Those definitions depart with regard to territoriality, but the three shared characteristics that constitute terrorist speech are acts "(i) to intimidate or coerce a civilian population; (ii)

178. *See* Reich, *supra* note 2.

179. *See* Reich, *supra* note 2.

180. *See generally* Bambauer, *supra* note 25, at 390–400 (discussing "openness, transparency, narrowness, and accountability" as the primary factors in evaluating a country's Internet filtering practices).

181. *Cf. id.*

182. 18 U.S.C. § 2331(1) (2012).

to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping."[183] Given this definition, STOP IT would cover acts that "depict or advocate for violent acts, or acts dangerous to human life, by use of the unique, visual influence of mass media." Video and photographic representations of acts of terrorism and active recruitment postings, according to these definitions, would be censorable by the FCC to combat against the "going viral" effect.[184]

To combat the viral nature of content on the Internet, STOP IT could model the UK's Counter Terrorism Internet Referral Unit's strategy of having members of the public flag what they view as posts and videos that showcase acts of terror in addition to having a federal bureau with the ability to flag and remove the source of terror from the Internet.[185] A federal bureau devoted to national security and cybersecurity threats would be an asset to STOP IT as they would be able to offer their expertise regarding what information to flag. First, members of the public would flag the materials; second, the appropriate federal bureau would review what the public has flagged in addition to being able to flag material itself; and third, the FCC would decide whether to remove the flagged materials, or reject the removal of the website, post, or video, and let it remain in the public's eye.

The FCC is an appropriate body to take this course of action because STOP IT would mirror the FCC's responsibilities in its obscenity regulations.[186] It would be natural for the FCC to step into this type of role, given the interpretative powers the FCC employs under the obscenity and indecency regulations. Despite modern criticisms of the *Pacifica* doctrine, the FCC has continued to regulate profanity, indecency, and obscenity in broadcast, and the agency has expressed its willingness to engage in the regulation of the Internet through net neutrality and Internet subsidy plans.[187] Under STOP IT, every website, post, or video flagged would be collected and stored in a database and remain confidential unless the censorship became an issue of a law suit. This would create an internal record of the websites that are being censored; a record which could contribute to a greater

183. *Id*.

184. *See* Mohr, *supra* note 15at 43.; CBS DC, *supra* note 22.

185. *See Tackling Extremism in the UK*: *Report from the Prime Minister's Task Force on Tackling Radicalisation and Extremism*, H.M. GOVERNMENT 1, 3 (2013); *Report Online Terrorist Material*: *Reporting Crimes and Getting Compensation*, UK GOV., https://www.gov.uk/report-terrorism (last updated Sep. 23, 2016) [https://perma.cc/8VDR-6L2V].

186. *See generally* 18 U.S.C. § 1464 (2012).

187. *See, e.g.*, Protecting and Promoting the Open Internet, *Report and Order on Remand, Declaratory Ruling, and Order*, 30 FCC Rcd 5601, 5603–04 (2015); *Universal Service*, FCC, https://www.fcc.gov/general/universal-service (last visited May 28, 2017) [https://perma.cc/AG6X-XDEV]; *Regulation of Obscenity, Indecency and Profanity*, FCC, https://www.fcc.gov/general/regulation-obscenity-indecency-and-profanity (last visited May 28, 2017) [https://perma.cc/T9P4-CMM5]. The FCC is showing increased willingness to engage in conversations outside of radio and broadcasting into Internet services.

understanding of terrorist enemies.[188] More information on the terrorist usage of social media would be helpful considering the new body of scholarship pointing to the increased significance of social media as a multi-use tool for terrorist organizations.[189]

STOP IT would confer standing to appeal a censorship decision to owners of sites with removed data or account owners of an affected social media account. This would create transparency and incentivize the FCC to regulate as they deem fit, but not give them unlimited power without a proper constitutional check.[190] Having a standing-to-sue based policy would also promote government legitimacy.[191] Similar to the UK's Initiative, the tactical form of blocking employed under STOP IT would likely be URL blocking for the ease of the public and federal bureau to flag materials and the FCC to block specific URLs.[192] If a video, such as the James Foley video, went viral and was posted on a variety of websites, URL blocking for each would be harder to track, but with three levels of website flagging, and the general knowledge of a viral video circulating, URL blocking should not create a legitimate enforcement issue. STOP IT would also stipulate review of the success of the project in a quantifiable deadline, potentially five years after implementation. The specifics of STOP IT's constitutionality is the most pressing issue for its creation.

B. STOP IT Would Provide a Medium Through Which Censorship of Terrorist Speech Could be Narrowly Tailored to Meet Constitutional Muster.

There are two potential avenues STOP IT could be analyzed under the First Amendment: strict scrutiny or incitement, depending on the Supreme Court's application of the scope of the act.[193] If STOP IT is considered to cover only incitement-based speech, it would not afford any First Amendment protections, however if STOP IT covers content-based speech outside of incitement doctrine, a strict scrutiny test would be employed to the speech at issue. STOP IT would have a difficult time meeting the requirements of either strict scrutiny or incitement, but could satisfy strict scrutiny more easily than incitement given a flexible Supreme Court bench.

First, STOP IT could be viewed solely through the doctrine of incitement. If viewed as incitement, the test would be whether the speech prohibited by the government is "directed [at] inciting or producing imminent

188. *See* Bambauer, *supra* note 25, at 393 .

189. *See* Secara, *supra* note 23, at 79–81 .

190. *See* Bambauer, *supra* note 25, at 394–95.

191. *Id.* at 408.

192. *See* Carlo Davis, *UK 'Porn' Filter Will Also Block Violence, Alcohol, Terrorism, Smoking, And 'Esoteric Material'*, (Jul. 29, 2013, 11:40 AM), http://www.huffingtonpost.com/2013/07/29/uk-internet-filter-block-more-than-porn_n_3670771.html [https://perma.cc/7C8R-6MTD].

193. *See* discussion, *supra* Section II(C).

lawless action and is likely to incite or produce such action."[194] The two key clauses for the purposes of this Act are "directed to" and "imminent lawless action."[195]

"Directed to" was key to the Supreme Court's decision in *Schenck*, which upheld an individual's criminal conviction for anti-draft pamphleteering during World War I.[196] For the *Schenck* court, there was an important distinction between the advocacy of general "Communist" principles and the advocacy of Communist behavior, such as draft evasion, which is more closely connected to actively disobeying the government.[197] This distinction is key to the STOP IT Act. STOP IT targets acts of terrorism that have been committed and are now online in photographic or video form, or active terrorist membership.[198] STOP IT does not limit discussing acts of terrorism, with which the Court disagreed in *Yates*, but rather the *specific* actions of terror and advancements of terrorism that the Court was concerned with in *Schenck* and *Dennis*.[199]

"Imminent lawless action" would be difficult to satisfy due to the requirement of "imminence.[200] The lawless action requirement, although not specifically defined, is generally understood as referring to serious, particularly violent, crimes, which would include acts of terrorism.[201] The "imminent" requirement, however, is lacking a formal definition.[202] In *Rowlee*, the Supreme Court refused to recognize mail fraud, a slower results-producing crime, as an imminent crime under incitement,[203] and lower circuits, such as the Fifth Circuit, have highlighted the importance of the public in incitement doctrine.[204] Timing is the principal issue with viral terrorist videos on the Internet and the active solicitation of members to join terrorist groups.[205] Recruiting an individual to join ISIS and engage in

194. *See* Brandenburg v. Ohio, 395 U.S. 444, 447 (1969).
195. *Id.*
196. *See* Schenck v. United States, 249 U.S. 47, 52–53 (1919).
197. *Id*.
198. *See* Friis, *supra* note 32, at 737.
199. Dennis v. United States, 341 U.S. 494, 510 (1951); *Schenck*, 249 U.S. at 52.
200. Brandenburg v. Ohio, 395 U.S. 444, 447 (1969).
201. *See* MAGGS, *supra* note 81, at 993.
202. *Id*.
203. *See* United States v. Rowlee, 899 F.2d 1275, 1280 (2d Cir. 1990).
204. *See* Herceg v. Hustler Magazine Inc., 814 F.2d 1017, 1023 (5th Cir. 1987).
205. Timing is an issue courts have unsympathetically addressed in recent lawsuits involving social media and terrorist organizations. *See* Eric Goldman, *Facebook Defeats Lawsuit Over Material Support for Terrorists–Cohen v. Facebook*, TECH. & MARKETING L. BLOG (May 18, 2017), http://blog.ericgoldman.org/archives/2017/05/facebook-defeats-lawsuit-over-material-support-for-terrorists-cohen-v-facebook.htm [https://perma.cc/W2FB-MJCT]. In *Cohen v. Facebook*, plaintiffs argued that the nature of Facebook allowed, and continues to allow, Hamas to freely recruit new members and plan attacks. *See generally* Cohen v. Facebook, Inc., 2017 WL 2192621, at *22 (E.D.N.Y. May 18, 2017). The case was dismissed for lack of subject matter jurisdiction in part because plaintiffs could not establish a specific harm based upon the threat of an imminent terrorist attack. *Id.* at *11. Although it addresses jurisdiction, *Cohen* exemplifies the challenges social media presents to the law, namely the difficulty in determining how much a party is harmed and the timeline of that specific harm.

terrorist activities could take hours, days, weeks, or months and cannot be quantified under nebulous Supreme Court language that defines imminence as not "some indefinite future time."[206] This is a more attenuated connection than the Court has traditionally accepted in its standard application of the *Brandenburg* test. [207]

Second, STOP IT could be viewed as effecting speech beyond the incitement doctrine and therefore would need to be "narrowly tailored to serve a compelling state interest" under strict scrutiny.[208] Preventing the spread of terrorism and the viewing of acts of terror are compelling state interests, and the Court has construed the interest of security broadly in times of war and military conflict—most recently with terrorism in *Humanitarian Law Project*.[209] The key, therefore, for STOP IT to pass a strict scrutiny test would be showing how STOP IT is not over or under inclusive, while utilizing the least restrictive means to achieve its goal.[210]

To surpass strict scrutiny, STOP IT would have to be narrowly tailored as to not over-include or under-include any speech in its regulation. This is challenging because the Court has referenced narrow tailoring repeatedly when striking down speech restrictions.[211] The CDA and COPA both established a compelling state interest for their Acts to stop the spread of child pornography, but failed to pass the narrowly tailored version of the test because they overburdened adult speech while attempting to protect child speech.[212] In contrast, CIPA met the narrow tailoring standard because it served the goal of stopping the spread of indecent materials to minors by limiting the Act to apply to K-12 schools and libraries.[213] The Court found CIPA to be specific enough to target the eyes of children and stop them from viewing indecent materials.[214]

In order to not be under-inclusive or over-inclusive, STOP IT, like CIPA, would have to show how narrow of a category of speech it is impacting.[215] By defining terrorist speech as largely electronic representations of terrorist acts and active recruitment and solicitation by terrorist organizations, STOP IT is targeted at expression that itself is an act of terror.[216] STOP IT is not intended to stop members of the American press

206. *See* Hess v. Indiana, 414 U.S. 105, 108 (1973).

207. *See* Tom Hentoff, *Speech, Harm, and Self-Government: Understanding the Ambit of the Clear and Present Danger Test*, 91 COLUM. L. REV., 1453, 1456–59 (1991).

208. Eugene Volokh, *Freedom of Speech, Permissible Tailoring and Transcending Strict Scrutiny*, 144 U. PA. L. REV. 2417, 2417 (1996).

209. *See generally* Holder v. Humanitarian Law Project, 561 U.S. 1, 5 (2010); s*ee also* Chaplinksy v. New Hampshire, 315 U.S. 568, at 574 (1942); Schenck v. United States, 249 U.S. 47, 52–53 (1919).

210. *See, e.g.*, Reno v. Am. Civil Liberties Union, 521 U.S. 844, 875, 879 (1997).

211. *See* Richard H. Fallon, Jr., *Strict Judicial Scrutiny*, 54 UCLA L. REV. 1267, 1304 (2007) (quoting Gerald Gunther's epic "'strict' in theory and fatal in fact").

212. *Compare Reno*, 521 U.S. at 882 , *with* Ashcroft v. Am. Civil Liberties Union, 535 U.S. 564, 585 (2002).

213. *See* United States v. Am. Library Ass'n, Inc., 539 U.S. 194 (2003).

214. *Id*.

215. *See, e.g.*, *Reno*, 521 U.S. at 875, 879 .

216. *Contra* Reich, *supra* note 2.

from reporting their thoughts on ISIS, nor from posting about terrorist attacks generally, but is specifically targeted to stop online communications that promote and incite further terrorist action.[217] Factors that would contribute to the definition would include visual representations of violence and active communication with known international terrorist-based communities for the purpose of recruitment, such as ISIS.[218]

To surpass strict scrutiny, STOP IT would also need to remove terrorist speech from the Internet through the least restrictive means,[219] which begs the question of what other means could restrict this type of behavior? Could social media sites, like Twitter, simply continue enforcing their own take down policy?[220] It is likely this approach would be too individualistic, with videos being deleted on some sites and not others. Could the government educate American citizens on the dangers of ISIS recruitment techniques?[221] This approach would be even more intrusive into a citizen's daily life than blocking the action of the recruitment before most people know it is gone. Could the Act criminalize or fine Internet sites that hosted these videos?[222] Again, this approach is less tailored to achieving the stated goal because of the number of users on social media sites and the difference between the user of the site and the owner of the site. However, the Supreme Court would have to take a flexible view on the proposed legislation, as it did in *Humanitarian Law Project*, to uphold the Act under a traditional strict scrutiny analysis.

The Supreme Court's decision in *Humanitarian Law Project* may signal a willingness to assume a more flexible posture toward First Amendment scrutiny in the context of terrorism.[223] Without a strong discussion as to how the statute at issue specifically satisfied scrutiny, the Court held in *Humanitarian Law Project* that a content-based, national security material-support statute for foreign terrorist organizations did not violate the First Amendment.[224] Because the statute upheld in *Humanitarian Law Project* applied to lawful, nonviolent activities, the STOP IT Act might have an even stronger case for constitutionality, given that it targets unlawful, violent activities by international terrorist organizations.

---

217. *Id.*

218. *See generally* CBS DC, *supra* note 22.

219. *Id.*

220. *See* E.W., *Twitter, Terror and Free Speech: Should Twitter Block Islamic Snuff Videos?*, THE ECONOMIST:BLOG (Aug. 21, 2014, 11:17 AM), http://www.economist.com/blogs/democracyinamerica/2014/08/twitter-terror-and-free-speech [https://perma.cc/T8VA-FPRH].

221. *See* Ryan Reilly, *If You're Trying to Join ISIS Through Twitter, The FBI Probably Knows About It*, HUFFINGTON POST (July 9, 2015), http://www.huffingtonpost.com/2015/07/09/isis-twitter-fbi-islamic-state_n_7763992.html (examples of modern-day ISIS recruitment techniques) [https://perma.cc/N5X4-Q3MT].

222. As President Woodrow Wilson did with the Espionage Act of 1917. *See generally* 18 U.S.C. §§ 792–98 (2012).

223. *See* Tom Hentoff, *supra* note 13, at 1456–59. ; *see also* Holder v. Humanitarian Law Project, 561 U.S. 1, 36 (2010); Brandenburg v. United States, 395 U.S. 444, 446 (1944).

224. *See Humanitarian Law Project*, 561 U.S. at 36.

C. If STOP IT Were to Fail Constitutional Muster, an Alternative to this Act Would be the Creation of a Uniform "Code of Ethics" for Major Social Media Sites.

Given the modern, practical limitations on the actions of Congress and the harsh reality of the strict scrutiny test, a non-governmental method to address terrorist speech through voluntary action on behalf of social media sites themselves might be more viable, or desirable, as a backup solution. Most prominent sites already employ their own standards and codes of ethics articulating their ability to take down user content,[225] and some sites, such as Twitter, have specifically expressed their desire to adequately address the growing problem of terrorist speech.[226]

By creating their own universal "Terrorist Speech Code of Ethics," these media sources could band together to take down user content related to the categories discussed above: representations of acts of terrorism and active terrorist recruitment. The Office of Censorship during World War II establishes the precedent for a voluntary self-censorship program, with the exception that this would be privately, rather than publicly, introduced.[227] The benefits of a universal code would include more consistent and rigorous application in blocking these types of speech. A potential weakness of this approach would be dealing with the reality that some sites have less wealth and manpower than other sites to monitor this type of activity. These organizations, therefore, could create a committee to oversee all the involved social media sites as one coalition, or attempt to enforce the doctrines separately and measure the effectiveness on a month-to-month basis. Another benefit of this approach would be adaptability, as the potential coalition could adequately adjust any of its policies to meet the needs of the project. The first step in launching such an initiative would involve a meeting and discussion among the major social media platforms (e.g., Twitter, Facebook, YouTube, etc.) and take-down policy experts.[228]

V. CONCLUSION

The viral dissemination of James Foley's execution gave ISIS exactly the free publicity it was hoping for. America cannot continue to let this

---

225. *See, e.g.*, Community Guidelines, YOUTUBE, http://www.youtube.com/yt/policyandsafety/communityguidelines.html (last visited Mar. 27, 2017) [https://perma.cc/G3N3-Y4H8].

226. *See* Ryan Reilly, *If You're Trying to Join ISIS Through Twitter, the FBI Probably Knows About It*, HUFFINGTON POST (July 9, 2015, 3:32 PM EST), http://www.huffingtonpost.com/2015/07/09/isis-twitter-fbi-islamic-state_n_7763992.html [https://perma.cc/4CTR-EFQF].

227. *See* ROEDER, *supra* note 49, at 8.

228. *Compare Help Center: Abusive Behavior Policy*, TWITTER, https://support.twitter.com/articles/20169997, *with Community Guidelines*, YOUTUBE, http://www.youtube.com/yt/policyandsafety/communityguidelines.html [https://perma.cc/K4UA-PYK9].

content freely circulate in 2017. The historical practice of wartime censorship continues to exist as it has at least for the last two centuries.[229] The legal trend, although more protective of speech than not, continues to vacillate the shifting balance between liberty and order.[230] It is time for that censorship to take a more formal and transparent place in our legal system. Starting with the regulation of terrorist speech that directly represents an act of terror, the beheading of an American national, or the recruitment of American citizens to ISIS, should be within the discretion of the federal government to regulate. This regulation could start on social media sources, before expanding to other sources on the Internet to sufficiently tailor the regulation to the constraints of the First Amendment. Short of such ambitious legislation, however, a more realistic plan for curtailing online terrorist speech would be to spur major social media sites to develop a voluntary, uniform "Code of Ethics" addressing the issue.[231]

229. *See* discussion *supra* Section II(B).
230. *See* HALLIN, *supra* note 12, at 215.
231. *See* discussion *supra* Section III(C).

Let Me Tell You Who I Am: Establishing a Federal Remedy for Interference with Online Identity

Laura K. Hamilton*

TABLE OF CONTENTS

* J.D., The George Washington University Law School, May 2017. Senior Publications Editor, *Federal Communications Law Journal*, 2016–17. B.A., History with Honors, Minors in Middle Eastern Studies & French, New York University, 2011. This Note is dedicated to the late Jill N. Claster of New York University, to whose grace, wit, and intelligence I will always aspire. The author would also like to thank Professors Peter J. Smith and Orin Kerr of The George Washington University Law School for shepherding this Note's thesis along (knowingly or not). Special thanks goes to Mona Sedky and the prosecutors of the Computer Crime & Intellectual Property Section of the Department of Justice. The author would also like to recognize Dr. Holly Jacobs for her continuing work on behalf of victims.

I. FOREWORD

Since this Note's conception in the fall of 2015, the politics of online speech have changed dramatically. As of January 2017, the specter of a weakened First Amendment continues to spur debate—with the press, in particular, being admonished.[1] At the same time, women's rights and sexual freedoms have also become increasingly controversial.[2] Striking the proper balance between protecting individual rights and buttressing the First Amendment has never been more important. Accordingly, this Note argues that this delicate balance can, and should, be struck by careful and comprehensive federal legislation.

II. INTRODUCTION

The Internet disrupts. From Fort Meade to Silicon Valley, concerns about online identity resonate. Can members of "Anonymous" remain truly anonymous?[3] What happens when Twitter can't verify a person's identity?[4] Will there come a time when we can no longer separate fact from fiction on the Internet?

A distinct personal identity and the right to reinvention are quintessential American ideals. In 2015, the New York Times published an article branding that year "The Year We Obsessed Over Identity."[5] As the Internet becomes increasingly intertwined with all aspects of human life—such as medical care, shopping lists, mobile payments, travel documents—it is becoming increasingly difficult to separate a person's online identity from who the person is in the physical world. For most Internet users, it is unlikely

---

1. *See, e.g.*, Stephen Collinson, *Trump takes aim at First Amendment*, CNN (Nov. 30, 2016, 7:34 AM EDT), http://www.cnn.com/2016/11/29/politics/donald-trump-first-amendment [https://perma.cc/TQA4-36L4]; Michael M. Grynbaum, *Trump Strategist Stephen Bannon Says Media Should 'Keep Its Mouth Shut'*, N.Y. TIMES (Jan. 26, 2017), https://www.nytimes.com/2017/01/26/business/media/stephen-bannon-trump-news-media.html [https://perma.cc/WSQ5-4Q9R].

2. *See, e.g.*, Yamiche Alcindof & Susan Chira, *Defiant Voices Flood U.S. Cities as Women Rally for Rights*, N.Y. TIMES (Jan. 21, 2017), https://www.nytimes.com/2017/01/21/us/women-march-protest-president-trump.html [https://perma.cc/RC6Q-YPLA]; Jeremy W. Peters, *Trump on Their Side, Conservatives See Hope in Lengthy Abortion Fight*, N.Y. TIMES (Jan. 26, 2017), https://www.nytimes.com/2017/01/26/us/politics/democrats-republicans-planned-parenthood.html [https://perma.cc/MGN5-DH6A].

3. *See*, *e.g.*, Betsy Isaacson, *7 Anonymous Hackers Who Have Been Unmasked*, HUFFINGTON POST (Jun. 7, 2013), http://www.huffingtonpost.com/2013/06/07/anonymous-hackers_n_3398282.html [https://perma.cc/R6QC-3U3W].

4. *See, e.g.*, Rebecca Greenfield, *The Ethics of Fake Twitter Accounts*, WIRE (Feb. 1, 2012), http://www.thewire.com/technology/2012/02/learning-cormac-mccarthy-twitter-hoax/48147 [https://perma.cc/FAZ9-BDNG].

5. Wesley Morris, *The Year We Obsessed Over Identity*, N.Y. TIMES MAGAZINE (Oct. 6, 2015), http://www.nytimes.com/2015/10/11/magazine/the-year-we-obsessed-over-identity.html [https://perma.cc/T3BH-UY6Z].

that these two identities will differ significantly.[6] When individuals suffer from non-consensual pornography ("NCP"), popularly known as "revenge porn," separating offline fact from online fiction is difficult, expensive, and often impossible.[7] This Note will focus on the novel harms arising out of our dependency on the Internet, examine the current legislative landscape in the United States, and recommend that a federal statute should provide a remedy for individuals whose online identities are maliciously compromised.

There are two general categories of harm that flow from tampering with online identity: (1) reputational harm, and (2) "historical" harm. Reputational harm concerns "true" statements that,[8] due to the Internet's unparalleled ability to reach a global audience, are expanded beyond their original scope such that the individual's reputation in the broader community is denigrated disproportionately. The consequences of reputational harm on an individual can be economic (e.g., job loss[9]), as well as emotional and physical (e.g., loss of friendships, depression,[10] and even suicide[11]).

"Historical" harm, by contrast, concerns "false" online facts substituted for the offline truth, such that consumers of this information are unable to parse historical reality from fantasy. In extreme cases, individuals relying on

---

6. Tomas Chamorro-Premuzic, *How Different are Your Online and Offline Personalities?*, GUARDIAN (Sept. 24, 2015), https://www.theguardian.com/media-network/2015/sep/24/online-offline-personality-digital-identity [https://perma.cc/UP2D-ZD4S] ("[O]nline activities are no longer separable from our real lives, but an integral part of it.").

7. Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 346 (2014). This is fundamentally distinct from the idea of "poster's remorse," where an Internet user comes to regret something they have voluntarily uploaded. Lance Whitney, *Poster's remorse common for social-network users*, CNET (May 18, 2010, 11:03 AM), http://www.cnet.com/news/posters-remorse-common-for-social-network-users [https://perma.cc/EA33-E8U7]. Though some scholars have made compelling arguments to counteract the Internet's perfect memory by integrating an expiration date for information, for example, and the European Union has instituted the "Right to be Forgotten"— that discussion is regrettably outside the scope of this Note. *See, e.g.*, Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN [https://perma.cc/V4ZE-27HW]; VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 15 (4th prtg. 2011); *see also Factsheet on the "Right to be Forgotten" Ruling (C-131/12)*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf [https://perma.cc/2N97-P547] (last visited Apr. 6, 2016).

8. There is much ongoing controversy, especially in a First Amendment context, on the question of how much the law can dictate what is "true" online. Given the potentially endless breadth of this topic, what online speech should qualify as "true" is not discussed. *See generally* Yasmine Agelidis, Note, *Protecting the Good, the Bad, and the Ugly: "Exposure" Data Breaches and Suggestions for Coping with Them*, 31 BERKELEY TECH. L.J. 1057, 1057 (2016).

9. *See* Jon Ronson, *How One Stupid Tweet Blew Up Justine Sacco's Life*, N.Y. TIMES MAGAZINE (Feb. 12, 2015), http://www.nytimes.com/2015/02/15/magazine/how-one-stupid-tweet-ruined-justine-saccos-life.html [https://perma.cc/92ZF-79EH].

10. *See id.*

11. Michelle Dean, *The Story of Amanda Todd*, NEW YORKER MAGAZINE (Oct. 18, 2012), http://www.newyorker.com/culture/culture-desk/the-story-of-amanda-todd [https://perma.cc/F4MP-P643].

false online information have committed violent crimes.[12] There is often an overlap between the two categories: NCP could be considered reputational harm, for the original photographs are generally consensual, and it may also be considered historical harm, as the original photos can be altered in Photoshop or posted alongside false statements. Clearly delineating the types of harm the federal statute is designed to prevent is crucial to understanding the feasibility of introducing legislation.

The most obvious and important obstacle to such legislation is the First Amendment. It is also important to recognize and appreciate that the First Amendment plays a crucial role in cabining laws that seek to control activity and speech on the Internet.[13] But the First Amendment does not fully protect defamation or libel, and the Supreme Court has ruled that a private figure need not demonstrate malice in a defamation suit in order to recover.[14]

In the United States, we are increasingly concerned with historical harm arising out of NCP, identity theft, and data privacy.[15] Section III of this Note will examine the landscape of existing legislation and explain the development of applicable tort law, ultimately concluding that neither is sufficient to address modern harms. Section IV will propose a recommendation for enacting comprehensive federal legislation. Recognizing the Internet's broad scope, the need for uniformity across state lines, and the current lack of redressability for actual harm, the proposed federal statute will allow for both civil and criminal causes of action to protect individuals from malicious interference with their online identity.

III. BACKGROUND

"Right or wrong, the [I]nternet is a cruel historian."[16] The twenty-first century has been characterized by a perfect storm of identity information technology. With the emergence of Facebook, a billion users logged on "in a single day" in 2015 to interact on a website not dissimilar to an online Rolodex.[17] Sergey Brin and Larry Page developed a smart search engine in Google that aims to provide users with more accurate and more detailed

12. *See* DeeDee Correll, *Former boyfriend used Craigslist to arrange woman's rape, police say*, L.A. TIMES (Jan. 11, 2010), http://articles.latimes.com/2010/jan/11/nation/la-na-rape-craigslist11-2010jan11 [https://perma.cc/FWD3-4EHY].

13. While the Supreme Court has not directly addressed this proposition, it is widely presumed and for purposes of this Note not especially controversial. *See* Reno v. ACLU, 521 U.S. 844, 870 (1997) ("[O]ur cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to [the Internet].").

14. *See* David S. Ardia, *Reputation in a Networked World: Revisiting the Social Foundations of Defamation Law*, 45 HARV. C.R.-C.L. L. REV. 261, 281 (2010) (citing Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749 (1985)).

15. *See, e.g.*, Citron & Franks, *supra* note 7; *see also* Alina Tugend, *Oh, No! My Identity's Gone! Call the Insurer.*, N.Y. TIMES:BUSINESS DAY (May 28, 2005), http://www.nytimes.com/2005/05/28/business/oh-no-my-identitys-gone-call-the-insurer.html?_r=0 [https://perma.cc/AW56-Z8VF].

16. DANIEL J. SOLOVE, THE FUTURE OF REPUTATION, GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 11 (2007).

17. Mark Zuckerberg, FACEBOOK (Aug. 27, 2015, 4:33pm), https://www.facebook.com/zuck/posts/10102329188394581 [https://perma.cc/53L3-62ZC].

information than ever before.[18] The inevitable result is that more information about a person's online identity is readily available, with an extraordinarily low barrier to entry. And, in a post-Snowden world, many Americans no longer expect privacy in online communications[19], whatever the federal courts may hold.[20] Once information is disseminated online, it is impossible to take back.[21] As a fictionalized Erica Albright, Mark Zuckerberg's ex-girlfriend, declares in *The Social Network*, "the Internet's not written in pencil, Mark, it's written in ink."[22] The Internet is permanent.[23]

A. Modern Problems Mandate Modern Solutions

NCP is a quintessential example of malicious interference with online identity that encompasses both reputational and historical harm. In November 2011, Holly Jacobs received an anonymous email stating, "someone is trying to make life very difficult for you."[24] The email contained a link to a site that

---

18. *What We Do*, GOOGLE, https://www.google.com/about/company/products [https://perma.cc/XTN6-LMJK] (last visited Feb. 27, 2016).

19. *See, e.g.*, Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RES. CTR. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ [https://perma.cc/D5GK-5C2Z] (finding 91% of those surveyed "agree" or "strongly agree" that consumers have lost control over how personal information is collected or used by companies); Timothy J. Geverd, *Bulk Telephony Metadata Collection and the Fourth Amendment: The Case for Revisiting the Third-Party Disclosure Doctrine in the Digital Age*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 191, 193 ("[I]n the wake of the Edward Snowden leaks, federal courts will be forced to consider the continued vitality of the third-party disclosure doctrine in today's technological age."); John Levin, *The Cloud and the NSA*, C2014BA Rec., April/May , at 38 ("I believe that Snowden's disclosures make it safe to say that nothing that is transmitted through or stored in the cloud is confidential.").

20. *Compare* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (holding that a reasonable expectation of privacy exists in the contents of email communications), *with* Rehberg v. Paulk, 598 F.3d 1268, 1281 (11th Cir. 2010) ("A person also loses a reasonable expectation of privacy in emails, at least after the email is sent to and received by a third party."), *vacated on panel reh'g on other grounds*, 611 F.3d 828 (11th Cir. 2010).

21. *See, e.g.*, Ronson, *supra* note 9; Katie Mettler, *What Rob Kardashian did to Blac Chyna could be 'revenge porn,' lawyers say, and illegal*, WASH. POST (July 6, 2017), https://www.washingtonpost.com/news/morning-mix/wp/2017/07/06/what-rob-kardashian-did-to-blac-chyna-could-be-revenge-porn-lawyers-say-and-illegal/ [https://perma.cc/FWL4-MHC4] ("Even though Instagram quickly shut down his account, Kardashian managed to move the rant and nude photos temporarily to Twitter, before that social platform also blocked the revealing photo. But just within the few minutes the nude picture was online, it got thousands of retweets and was likely screenshot just as many times . . . .").

22. THE SOCIAL NETWORK (Columbia Pictures 2010). Though Erica Albright is a real person, the quote is fictional. It does, however, perfectly encapsulate a common theme in modern Internet use. Other commentators have been less artful. As Chief Judge Kozinski of the Ninth Circuit described it: "They say that removing something from the internet is about as easy as removing urine from a swimming pool, and that's pretty much the story." Alex Kozinski, Symposium Keynote, *The Dead Past*, 64 STAN. L. REV. ONLINE 117, 124 (Apr. 2012).

23. *See* MAYER-SCHÖNBERGER, *supra* note 7, at 68–69 ("[I]t is obvious that not just individuals, but private as well as public organizations, too, experience the consequences of permanent comprehensive memory.").

24. *See* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 45 (2014).

hosted nude photos of her and an explicit video taken during a former relationship.[25] Googling her name revealed the images appeared on hundreds of other sites as well.[26] Perhaps the most horrifying detail, however, was that the posts were not limited to revealing photos, but also included contact information about her offline identity, such as her full name, email address and Facebook page.[27] When Jacobs initially approached the Miami police and the FBI, both disclaimed the existence of any legal remedies, despite several federal laws criminalizing cyberstalking and online harassment.[28] At a loss, she even resorted to copyright law by sending the linking websites takedown notices, arguing she was the original creator and owner of the nude photographs.[29]

In exposing sensitive photographs to the Internet, NCP causes reputational harm in publishing "true" facts (real photographs of a victim's naked body) to a broader audience than intended, creating negative social and economic consequences.[30] And though the fact of the photograph may be true, its context may not be; historical harm can occur, for example, by posting NCP alongside an allegation that the victim consented to its disclosure, or that he or she has certain sexual preferences or proclivities.[31]

In Holly Jacobs's case, Googling her name after the original images were uploaded almost exclusively brought up results of the nude photos and video.[32] As a PhD candidate who also taught undergraduate students, Jacobs worried that her professional future would be forever compromised; she legally changed her name, asking for a seal to be placed on her records, only to have the motion to seal (including both names) posted online by the county.[33] Her online identity was shattered. But the online abuse crept into her offline life when Jacobs was forced to cancel her thesis presentation for the American Psychological Association after someone reposted the nude photos alongside the date, time, and location of her talk.[34] Not only was it embarrassing to have her photos and video posted online, but prospective employers might have trouble differentiating between Holly Jacobs, PhD, and "Holly Jacobs," anonymous sex addict. How would the employer know which identity was "real"? And how likely is it that an employer would ever give her a chance to explain, instead of taking the path of least resistance and moving on to the next resume in the pile?

---

25. *See id.*
26. *See id.*
27. *See id.*
28. *See id.* at 46–47.
29. *See id.*
30. LastWeekTonight, *Online Harassment: Last Week Tonight with John Oliver (HBO)*, YOUTUBE (Jun. 21, 2015), https://www.youtube.com/watch?v=PuNIwYsz7PI [.
31. *See, e.g.*, Bekah Wells, *An Involuntary Pornstar: My Story*, WOMEN AGAINST REVENGE PORN, (Mar. 30, 2016), http://www.womenagainstrevengeporn.com/#!An-Involuntary-Pornstar-My-Story/c618/6151C735-CEEF-45B2-A175-AC3E61347B3A [https://perma.cc/UC4Q-E24F] (last visited Apr. 8, 2016).
32. *See* CITRON, *supra* note 24, at 45–47.
33. *See id.* at 48.
34. *See id.* at 49.

Jacobs founded the "End Revenge Porn" campaign in 2012,[35] and now heads a non-profit called the "Cyber Civil Rights Initiative," dedicated to "advocating for state and federal legislative" reforms.[36] Since she began her advocacy work, thirty-five states (and the District of Columbia) have initiated anti-NCP laws and many more have legislation pending.[37]

Unlike Dr. Jacobs, Anita Sarkeesian's ability to get hired does not depend on her Google search results, since she is self-employed.[38] However, like Dr. Jacobs, Sarkeesian is a victim of NCP of a slightly different variety. Sarkeesian is an avid video gamer, media critic, and activist with a popular YouTube channel called "Feminist Frequency."[39] She has garnered over 220,000 followers, posted nearly ninety YouTube videos deconstructing anti-feminist tropes in games, and her videos have tallied over twenty-six million views.[40] In 2012, when Sarkeesian launched the Kickstarter campaign to fund her now-successful YouTube channel, she received violent personal threats as well as Photoshopped pornographic images of herself.[41] These images were not versions of originals she had shared consensually, but rather what she called "image based harassment," including vulgar photo manipulation and creating pornographic or degrading drawings of rape or sexual assault with the target's likeness.[42] Just two years later, one of her videos, "Women as Background Decoration,"[43] attracted the attention of angry Internet users who sent serious enough threats that Sarkeesian fled her home as a result.[44] The threats continued, escalating to the point that Sarkeesian cancelled a talk she was scheduled to give at Utah State University after receiving a "terror threat" that promised to perpetrate "the deadliest school shooting in American history."[45]

---

35. *About*, CYBER CIVIL RIGHTS INITIATIVE, http://www.cybercivilrights.org/welcome (last visited Apr. 8, 2016).

36. *Our Mission*, CYBER CIVIL RIGHTS INITIATIVE, http://www.cybercivilrights.org/about (last visited Apr. 8, 2016).

37. *See 35 STATES + DC HAVE REVENGE PORN LAWS*, CYBER CIVIL RIGHTS INITIATIVE, https://www.cybercivilrights.org/revenge-porn-laws/ [https://perma.cc/UHQ7-5VGS] (last visited Apr. 15, 2017).

38. *Biography*, *infra* note 39.

39. *See Biography*, ANITASARKEESIAN.COM, http://www.anitasarkeesian.com/media-kit/ [https://perma.cc/73R2-A5NH] (last visited Feb. 6, 2017) [hereinafter *Biography*].

40. *See* feministfrequency, *About*, YOUTUBE, https://www.youtube.com/user/feministfrequency/about (last accessed Feb. 20, 2017).

41. *See* Amy O'Leary, *In Virtual Play, Sex Harassment Is All Too Real*, N.Y. TIMES (Aug. 1, 2012), http://www.nytimes.com/2012/08/02/us/sexual-harassment-in-online-gaming-stirs-anger.html [https://perma.cc/YMK9-ZHAB].

42. Anita Sarkeesian, *Image Based Harassment and Visual Misogyny*, feministfrequency (July 1, 2012), https://feministfrequency.com/2012/07/01/image-based-harassment-and-visual-misogyny/ [https://perma.cc/TZ6Y-S823].

43. feministfrequency, *Women as Background Decoration: Part 2 – Tropes vs. Women in Video Games*, YOUTUBE (Aug. 25, 2014), https://youtu.be/5i_RPr9DwMA.

44. *See* Anna North, *Why a Video Game Critic Was Forced to Flee Her Home*, N.Y. TIMES: OP TALK (Aug. 29, 2014, 11:34 AM), http://op-talk.blogs.nytimes.com/2014/08/29/why-a-video-game-critic-was-forced-to-flee-her-home [https://perma.cc/LN4J-WYM3].

45. *See* Soraya Nadia McDonald, *'Gamergate': Feminist video game critic Anita Sarkeesian cancels Utah lecture after threat*, WASH. POST (Oct. 15, 2014),

Luckily for Sarkeesian, she has developed a large enough public persona through her YouTube channel that it is unlikely a prospective employer would believe the Photoshopped images to be real. But this is no consolation for the vast majority of everyday victims. Sarkeesian may be less likely to suffer permanent historical harm where a quick Google search of her name yields a substantive Wikipedia page with coverage detailing her online harassment.[46] But, her reputational harm persists; Sarkeesian has had to warn her neighbors that they might see some "shady" characters around the building due to her continued notoriety.[47] Participating in a June 2017 panel at VidCon about women's online experiences, Sarkeesian was confronted by her online harassers, who sat in the front two rows filming her.[48] One of those harassers later posted a video to YouTube about their planned presence, crowing, "[w]e had a blast with this."[49] Sarkeesian herself commented on the parallels between her treatment during the "GamerGate" scandal and the increase in internet vitriol during and after the 2016 presidential election.[50]

B. American Torts & the Development of Information Privacy

The modern conception of information privacy begins with Samuel Warren and Louis Brandeis' 1890 treatise *The Right to Privacy*.[51] Warren and Brandeis were primarily concerned with reputational harm, where journalists' invasion of private and domestic life could cause emotional distress and

---

https://www.washingtonpost.com/news/morning-mix/wp/2014/10/15/gamergate-feminist-video-game-critic-anita-sarkeesian-cancels-utah-lecture-after-threat-citing-police-inability-to-prevent-concealed-weapons-at-event [https://perma.cc/4LGG-85V6].

46. *Anita Sarkeesian*, WIKIPEDIA, https://en.wikipedia.org/wiki/Anita_Sarkeesian [https://perma.cc/AS3W-8226] (last visited Apr. 8, 2016). Notably, Sarkeesian's Wikipedia page has been locked from editing by the community after it was vandalized in response to her project against anti-feminist video game tropes, which is arguably the definition of historical harm. *See* Angela Watercutter, *Feminist Take on Games Draws Crude Ridicule, Massive Support*, WIRED (June 14, 2012, 6:30 AM), http://www.wired.com/2012/06/anita-sarkeesian-feminist-games [https://perma.cc/4SGE-U8K7].

47. Todd Martens, *Video game critic Anita Sarkeesian's Web series 'Ordinary Women' to reveal little-known stories*, L.A. TIMES (Apr. 6, 2016, 4:53 PM), http://www.latimes.com/entertainment/herocomplex/la-et-hc-anita-sarkeesian-20160407-story.html [https://perma.cc/BHN7-EGWL].

48. Lindy West, *Save Free Speech From Trolls*, N.Y. TIMES: SUNDAY REV. (July 1, 2017), https://www.nytimes.com/2017/07/01/opinion/sunday/save-free-speech-from-trolls.html [https://perma.cc/E3WK-5F32].

49. Colin Campbell, *Anita Sarkeesian's astounding 'garbage human' moment*, POLYGON (June 27, 2017), https://www.polygon.com/features/2017/6/27/15880582/anita-sarkeesian-garbage-human-vidcon-interview [https://perma.cc/6QYS-YRNU].

50. *See* Anita Sarkeesian, *Understand the Power of Untapped Technology*, REFINERY29 (Jan. 19, 2017), http://www.refinery29.com/2017/01/136447/women-empowerment-trump-presidency-essays [https://perma.cc/28CR-FDYJ]; *see also* Martens *supra* note 47 at 3–4 (stating "GamerGate" "rose to prominence in mid-2014 and became an Internet hashtag championed by those who feared that any sort of cultural criticism about games . . . would result in some sort of politically correct makeover of the medium.").

51. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); *see also* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 17 (2015) ("It came to define not just the field of privacy law but also popular understandings of what privacy means.").

psychological injury.[52] At the time, the idea that a plaintiff should recover for purely emotional harm was a radical one.[53] For 125 years, lawyers have worried about the effect of new media technology on reputation, and the advent of the Internet has only accelerated these concerns. Although Warren and Brandeis have been labeled "elitists" for seeking emotional damages on behalf of the upper class, whom viewed gossip as a threat to class dignity, this traditional calculus has been upended.[54] Now the class of individuals for whom an interference with identity would be most damaging is not the elite or famous, who already occupy sizable portions of the Internet and have armies of social media publicists. While celebrities face a larger potential audience when their nude photos are uploaded to the Internet, for example, their identity rehabilitation is considerably easier due to a powerful preexisting reputation.[55] Reputational and historical harms are most damaging to the public who operates neither entirely offline nor online. Entirely offline individuals can avoid online reputational harm because their local communities are less likely to be confused—for example, an individual who has never joined Facebook can more easily argue that a Facebook account in their name is purely false. Fully online individuals with substantive and long histories of social media presence may defeat reputational and historical harms by simply continuing to create content such that negative search results decrease in proportion to in their social media presence.[56] But for those whose online presence is not deeply established prior to their victimization by NCP, it may be much more difficult to limit the negative consequences to their community reputation and historical identity. Where Warren and Brandeis worried about the reputational damage that might follow a newspaper gossip column, what happens now that Google's memory is nearly perfect? What rights, if any, does an individual have to her online identity?

Seventy years later, William Prosser refined the Warren and Brandeis conception of privacy by delineating the four distinct privacy torts commonly known today: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light; and (4) appropriation of likeness.[57] This quad-furcation of the unitary privacy right has throttled common law progression alongside technology that doesn't fit neatly into any single category, rather than

52. *See* RICHARDS, *supra* note 51, at 18.

53. *See id.*

54. *See id.* at 19.

55. Without making light of her experience, Jennifer Lawrence, for example, has fully recovered her positive reputation since her nude photos were leaked online in 2014. *See, e.g.*, Jonathan Van Meter, *Jennifer Lawrence is Determined, Hilarious, and—Above All—Real*, VOGUE (Nov. 11, 2015, 9:48 PM), http://www.vogue.com/13368193/jennifer-lawrence-december-2015-cover-hunger-games [https://perma.cc/KFZ2-6LJW].

56. *See id.*

57. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1733 (2010) (citing William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960)); RESTATEMENT (SECOND) OF TORTS § 652B (1977) (Intrusion upon Seclusion)).

allowing courts to gradually respond to changing circumstances.[58] It has also had the effect of condensing breach of privacy concerns into a checklist, rather than focusing on the specific right to be protected.[59] And because these torts have offered few protections for modern victims of NCP, [60] for example, it is difficult to see how adherence to the old regime will be flexible enough to tackle new problems.

Although "tort law is traditionally a matter of state law,"[61] the Internet is by nature multi-jurisdictional,[62] and basic principles of fairness and uniformity suggest that a federal remedy is needed. In a criminal case, venue can be problematic where, for example, the perpetrator of NCP lives in Florida but their victim lives in California.[63] The nuances of each state's online identity protection laws and long-arm statutes could also lead to vastly dissimilar results; a federal statute has the benefit of establishing a bright line rule which can be broadly applied. The Supreme Court has yet to rule on the proper jurisdictional test for personal jurisdiction over the Internet, however, the Court of Appeals for the Ninth Circuit has formulated a prototypical approach: applying *Calder v. Jones,*[64] "personal jurisdiction can be based upon: (1) intentional actions (2) expressly aimed at the forum state (3) causing harm, the brunt of which is suffered—and which the defendant knows is likely to be suffered—in the forum state."[65] This test, however, requires a level of purposeful targeting that is at odds with modern Internet usage; the

58. *See* Robert M. Connallon, *An Integrative Alternative for America's Privacy Torts*, 38 GOLDEN GATE U.L. REV. 71, 86–87 (2007) ("[T]he development of privacy-tort law has been devoid of doctrinal adjustments that would allow courts to respond to new conditions.").

59. *Id.* at 88.

60. In one of the few encouraging examples, a Colorado woman obtained a judgment against her ex-boyfriend for intentional infliction of emotional distress, but the court declined to evaluate her intrusion upon seclusion claim, finding it duplicative of the underlying facts alleged in the IIED claim. The court did, however, allow the public disclosure of private facts claim. *See* Doe v. Hofstetter, No. 11-CV-02209-DME-MJW, 2012 WL 2319052, at *7–9 (D. Colo. June 13, 2012). As an unpublished decision, however, it is of no precedential value.

61. Mary Wood, *O'Connell, A Pioneer of Insurance Law, Retires from Law School, University of Virginia School of Law* (May 10, 2012), http://content.law.virginia.edu/news/2012_spr/oconnell_retirement.htm [https://perma.cc/HML4-UQER].

62. *See, e.g.*, Dan L. Burk, *Jurisdiction in a World Without Borders*, 1 VA. J. L. & TECH. 3, 10 (1997) ("There is no centralized control of the packet routing, or for that matter, of almost any other aspect of the Internet.").

63. *See id.* at 22 ("The government may have wide latitude in deciding where to bring a prosecution against alleged on-line offenders, as the nature of the Internet is to facilitate contact between many jurisdictions, and elements of the offense may conceivably have been initiated, completed, or furthered not only where the defendant was physically located, but in all the jurisdictions that his actions electronically touched."); *see also* United States v. Rowe, 414 F.3d 271, 277–80 (2d Cir. 2005) (finding venue in the Southern District of New York proper despite the fact that defendant resided in and used his computer to post the child pornography advertisement in the Eastern District of Kentucky).

64. *See generally* Calder v. Jones, 465 U.S. 783 (1984) (establishing the "effects test" for personal jurisdiction).

65. 4A CHARLES ALAN WRIGHT ET AL., FEDERAL PRACTICE AND PROCEDURE § 1073 (4th ed.) (quoting Panavision Int'l., L.P. v. Toeppen, 141 F.3d 1316 (9th Cir. 1998), *modified on other grounds by* Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme, 443 F.3d 1199 (9th Cir. 2006)).

structure of the interconnected Internet makes it impossible to control where all of a user's data goes, short of staying off the Internet entirely.[66] To establish a federal tort-like remedy for interference with online identity, it is necessary to return to the historical unitary cause of action and center it around the protected right: online identity.[67]

C. Criminal Law: Non-Consensual Pornography and Cyberstalking

Civil remedies do not stand alone. Criminal penalties have also been levied against perpetrators of interference with online identity. The Philippines was the first country to criminalize NCP in 2009.[68] In the United States, California is considered a leader in online criminal legislation and anti-NCP laws[69]; New Jersey, however, was both the first state to criminalize NCP and the first to convict for its distribution.[70] As of this writing, thirty-five states and the District of Columbia have anti-revenge porn laws.[71] Of those, New Jersey's statute has been rarely used,[72] and California's statute classifies revenge porn as a disorderly conduct misdemeanor.[73] Notably, the District of Columbia's law makes publication of NCP a felony punishable by up to three years in prison, though it also includes a misdemeanor subsection.[74] Only California has amended its state constitution to include a right to privacy.[75]

---

66. *See* Burk, *supra* note 62, at 50.

67. *See* Cristina Carmody Tilley, *Rescuing Dignitary Torts from the Constitution*, 78 BROOK. L. REV. 65, 70 (2012) ("Historically, the dignitary torts were treated as a unitary cause of action, protecting a key component of personal security—namely, interests in individual personality. The fracturing of this interest into distinct torts has marginalized the underlying interest they protect.").

68. Mary Anne Franks, *The Fight Against Digital Abuse: The View from the US*, WOMEN'S AID (Dec. 15, 2015 12:25 PM), http://www.womensaid.ie/16daysblog/2015/12/15/the-fight-against-digital-abuse-the-view-from-the [https://perma.cc/E8C2-QVNX].

69. *See generally California Online Privacy Protection Act*, CONSUMER FED'N CAL.: EDUC. FOUND., https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/ [https://perma.cc/LU2U-UP27] (last accessed Apr. 2, 2017).

70. *See* Paul J. Larkin, Jr., *Revenge Porn, State Law, and Free Speech*, 48 LOY. L.A. L. REV. 57, 94–95 (2014); *see also* State v. Parsons, 2011 WL 6089210 (N.J. Super. Ct. App. Div. Dec. 8, 2011).

71. CYBER CIVIL RIGHTS INITIATIVE, *supra* note 35.

72. *See* Paul J. Larkin, Jr., *Revenge Porn, State Law, and Free Speech*, 48 LOY. L.A. L. REV. 57, 95 (2014) (noting the statute was also used against the roommate of Tyler Clementi, the Rutgers University student who committed suicide after the roommate live broadcasted Tyler and another man having consensual sex).

73. *See* CAL. PENAL CODE § 647(j)(4) (West 2017).

74. D.C. CODE § 22–3053 (West 2015); *see also* Keith L. Alexander, *D.C. man becomes first to be convicted under District's new revenge porn law*, WASH. POST (Apr. 19, 2017), https://www.washingtonpost.com/local/public-safety/dc-man-becomes-first-to-be-convicted-under-districts-new-revenge-porn-law/2017/04/19/2e6ab4ca-2516-11e7-b503-9d616bd5a305_story.html?utm_term=.44dd6f5a2603 [https://perma.cc/J5UC-NHPQ].

75. *See* CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.").

This state constitutional right has been extended to some aspects of digital privacy, but its development has been far from straightforward.[76] While promising, this approach is necessarily limited to California residents or to individuals with deep enough pockets to pursue litigation in the venue of the perpetrator. And although California recently announced its first conviction under its anti-NCP statute,[77] the piecemeal protection of various rights afforded by state tort law is, at best, insufficiently flexible to adapt to changing technologies. As Holly Jacobs's experience demonstrates, local state and federal law enforcement is often unfamiliar with or unwilling to research the remedies already available to victims.[78]

In contrast to the patchwork state approach, there is no federal anti-revenge porn law. United States House Representative Jackie Speier was set to introduce a federal bill in late 2015,[79] but it has yet to cross the House floor. Previous attempts to legislate at the federal level have faced strong opposition from free speech advocates, and on fundamental issues like whether NCP should even be considered a criminal act.[80] Given the ambivalence in even progressive political circles,[81] which are more likely to support a bill, it seems unlikely that such legislation will be taken up seriously for some time. However, the realistic pace of a historically unproductive Congress should not factor into the equation of whether these harms *should* be redressed. A federal statute criminalizing behavior that impermissibly interferes with an online identity would effectively deter several types of offenses that plague Internet use in society today.

Despite the lack of federal action to criminalize NCP, cyberstalking and child pornography are established federal crimes whose underlying statutes may provide a model for a federal statute concerned with online identity.[82]

---

76. *See* White v. Davis, 533 P.2d 222, 233–35 (Cal. 1975) (looking to text of voter advocate brochures to determine whether constitutional amendment was intended to extend to information privacy).

77. *See* Veronica Rocha, *'Revenge porn' conviction is a first under California law*, L.A. TIMES, (Dec. 4, 2014, 5:00 PM), http://www.latimes.com/local/crime/la-me-1204-revenge-porn-20141205-story.html [https://perma.cc/9SRH-6PFM].

78. *See* CITRON, *supra* note 24, at 41.

79. *See* Lydia Wheeler, *Lawmaker eyes 'revenge porn' crackdown*, HILL (Jul. 15, 2015 6:00 AM), http://thehill.com/regulation/247954-lawmaker-eyes-revenge-porn-crackdown [https://perma.cc/A4VX-SULY].

80. *See* Kaveh Waddell, *Bill to Criminalize Revenge Porn Coming After Recess*, NAT'L J. (Aug. 12, 2015, 1:00 AM) (quoting an ACLU staff attorney as saying: "[w]e don't use criminal law to remedy humiliation"), https://www.nationaljournal.com/s/70267 [https://perma.cc/W8CT-UGZB].

81. *Compare* Mary Anne Franks, *The ACLU's Frat House Take on 'Revenge Porn'*, HUFFINGTON POST, http://www.huffingtonpost.com/mary-anne-franks/the-aclus-frat-house-take_b_6980146.html [https://perma.cc/535L-Z234] (Apr. 1, 2015 1:23 PM) (criticizing the ACLU's opposition to state revenge porn legislation), *with* Lee Rowland, *VICTORY! Federal Judge Deep-Sixes Arizona's Ridiculously Overbroad 'Nude Photo' Law*, ACLU (July 10, 2015 6:45 PM), https://www.aclu.org/blog/speak-freely/victory-federal-judge-deep-sixes-arizonas-ridiculously-overbroad-nude-photo-law [https://perma.cc/URL8-SR6P] (defending ACLU's stance on "opposing laws that chill or criminalize protected speech, even when we condemn the conduct that well-meaning legislators are trying to target").

82. *See generally* Naomi Goodno, *Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 MO. L. REV. 125, 127–28 (2007).

The Violence Against Women Reauthorization Act of 2013 ("VAWA") amended the federal cyberstalking statute to include harsher sentences.[83] However, the Supreme Court struck down the part of the original VAWA that allowed victims to sue their attackers for damages in federal court.[84] The Court reasoned that "[t]he Constitution requires a distinction between what is truly national and what is truly local."[85] But since 2000, when *United States v. Morrison* was decided, Internet access has permeated the country to an extent unanticipated by Chief Justice Rehnquist's opinion.[86] The federal Circuits have disagreed on whether the Internet is more properly described as a channel or instrumentality of interstate commerce, or both, under the Commerce Clause.[87]

Most of these decisions have arisen in the context of child pornography cases, in which the defendants have used the Internet to store or obtain criminal images.[88] At the very least, cyberstalking and child pornography statutes and case law provide a helpful blueprint for identifying constitutional questions that should be addressed in any proposed legislation.

D. Good but Not Good Enough: Copyright Law, the Communications Decency Act, and the Fair Credit Reporting Act

As the law currently stands, there is no comprehensive statutory structure to protect online identity; rather, one who experiences this kind of harm must look to the federal laws to see if a remedy exists. Recent scholarship on anti-NCP statutes and online harms have focused on a variety of well-established precedents to import into the new technology.[89] Even popular news programs, such as the HBO show "Last Week Tonight with

83. *Compare* 18 U.S.C. § 2261(b) (2000), *with* 18 U.S.C. § 2261(b)(6) (2012) (adding a provision punishing violation of injunction, restraining order, or no-contact order with not less than one year's imprisonment).

84. *See* United States v. Morrison, 529 U.S. 598, 598 (2000).

85. *See id*. at 617.

86. *See* generally Diane McGimsey, *The Commerce Clause and Federalism after Lopez and Morrison: The Case for Closing the Jurisdictional-Element Loophole*, 90 CAL. L. REV. 1675, 1719 (2002) ("[T]he growth of communications networks across the United States has greatly increased the likelihood that any activity will involve some line crossing and thus potentially permits all activities to be regulated under the Court's current approach to the jurisdictional element [of Commerce Clause jurisprudence].").

87. *Compare* United States v. MacEwan, 445 F.3d 237, 253 (3d Cir. 2006) ("We therefore hold that the Internet is both a channel and instrumentality of interstate commerce and that Congress can regulate the downloading of child pornography over the Internet under 18 U.S.C. § 2252A(a)(2)(B) even if the transmission never crossed state lines."), *with* United States v. Hornaday, 392 F.3d 1306, 1311 (11th Cir. 2004) ("The internet is an instrumentality of interstate commerce.").

88. *See, e.g.*, *MacEwan*, 445 F3d. at 253; *Hornaday*, 392 F.3d at 1311 .

89. *See, e.g.*, Citron & Franks, *supra* note 7, at 346–347 (drawing on First Amendment doctrine); Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 67 (2009) (arguing for free speech protection); Derek E. Bambauer, *Exposed*, 98 MINN. L. REV. 2025, 2052–56 (2014) (proposing copyright law as a framework).

John Oliver," have discussed the applicability of copyright remedies to NCP, for example.[90]

Copyright law, as a potential method of combatting NCP, has the distinct advantage of being rooted in the federal Constitution and in a well-established statutory scheme.[91] It therefore might appear to offer an attractive alternative system of control over the use of information without violating the First Amendment.[92] In practice, however, copyright law leaves much to be desired, because website owners often ignore takedown requests, betting correctly that few victims will have the financial resources to go through protracted litigation.[93] The victim of NCP also may not have been the photographer, and therefore not the copyright owner.[94] Even if the victim took the photograph herself, the victim must first register new photos of her body with the United States Copyright Office in order to claim ownership of the content.[95]

More intangibly, reliance on copyright characterizes the harm as a violation of a property right, rather than a dignitary tort.[96] And, crucially, even a successful takedown notice cannot "put the genie back in the bottle" and prevent the same content from being reposted on another website.[97] Even if a victim owns the copyright and makes a timely demand for removal, Google will delink NCP, but will also provide a disclaimer, stating: "In response to a complaint we received under the US Digital Millennium Copyright Act, we have removed X result(s) from this page. If you wish, you may read the DMCA complaint that caused the removal(s) at [the website]," providing a direct link to the original content.[98]

Regardless of its shortcomings, copyright law is a quintessential example of one way the law regulates the flow of information in a way society feels is reasonable.[99] And, crucially, copyright even restricts some First Amendment rights.[100] Copyright protections may even be too strong, but the existence of a large body of copyright law makes it arguable that creating a protection for online identity, which could be seen as an individual's fundamental intellectual property, is not unprecedented. And copyright does

---

90. LastWeekTonight, *supra* note 30.

91. *See* U.S. CONST. art. I, § 8, cl. 8; Digital Millennium Copyright Act of 1998, 17 U.S.C. § 1201 *et seq.* (2012).

92. *See* SOLOVE, *supra* note 16, at 185.

93. *See* Citron & Franks, *supra* note 7, at 359–60.

94. *See id.*

95. *See* Mitchell A. Matorin, *In the Real World, Revenge Porn is Far Worse Than Making It Illegal*, TALKING POINTS MEMO (Oct. 18, 2013, 6:00 AM), http://talkingpointsmemo.com/cafe/our-current-law-is-completely-inadequate-for-dealing-with-revenge-porn [https://perma.cc/2JMN-XXWN].

96. *See* Citron & Franks, *supra* note 7, at 357 (citing Cristina Carmody Tilley, *Rescuing Dignitary Torts from the Constitution*, 78 BROOK. L. REV. 65, 65 (2012)).

97. *Id.* at 360.

98. *See* Matorin, *supra* note 95.

99. *See* SOLOVE, *supra* note 16, at 185 ("Control in the privacy context is seen as outlandish or impossible. Copyright law demonstrates otherwise.").

100. *See id.* at ch.7 n.77 (citing to Eldred v. Ashcroft, 537 U.S. 186, 190 (2003) ("Copyright's protections are so strong that even the First Amendment right to freedom of expression yields before them.")).

offer a way around another potential barrier to recovery for victims of NCP: section 230 of the Communications Decency Act.[101]

The Communications Decency Act ("CDA") was passed on February 1, 1996, in response to conservatives' concerns about Internet pornography.[102] Despite its origin as an attempt to protect children from "indecent" material on the Internet,[103] the statute has been broadly interpreted.[104] Though the Supreme Court struck down the vast majority of section 230 in a landmark case, the immunity provisions of section 230 that exempt secondary posters of content from liability remain.[105] Specifically, section 230 of the CDA has been applied by some courts to allow purposeful republishing by website owners of known illegal material (in some cases, including NCP) while effectively enjoying legal immunity.[106] State criminal law is also preempted by section 230, leaving a sizable loophole for intermediary posters, even in states with more stringent standards of liability.[107]

Accordingly, a federal statute aimed at protecting online identity might more appropriately be modeled after the Fair Credit Reporting Act. The Fair Credit Reporting Act ("FCRA") was adopted in 1970,[108] with an express goal of protecting consumer privacy.[109] To that end, the statute contains two provisions allowing private citizens to sue: one for willful non-compliance, and one for negligent non-compliance.[110] A recent case, however, which is again pending before the Ninth Circuit on remand from the Supreme Court,[111] has highlighted a potential constitutional standing issue with Congress's attempt to create private causes of action under the FCRA;[112] the plaintiffs

---

101. *See* Citron & Franks, *supra* note 7, at 359 ("[Section] 230 does not immunize websites from federal intellectual property claims.").

102. *See* Amanda L. Cecil, *Taking Back the Internet: Imposing Civil Liability on Interactive Computer Services in an Attempt to Provide an Adequate Remedy to Victims of Nonconsensual Pornography*, 71 WASH. & LEE L. REV. 2513, 2538–39 (2014).

103. *See* Reno v. ACLU, 521 U.S. 844, 868 (1997) ("[T]he purpose of the CDA is to protect children from the primary effects of 'indecent' and 'patently offensive' speech . . . .").

104. *See* Danielle Keats Citron & Neil Richards, *Can and Should Perez Hilton Be Held Liable for Reposting Celebrities' Private Nude Photos Without Their Consent?*, FORBES (Sept. 3, 2014, 4:41 PM), http://www.forbes.com/sites/daniellecitron/2014/09/03/can-and-should-perez-hilton-be-held-liable-for-reposting-celebrities-private-nude-photos-without-their-consent/#2715e4857a0b6a10e553327e [https://perma.cc/BS5E-DGTQ].

105. *See Reno*, 521 U.S. at 868 (1997); *see also* Citron & Franks, *supra* note 7, at 7.

106. *See* Citron & Franks, *supra* note 7, at 8.

107. Bambauer, *supra* note 89, at 2088 (citing 47 U.S.C. § 230(e)(3)).

108. Fair Credit Reporting Act, Pub. L. No. 91-508, 84 Stat. 1128 (codified as amended at 15 U.S.C. § 1681 et seq. (2012)).

109. *See* United States v. Bormes, 133 S. Ct. 12, 15 (2012).

110. *See generally* James Lockhart, Annotation, *Remedies Available in Private Action Under §§ 616 and 617 (15 U.S.C.A. §§ 1681n, 1681o) of Fair Credit Reporting Act—Other than Attorney's Fees*, 20 A.L.R. Fed. 2d 509 (2007) (compiling and analyzing cases that explore the types of remedies, other than attorneys' fees, available under the FCRA's two private causes of action); *see also* 15 U.S.C. §§ 1681n, 1681o.

111. *See* Robins v. Spokeo, Inc., 742 F.3d 409, 412 (9th Cir. 2014), *vacated*, 136 S. Ct. 1540 (2016).

112. *See* Brief for Petitioner Spokeo, Inc. at 36, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (No. 13–1339).

alleged that under the "statutory" cause of action, a plaintiff need not show actual harm to have standing, and that the false information about Robins itself was a willful violation of the statute.[113]

E. Jurisdiction and the Internet

The most compelling benefit of a federal statute cementing a federal cause of action and remedy is a simple one: uniformity and fairness. By nature, the Internet is multi-jurisdictional.[114] The need for a federal statute to combat malicious interference with online identity is apparent when considering the alternatives. Although tort law may appear attractive, it has traditionally been a matter of state discretion, which poses inherent problems to any comprehensive legislative remedy.

Questions of personal jurisdiction have arisen as a particularly problematic area of Internet law, and the varying approaches taken by federal courts around the country only serve to contribute to this general feeling of confusion.[115] Some federal courts, in analyzing whether personal jurisdiction exists over Internet activity, require the forum state to be the focal point of the defendant's allegedly slanderous or libelous statements, *and* that there be evidence of the website being accessed by residents of the forum state other than the plaintiff.[116] Does unauthorized access to a victim's Facebook account constitute "minimum contacts"? What about where the harm is felt? Many courts still apply a version of the *Calder* test, which leads to, at best, inconsistent results when applied to the Internet.[117] When NCP is posted to a website hosted on servers located exclusively in Indiana, hypothetically, what jurisdiction would a California court have over the contents? Will every court agree with the Northern District of Illinois that "[t]he fact that cyber-space was the medium for inflicting harm is of no moment"?[118]

F. Standing

In early 2016, the Supreme Court released its opinion in *Spokeo, Inc. v. Robins*, which focused on whether Congress has the power to grant a plaintiff standing to sue in federal court by statute, the FCRA, without a showing of traditional concrete harm.[119] Standing consists of three elements: 1) an injury-

113. *See Robins*, 742 F.3d at 412.

114. *See, e.g.*, WRIGHT ET AL., *Supra* note 65; *see also* Burk, *supra* note 62, at 21–24.

115. *See, e.g.*, Diane McGimsey, *The Commerce Clause and Federalism after Lopez and Morrison: The Case for Closing the Jurisdictional-Element Loophole*, 90 CAL. L. REV. 1675, 1719–20 (2002) (discussing holding in United States v. Kammersell, 196 F.3d 1137 (10th Cir. 1999), that a Utah resident who sent his girlfriend a threatening instant message via AOL, which traveled through a server in Virginia, was sufficient to satisfy "interstate commerce" requirement of federal statute).

116. *See* WRIGHT ET AL., *Supra* note 65.

117. *See id.*

118. *See* Info. Techs. Intern., Inc. v. ITI of N. Fla., Inc., 2001 WL 1516750, at *7–8 (N.D. Ill. 2001).

119. *See* Brief for Petitioner Spokeo, Inc. at 36, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (No. 13–1339); *see also* Spokeo Inc. v. Robins, 136 S. Ct. 1540, 1544–45 (2016).

in-fact, 2) which is fairly traceable to the defendant's conduct, and 3) is likely to be redressed by judicial decision.[120] Because injury-in-fact is an Article III constitutional requirement, Congress cannot grant standing to a plaintiff merely through statutory fiat.[121] The FCRA establishes, in sections 1681n and 1681o, that failure to comply with certain minimum standards gives rise to a cause of action.[122] Robins argued that the statutory violation was harm in and of itself.[123] In terms of devising an online identity statute, this problem should be avoided by writing into the statute itself that damage to an online identity is a cognizable harm. A major barrier to potential lawsuits is that the current trends in data breach law, for example, do not allow for lawsuits when economic injury cannot be shown.[124] Typically, most courts do not find a threat of future harm to be sufficient injury to confer standing upon a plaintiff.[125] The Supreme Court's doctrine of Article III standing requires "injury in fact," which is both "concrete and particularized," and "not conjectural or hypothetical".[126] The Court attempted to clarify the "concrete and particularized" requirement in *Spokeo* by explaining that "particularized" injury means it "must affect the plaintiff in a personal and individual way."[127] While particularization is necessary to establish injury in fact, it is not sufficient; the injury must also be concrete.[128] In the words of the Court, a concrete injury must "actually exist," but that is not necessarily synonymous with "tangible."[129] In dicta, the Court explained the risk of real harm can, in circumstances like libel or slander *per se*, satisfy the concreteness requirement.[130] In such cases, the plaintiff "need not allege any *additional* harm beyond the one Congress has identified."[131] This Note will therefore argue that the interference with online identity itself is one of those cases where a technical violation would result in a cognizable injury-in-fact, as specifically defined in the proposed federal statute, and should be sufficient to provide standing, even under the current *Spokeo* framework.[132]

120. *See* 136 S.Ct. at 1547 (citing Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992)).

121. *See* 136 S.Ct. at 1547–48.

122. *See* 15 U.S.C. §§ 1681n, 1681o.

123. *See* Brief of Respondent Thomas Robins at 15, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (No. 13–1339).

124. *See generally In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1211–12 (N.D. Cal. 2014); Carlsen v. GameStop, Inc., 112 F. Supp. 3d 855, 860 (D. Minn. 2015) (pending appeal).

125. *See generally* Brief for Petitioner Spokeo, Inc. at 36, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (No. 13–1339).

126. *Spokeo Inc.*, 136 S. Ct. at 1548.

127. *See id.* (citations omitted).

128. *See id.*

129. *See id.* at 1549.

130. *See id.*

131. *See id.*

132. The case is currently on remand to the Ninth Circuit, and may return to the Supreme Court for another round. *See* Allison Grande, *Spokeo Points 9th Circ. to Sister Court's Denials*, LAW360 (Dec. 2, 2016), https://www.law360.com/appellate/articles/868587/spokeo-points-9th-circ-to-sister-courts-denials.

IV. ANALYSIS & PROPOSAL: TOWARD A FEDERAL STATUTE

A federal statute would be the most effective remedy for the current state of affairs, where the Supreme Court has yet to fully confront questions of Internet jurisdiction, speech, and online-to-offline harm.[133] Though several states have made efforts to create or expand a right to online identity, they have largely sought to accomplish this through modest expansions of traditional privacy-tort law.[134] Law will never develop simultaneously with technology;[135] but as our technology becomes rapidly more complex, it is essential that any new legislation leave substantial breathing room for novel concepts.

The federal statute proposed here includes both civil and criminal elements. Tort law lends a useful framework to this statute, and constitutional torts can similarly create a federal cause of action.[136] After first laying out a substantive proposal, this section of the Note will then discuss arguments in favor of, and in opposition to, such a statute, and finally will conclude by disposing of likely constitutional challenges.

A. Malicious Interference with Online Identity

This Note proposes establishment of a federal tort and a federal crime for malicious interference with online identity. The ideal formulation for the tort of malicious interference with online identity is similar to civil battery[137]: 1) an act, uploading the information to the Internet; 2) with intent to harm the victim or their online identity; and contact, where information that reaches the victim is harmful or offensive to a reasonable person,[138] or which the perpetrator would have reason to know would be harmful or offensive to that particular person (e.g., NCP uploaded by a former lover). Crucially, like the FCRA, and as discussed in *Spokeo*, the cause of action must be specific, concrete, and identify the misinformation itself as the harm against which the

133. *See* discussion *supra* Section III.E–F.

134. *See, e.g.*, Connallon, *supra* note 58, at 77–82 (reviewing modern state privacy-tort law in the context of the Restatement Prosser-style four privacy rights). *Compare* MASS. GEN. LAWS ANN. ch. 214, § 1B (West 2015) ("A person shall have a right against unreasonable, substantial or serious interference with his privacy."), *with* White v. Davis, 13 Cal. 3d 757, 775 (1975) (en banc) ("[T]he amendment is intended to be self-executing, i.e., that the constitutional provision, in itself, creates a legal and enforceable right of privacy for every Californian." (interpreting Art. 1 § 1 of California State Constitution)).

135. *See* ROBERT J. KLOTZ, THE POLITICS OF INTERNET COMMUNICATION 136 (2004) ("One fundamental challenge of cyberlaw is that technology moves faster than the law.").

136. *See* Tilley, *supra* note 67, at 76–77 ("Several theories of the Ninth Amendment suggest that the rights protected by the dignitary torts may be among those 'retained by the people' and thus shielded from disparagement relative to those enumerated in the Constitution.").

137. *See, e.g.*, W. Va. Fire & Cas. Co. v. Stanley, 216 W.Va 40, 51 (2004) ("An actor is subject to liability to another for battery if (a) he acts intending to cause a harmful or offensive contact with the person of the other or a third person, or an imminent apprehension of such a contact, and (b) a harmful contact with the person of the other directly or indirectly results." (citing RESTATEMENT (SECOND) OF TORTS § 13 (1965)).

138. *See, e.g.*, *infra* note 157 (cat picture subreddit versus porn star).

statute should protect.[139] Further, civil damages should be measured similarly to the intentional infliction of emotional distress tort, including, but not limited to, physical injury, lost wages (with a duty to mitigate), reimbursement for psychotherapy, and costs of issuing takedown notices. The proposed federal tort statute should thus state: any person who, knowing he is not authorized or privileged to do so, intentionally discloses identity information about another that he knew, or should have known, would harm the individual's online identity, with the intent to cause or attempt to cause substantial emotional distress as a result, shall be liable to the individual victim for actual damages, such amount of punitive damages as the court may allow, and in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

Practically speaking, American tort law often requires a plaintiff to have two things: physical injury, and deep pockets. Interference with online identity, by its very nature, will frequently have no physical injury—until or unless humans have avatars walking the physical world in their stead.[140] But by establishing a federal cause of action that need not show physical injury, similar to sections 1681n and 1681o of the FCRA,[141] Congress should recognize that the injury-in-fact *is* the damage to the individual's online identity. Further, class actions are not without precedent, especially in the FCRA context,[142] and would alleviate the need for an individual plaintiff to bear the costs of the entire litigation. Given the heavy burden on a plaintiff tackling a civil and criminal case simultaneously, class actions would significantly lessen that burden and provide an avenue to obtain judgment against serial bad actors.

As with data privacy statutes, the most important section of this legislation will be the Definitions. Clearly defining "online identity" and "malicious interference" is essential. As a threshold matter, what should "online identity" mean? Implicitly, the phrase assumes that there is something inherently distinct about an online identity. The statute should define online identity as a comprehensive overview of information about an individual,

---

139. *See* Transcript of Oral Argument at 21, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (No. 13–1339), https://www.supremecourt.gov/oral_arguments/argument_transcripts/2015/13-1339_j5fl.pdf [https://perma.cc/6ZQY-BJA6].

140. This is not especially far-fetched. *See, e.g.*, Victoria Thorp, *Beam store on University Avenue gives Palo Alto a glimpse into a robotic future*, PALO ALTO PULSE (Mar. 2, 2015), http://www.paloaltopulse.com/2015/03/02/beam-store-on-university-avenue-gives-palo-alto-a-glimpse-into-a-robotic-future [https://perma.cc/78TW-UUYE]; *see also President Obama greets Alice Wong via Beam during the ADA's 25th Anniversary*, BEAM:BLOG (July 21, 2015), http://blog.suitabletech.com/2015/07/21/president-obama-beam [https://perma.cc/H7EF-G29K].

141. *See* 15 U.S.C. §§1681n, 1681o.

142. *See generally In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 851 F. Supp. 2d 1040, 1047 (S.D. Tex. 2012); Soutter v. Equifax Info. Servs., LLC, 307 F.R.D. 183, 195 (E.D. Va. 2015).

information which is "continuous and dynamic," and which can be ascribed to the individual by others.[143]

To simplify, in the following example "the individual" will be referred to as "N." Identity information can be directly within N's control (e.g., a personal Facebook profile, to which she has a right to exclude others);[144] indirectly within her control (e.g., a photograph taken by N's Facebook friend in which N is tagged); or entirely outside her control (e.g., a Craigslist solicitation posting uploaded by an ex-boyfriend).[145] The federal statute should not limit online identity to the sources with which the public is currently familiar, such as Google and Facebook, but should extend to any website or platform that hosts, links to, compiles or processes an individual's personal information. Platforms should not be directly liable for hosting information about N which later turns out to be false, as that would result in a profoundly overbroad chilling effect on speech.[146] But this must be balanced against N's interest in recovering against, for example, an ex-boyfriend "P", who posts nude photographs to a shared Facebook group.[147] It is not difficult to imagine how, to proving liability, a plaintiff may have difficulty attributing the unconsented-to content to a particular perpetrator—e.g., if Facebook expeditiously removes the original photos, but duplicates continue to be hosted on a subdomain of the social media site reddit (also known as a "subreddit"); an individual plaintiff without very deep pockets would effectively be estopped from asserting her rights altogether.[148] Ideally, a malicious user should not be able to escape liability by simply reposting the content to another web host.[149] It is crucial to recognize that this statute aims

---

143. *See* Elad Oreg, *Right to Information Identity*, 29 J. MARSHALL J. COMPUTER & INFO. L. 539, 580–81 (2012).

144. This Note does not address the applicability of terms like Personally Identifiable Information ("PII"), agreeing with Professor Ohm that PII is unworkable, ever-expanding, and unsuccessful at defining what information will identify an individual. *See* Ohm, *supra* note 57, at 1742; *see also id.* at 1765–1768 (listing "five factors for assessing the risk of privacy harm": "data handling techniques," "private versus public release," "quantity," "motive," and "trust").

145. *See* DeeDee Correll, *Former boyfriend used Craigslist to arrange woman's rape, police say*, L.A. TIMES (Jan. 11, 2010), http://articles.latimes.com/2010/jan/11/nation/la-na-rape-craigslist11-2010jan11 [https://perma.cc/57DA-EP5E] (providing example of identity information outside the control of the individual).

146. *See* SOLOVE, *supra* note 16, at 182 ("A line must be drawn at cyberspace; once the information is out on the Internet, those subsequently discussing and disseminating it should not be liable. To conclude otherwise would seriously chill the freewheeling and lively discussion that rapidly erupts across the blogosphere.").

147. *See, e.g.*, Andrew Liptak, *The US military is investigating a secret Facebook group that spread naked pictures of service women*, VERGE (Mar. 5, 2017), https://www.theverge.com/2017/3/5/14820242/military-investigating-secret-facebook-group-marines-united-service-women [https://perma.cc/7VSM-82N6].

148. *See, e.g.*, Mitchell A. Matorin, *In the Real World, Revenge Porn is Far Worse Than Making It Illegal*, TALKING POINTS MEMO (Oct. 18, 2013, 6:00 AM), http://talkingpointsmemo.com/cafe/our-current-law-is-completely-inadequate-for-dealing-with-revenge-porn [https://perma.cc/97EV-3ZXM].

149. This is a classic and ongoing problem with hosting sites like The Pirate Bay, which envisions itself as a "hydra", alluding to its unstoppable rebirth as soon as one site is shut down. *See, e.g.*, Emil Protalinski, *The Pirate Bay is not down: Domain redirect problem has an easy fix*, VENTUREBEAT (May 24, 2015, 8:25 AM) http://venturebeat.com/2015/05/24/the-pirate-bay-is-not-down-domain-redirect-problem-has-an-easy-fix [https://perma.cc/2J9L-46YQ].

not to control the behavior of third-party consumers of N's information,[150] or of websites that may repost the original content. Rather, it aims to give the victim "decision-making authority about oneself, from which one can presumptively exclude others."[151]

Identifying information should not be strictly defined by Personally Identifiable Information ("PII"), as in data breach statutes.[152] Doing so would not only ensure that the statute would be vulnerable to rapid changes in technology,[153] but it also would enshrine a reductive understanding of what constitutes identity.[154] Instead of specifying particular characteristics to consider, the statute should be triggered when a reasonable person would be misled by the interference with the victim's identity. It is key to focus the law on the victim's ability to control the dissemination of identity information, rather than on the perpetrator's. As Professor Oreg notes, in impersonation law, certain jurisdictions only recognize the offense if there is intent to defraud, which exculpates perpetrators who impersonate a victim in order to harm the victim, and not others.[155] This is exactly the type of harm this statute is designed to rectify.

Factors to consider in an analysis of whether a reasonable person would confuse the two versions of an online identity (e.g., Dr. Holly Jacobs, PhD versus "Holly Jacobs", sex addict) should include: trustworthiness of the source;[156] ability to identify the content poster (anonymous posters are

---

150. As a moral issue, accessing such sensitive information may be repugnant, but a federal statute should refrain from addressing it due to First Amendment concerns. *See* SOLOVE, *supra* note 16, at 182 ("[O]nce the information is on the Internet, however, it would be impractical and problematic to hold liable others beyond the person who initially placed it there."). As a practical matter, a large part of modern internet culture involves online "stalking" one's acquaintances. *See, e.g.*, Carol Roth, *The Right Way to 'Stalk' People Online*, ENTREPRENEUR (July 15, 2014), http://www.entrepreneur.com/article/235080 [https://perma.cc/X2VU-UDEV].

151. *See* Daniel R. Ortiz, *Privacy, Autonomy, and Consent*, 12 HARV. J.L. & PUB. POL'Y 91, 92 (1989).

152. *See, e.g.*, Paul M. Schwartz and Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 82 N.Y.U. L. REV. 1814, 1845–47 (2011); *see also* Ohm, *supra* note 57, at 1742 (comparing the constant need to amend the definition of PII to a game of whack-a-mole).

153. For example, many state legislatures have pending bills to supplement data breach statutes' definition sections with obsolete additions. In New Jersey, for example, the State Legislature introduced A.B. 1239 in 2014, which proposed new restrictions on "magnetic-stripe data" of credit or debit cards. By October 2015, banks had moved to "chip-and-PIN" cards where customer data is stored only in an embedded microchip (and not in the magnetic strip). *See* A.B. 1239, NJ ASSEMBLY, http://www.njleg.state.nj.us/2014/Bills/A1500/1239_I1.HTM [https://perma.cc/GMX6-VHEF] (last visited Apr. 10, 2016); *see also* Kim Zetter, *Hacker Lexicon: What are Chip and PIN Cards?*, WIRED (Apr. 15, 2015, 9:00 AM), http://www.wired.com/2015/04/hacker-lexicon-chip-pin-cards [http://www.wired.com/2015/04/hacker-lexicon-chip-pin-cards].

154. *See* Oreg, *supra* note 143, at 585 ("There is a temptation to attempt to objectively determine the importance of different aspects of a person's life which constitute his identity . . . [but] [u]ltimately, any attempt to grade the aspects of a person's life using categorical classifications will be simplistic . . . .").

155. *See id.* at 587.

156. The trustworthiness of a source should consider the purpose of the hosting site; i.e., a post on Backpage, a website preferred by prostitutes for advertising, is far less trustworthy

generally less trustworthy than named posters); similarity to the victim's existing online profile; and the victim's subjective belief in the distortion's importance (e.g., N might not bring litigation to protect her identity from impersonation on a subreddit about cat pictures, but would find it more troubling to have her head Photoshopped onto the body of a porn star).[157] This test may also be satisfied by circumstantial evidence, if, for example, a victim can show a series of job interviews that were suddenly cancelled after a prospective employer initiated a Google search or background check that yielded misinformation, or if the general public and members of the community report knowledge of the perpetrator's misinformation.[158] But the individual need not show specific economic harm; so long as the harm shown satisfies Article III standing requirements,[159] the harm is the misinformation itself.[160]

B. Criminal Interference with Online Identity

Federal laws against cyberstalking and state laws against NCP are both useful tools to protect online identity, but they do not accomplish the expressive justice purpose that the proposed federal statute would. Take the example of Hunter Moore, the "most hated man on the Internet," who created Is Anyone Up?, a website that hosted and disseminated revenge porn images.[161] In contrast to Noe Iniguez, the first defendant to be convicted under California's state anti-revenge porn law and who received a year's prison sentence,[162] Moore and an accomplice were federally indicted.[163] He eventually pled guilty to one count of unauthorized access to a protected computer and one count of aggravated identity theft, and was sentenced to

---

than Facebook, Craigslist is less trustworthy than Google+, Facebook is less trustworthy than a verified Twitter, etc.

157. *See id.* at 588 ("[A]n offense reflecting a true commitment to the right of identity would grade the gravity of the offense and its surrounding circumstances in accordance with the importance of the stolen identity and the degree of its distortion, and not just according to the severity of the other offense made possible by the impersonation.").

158. *See* discussion *supra* Section III.A.

159. Again, *Spokeo* is back in the Ninth Circuit on remand, and leaves questions about what exactly is required for standing in such a case. Amy Howe, *Opinion analysis: Case on standing and concrete harm returns to the Ninth Circuit, at least for now*, SCOTUSBLOG (May 16, 2016, 6:45 PM), http://www.scotusblog.com/2016/05/opinion-analysis-case-on-standing-and-concrete-harm-returns-to-the-ninth-circuit-at-least-for-now/ [https://perma.cc/F3L6-T2FP].

160. Justice Ruth Bader Ginsburg's dissent in the latest iteration of *Spokeo* provides some support for this approach. *See* Spokeo, Inc. v. Robins, 136 S. Ct. at 1556 (Ginsburg, J., dissenting) ("I therefore see no utility in returning this case to the Ninth Circuit to underscore what Robins' complaint already conveys concretely: Spokeo's misinformation "cause[s] actual harm to [his] employment prospects.").

161. Jessica Roy, *Revenge-Porn King Hunter Moore Indicted on Federal Charges*, TIME (Jan. 23, 2014), http://time.com/1703/revenge-porn-king-hunter-moore-indicted-by-fbi [https://perma.cc/E2JC-UTEW].

162. *See* Rocha, *supra* note 77.

163. Roy, *supra* note 161.

two-and-a-half years in federal prison.[164] Had there been a federal criminal penalty for malicious interference with online identity, as herein proposed, Iniguez and Moore's sentences may have been similar, but expressive justice would be much better served. As Professors Danielle Keats Citron and Mary Anne Franks have noted, while Moore's conviction is cause for celebration, it does not make existing law any more successful at protecting an individual's identity: "[t]he fact that one revenge porn site owner allegedly broke numerous federal laws in running a revenge porn website does not change the fact that *he is facing no charges for publishing the content itself* . . . ."[165] In the absence of a federal remedy tailored to these specific societal concerns, the power of expressive justice is lost. The ends do not justify the means.

Moreover, the most salacious and well-publicized examples of interference with N's online identity typically cross over into criminal law. Here, the issue is not simply whether a reasonable person could tell the difference between the "real" N and the "doppelganger" N, but whether the perpetrator himself has breached a societal norm that deserves prosecution. And, crucially, a federal statute, with both civil and criminal enforcement mechanisms, provides a two-fold authority that encompasses both "judgment-proof" defendants and those practically immune to criminal prosecution (i.e., sites protected by section 230 of the CDA).

The existing federal cyberstalking statute, 18 U.S.C. section 2261(a), requires the perpetrator to engage in a "course of conduct" intended to harass or intimidate a victim;[166] a "course of conduct" is defined as "a pattern of conduct composed of [two] or more acts, evidencing a continuity of purpose."[167] However, this ignores the reality of viral sharing on the Internet today. A single upload may be shared thousands of times, reaching an audience of millions, and yet would not likely qualify as a "course of conduct."[168] Accordingly, the proposed federal statute would criminalize even the initial act of posting, but scale the penalties in accordance with the audience reached and harm caused. Taking elements from California's more narrow approach and New Jersey's broader one,[169] the federal statute would provide: it is a crime for an actor, knowing he is not authorized or privileged to do so, to intentionally disclose identity information about another that he knew, or should have known, would harm the individual's online identity, with the intent to cause or attempt to cause substantial emotional distress as a result. A knowledge requirement regarding consent is crucial in order to protect reporters and news media; it is the reporter's job to inquire into where

164. Abby Ohlheiser, *Revenge porn purveyor Hunter Moore is sentenced to prison*, WASH. POST (Dec. 3, 2015), https://www.washingtonpost.com/news/the-intersect/wp/2015/12/03/revenge-porn-purveyor-hunter-moore-is-sentenced-to-prison [https://perma.cc/M6W2-4PVR].

165. *See* Citron & Franks, *supra* note 7, at 368 (emphasis added).

166. *See* Citron & Franks, *supra* note 7, at 365–66.

167. *See* 18 U.S.C. § 2266 (2012).

168. *See* Citron & Franks, *supra* note 7, at 365–66.

169. *Compare* CAL. PEN. CODE § 647(j)(4) (2015) (listing specific sexual acts covered by statute), *with* N.J. STAT. ANN. § 2C:14–9 (2004) (criminalizing unconsented disclosure of reproduction of images showing "an act of sexual penetration or sexual contact").

the information comes from. There should also be a specific carve-out to defeat a "heat of passion" mitigating theory as in voluntary manslaughter: "adequate provocation" shall be no defense. The definition of online identity for criminal infractions, therefore, should be substantially similar to the civil one. This emphasizes the holistic intent of the statute to protect the integrity of online identity.

C. Arguments Against Creating a Right of Online Identity: Constitutional Challenges

The clearest obstacle to the proposed federal statute is the First Amendment's Free Speech Clause. There is evidence to suggest that the Supreme Court would not look favorably upon a federal statute of such breadth.[170] However, because this proposed statute is narrowly tailored, rejects the binary public/private conception of privacy and seeks to regulate a category of speech between historically circumscribed child pornography and defamation, it passes constitutional muster.

1. The First Amendment

Privacy interests clash directly with First Amendment jurisprudence because privacy is not limited to controlling falsehoods, as in defamation cases.[171] The essence of a right to privacy in one's online identity is effectively a right to exclude, but it is not absolute.[172] In order to avoid invalidation by the First Amendment, the federal statute must be narrowly tailored to focus on the individual's right to speak, on the Internet if she so chooses, about her own life, and to prevent others from interfering with the "intellectual property" of her identity.[173] The statute should not be evaluated under a strict scrutiny standard because the kind of speech the statute seeks to restrict is most analogous to defamation, and therefore is outside the scope of the First Amendment altogether.[174] But even if it were evaluated under strict scrutiny, this proposal should prevail.

---

170. *See, e.g.*, Bambauer, *supra* note 89, at 2087–88 ("Under Chief Justice John Roberts, the Supreme Court has been especially rigorous about evaluating[, under the First Amendment,] laws that also made strong claims to tangible harms, from bans on crush videos involving the torture of animals to limits on violent video games due to negative effects on minors, to tort liability for the deliberate infliction of emotional distress upon a deceased veteran's family during his funeral procession, and to limits on government funding based on the need to reduce prostitution as a means of fighting the spread of HIV/AIDS." (citations omitted)).

171. *See* SOLOVE, *supra* note 16, at 126–27 (2007).

172. *See id.* at 170 ("[Privacy] involves establishing control over personal information, not merely keeping it completely secret.").

173. *See id.* at 134.

174. *See id.* at 186–87 ("The right to withdraw from the public gaze at such times as a person may see fit, when his presence in public is not demanded by any rule of law, is also embraced within the right of personal liberty."(citing Pavesich v. New England Life Ins. Co., 50 S.E. 68, 70 (Ga. 1905) (the first decision to recognize the appropriation tort)). These cases developed before the Supreme Court had established the now-canonical system of levels of scrutiny; *Pavesich* grounded the right to control individual disclosure in the Fourteenth

The First Amendment does not protect every kind of speech. For example, it does not extend to speech used to "engage in fraud," "to form and advance conspiracies," or "to solicit criminal acts."[175] It also does not bar the imposition of tort liability for defamatory statements.[176] Similarly, punishing online speech that maliciously interferes with another's identity should not be considered an abridgement of the freedom of speech.[177] The trouble with First Amendment doctrine, however, is that the greater does not always include the lesser power.[178] NCP falls somewhere between child pornography, which the Supreme Court has held is entirely outside the First Amendment,[179] and traditional defamation law, which the Court has struggled to update to modern standards.[180] Defamation and libel law were both well-established at the time of the First Amendment's ratification, making a strong originalist argument for why they should still apply in an Internet context.[181] Supreme Court precedent suggests that it will view the Internet as the next frontier of communications technology, and will likely apply the same standards of First Amendment scrutiny.[182] In dicta, the Court also acknowledged the problem of the "community standards" test as applied to the Internet: "[T]he 'community standards' criterion as applied to the Internet means that any communication available to a nationwide audience will be judged by the

---

Amendment's "liberty" interest. 50 S.E. at 70 ("Liberty includes the right to live as one will, so long as that will does not interfere with the rights of another or of the public. One may desire to live a life of seclusion; another may desire to live a life of publicity; still another may wish to live a life of privacy as to certain matters, and of publicity as to others.").

175. Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 U.C.L.A. L. REV. 1149, 1171 (Apr. 2005) (citing to KENT GREENAWALT, SPEECH, CRIME, AND THE USES OF LANGUAGE 40 (1989)).

176. GREGORY E. MAGGS & PETER J. SMITH, CONSTITUTIONAL LAW: A CONTEMPORARY APPROACH 994 (3d ed. 2015) (citing Beauharnais v. Illinois, 343 U.S. 250, 266 (1952)).

177. Richards, *supra* note 175, at 1171.

178. *See, e.g.*, R.A.V. v. City of St. Paul, 505 U.S. 377, 401 (1992) (White, J., concurring in the judgment) ("It is inconsistent to hold that the government may proscribe an entire category of speech because the content of that speech is evil, but that the government may not treat a subset of that category differently without violating the First Amendment; the content of the subset is by definition worthless and undeserving of constitutional protection.").

179. *See* New York v. Ferber, 458 U.S. 747, 765 n. 18 (1982) ("Today, we hold that child pornography . . . is unprotected speech subject to content-based regulation. Hence, it cannot be underinclusive or unconstitutional for a State to do precisely that.").

180. *Compare* Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 758–59 (1985) ("[S]peech on 'matters of public concern' . . . is 'at the heart of the First Amendment's protection.'"), *with* Snyder v. Phelps, 562 U.S. 443, 454 (2011) (finding public concern present where the Westboro Baptist Church picketed an individual soldier's funeral due to the "overall thrust and dominant theme of Westboro's demonstration" speaking to broader public issues); *see also Phelps*, 562 U.S. at 465–471 (Alito, J., dissenting) ("[A]lthough this court has not decided the question, I think it is clear that the First Amendment does not entirely preclude liability for the intentional infliction of emotional distress by means of speech. . . . The First Amendment allows recovery for defamatory statements that are interspersed with nondefamatory statements on matters of public concern . . . .").

181. *See, e.g.*, Chaplinsky v. New Hampshire, 315 U.S. 568, 571–72 (1942) ("There are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which have never been thought to pose any Constitutional problem. These include . . . the libelous . . . .").

182. *See* Reno v. ACLU, 521 U.S. 844, 870 (1997).

standards of the community most likely to be offended by the message."[183] Therefore, the proposed federal statute must establish a firm baseline upon which potential perpetrators, prosecutors, and judges can rely.

Even if the Supreme Court were to determine this kind of restriction on speech to be content-based, it would still survive strict scrutiny because the proposed statute is narrowly tailored to advance the government's interest in protecting the health and safety of its citizens, as well as their ability to contribute to and participate in the national economy.[184] It is crucial to differentiate the proposed statute from other content-based restrictions on speech because this proposal does not seek to punish the *underlying speech*.[185] The statute is not aimed at preventing nude photographs from being taken, but *only* at preventing their dissemination, with scienter, via a particularly far-reaching mode of publication (i.e., the Internet).[186] Nonetheless, consent to share with a wider audience should be an absolute defense. As Professor Daniel Solove explains: "[w]e want to limit the flow of information, not stop it completely."[187] Consent to share should therefore be evaluated by degree. Consent to share between intimate partners, or even on some parts of the Internet like a support community, is quintessentially distinct from consent to share with the entire Internet. Finally, as a policy matter, criminalizing malicious dissemination of NCP will actually encourage *more* speech. In the current legal landscape, rather than risk being victimized, individuals are often told to simply stop engaging in the underlying speech.[188] Criminalizing NCP thus recognizes that consensual sexual photography is not a disappearing trend,[189] and will actually encourage more expression by removing some of the fear of exposure beyond the intended audience.

---

183. *See id.* at 877–78.

184. *See* Boos v. Barry, 485 U.S. 312, 321 (1988); Sable Commc'ns of Cal., Inc., v. FCC, 492 U.S. 115, 126 (1989) ("The Government may, however, 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.").

185. *Boos*, 485 U.S. at 336 ("[A]ny restriction on speech, the application of which turns on the content of the speech, is a content-based restriction regardless of the motivation that lies behind it.").

186. In one of the few existing court challenges to a state anti-NCP law, a Vermont court grappled with this problem. *See* State v. Van Buren, No. 1144-12-15Bncr (Vt. Super. July 1, 2016). Finding NCP to not fall into the obscenity category of unprotected speech, the court concluded the statute failed the least restrictive means test because, as a hypothetical, the statute would also "criminalize disclosure by a party who never had any relationship with complainant and who received such unsolicited sexual photographs and decided to disclose them to convince complainant not to send any more or out of anger for being the recipient." The proposed statute is narrowly tailored to punish only disclosure with intent to harm, and therefore should survive a similar challenge.

187. *See* SOLOVE, *supra* note 16, at 184.

188. *See, e.g.*, Helena Horton, *Revenge porn: 'Grow up' and stop taking naked photos to avoid becoming a victim, say police*, TELEGRAPH (Feb. 18, 2016), http://www.telegraph.co.uk/women/life/revenge-porn-grow-up-and-stop-taking-naked-photos-to-avoid-becom/ [https://perma.cc/FB7R-3LQM].

189. *See, e.g.*, Ashley Welch, *How popular is sexting? The numbers may surprise you*, CBS NEWS (Aug. 10, 2015), http://www.cbsnews.com/news/sexting-popular-among-adults-study-finds [https://perma.cc/9FRA-BLAY].

V. CONCLUSION

There will always be tension between the right to control one's identity and the right to free expression. Because the Internet is a relatively new technology—one that promises to bring long-lasting change—Congress is the appropriate body to put forward a federal law that addresses changing norms. The harms of NCP and the difficulty of extricating one's online identity from one's offline identity illustrate the clear benefits of a bright-line statutory rule. Yet the First Amendment can, and should, allow for some limited and narrowly tailored government regulation of online speech. Therefore, an omnibus law that includes both civil and criminal penalties would deliver a comprehensive castigation of those bad actors who seek to permanently damage others' online identities.